

Cisco ISE Syslogs

First Published: 2019-02-18

Last Modified: 2026-08-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

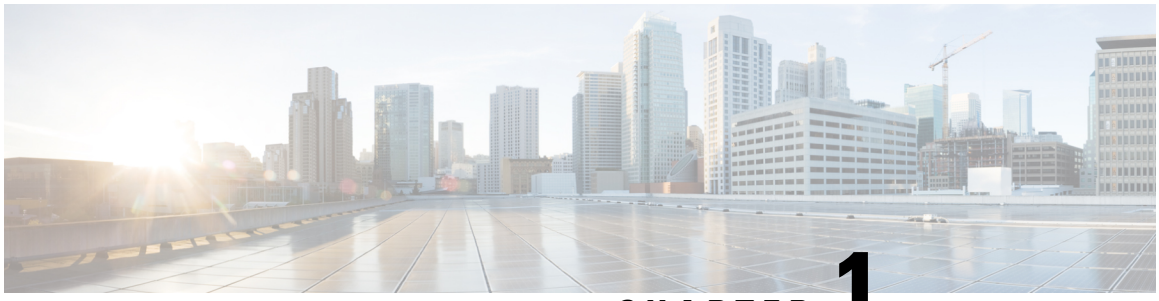
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Introduction to Cisco ISE Syslogs

- Cisco ISE Message Catalog , on page 1
- Local Store Syslog Message Format, on page 1
- Remote Syslog Message Format, on page 3

Cisco ISE Message Catalog

Cisco Identity Services Engine (ISE) provides a logging mechanism that is used for auditing, fault management, and troubleshooting. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

In Cisco ISE, system logs (syslogs) are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer them to an external server.

You can use the Message Catalog page of the Cisco ISE dashboard to view all possible log messages and the descriptions. Choose **Administration** > **System** > **Logging** > **Message Catalog**.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. The data available in this page are for display only. If you are using Cisco ISE 2.3 and greater releases, choose **Export** to export all the syslog messages in the form of a CSV file .

For more information on the Cisco ISE logging mechanism, configuring syslog purge, configuring remote syslog collection locations, and other tasks, see the Chapter Maintain and Monitor in the *Cisco ISE Administrator Guide* for your release.

Local Store Syslog Message Format

Cisco ISE log messages are sent to the local store with this syslog message format:

timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value

Field	Description
timestamp	Date of the message generation, according to the local clock of the originating the Cisco ISE node, in the following format : *YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm*. Possible values are: • YYYY = Numeric representation of the year. • MM = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • hh = The hour of the day—00 to 23. • mm = The minute of the hour—00 to 59. • ss = The second of the minute—00 to 59. • xxx = The millisecond of the second—000 to 999. • +/-zh:zm = The time zone offset from the Cisco ISE server's time zone, where zh is the number of offset hours and zm is the number of minutes of the offset hour, all of which is preceded by a minus or plus sign to indicate the direction of the offset. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
sequence_num	Global counter of each message. If one message is sent to the local store and the next to the syslog server target, the counter increments by 2. Possible values are 0000000001 to 999999999.
msg_ode	Message code as defined in the logging categories.
msg_sev	Message severity level of a log message. See **Administration** > **System** > **Logging** > **Logging Categories**.
msg_class	Message class, which identifies groups of messages with the same context.
msg_text	English language descriptive text message.
attr=value	Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the Cisco ISE dictionaries. Values of the Response direction AttributesSet are bundled to one attribute called Response and are enclosed in curly brackets {}. In addition, the attribute-value pairs within the Response are separated by semicolons. For example, Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;}

Remote Syslog Message Format

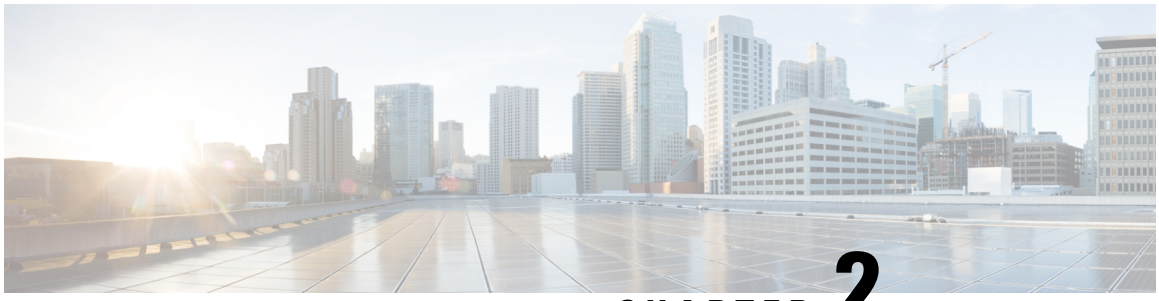
Cisco ISE log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format:

pri_num Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

Field	Description
pri_num	Priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. Refer the relevant Cisco ISE Administrator Guide for your release to set security levels for message codes. The facility code valid options are: • LOCAL0 (Code = 16) • LOCAL1 (Code = 17) • LOCAL2 (Code = 18) • LOCAL3 (Code = 19) • LOCAL4 (Code = 20) • LOCAL5 (Code = 21) • LOCAL6 (Code = 22; default) • LOCAL7 (Code = 23)
time	Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format Mmm DD hh:mm:ss. Possible values are: • Mmm = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number. • hh = The hour of the day—00 to 23. • mm = The minute of the hour—00 to 59. • ss = The second of the minute—00 to 59. Some devices send messages that specify a time zone in the format -/+hhmm, where - and + identifies the directional offset from the Cisco ISE server's time zone, hh is the number of offset hours, and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
xx:xx:xx:xx/host_name	IP address of the originating Cisco ISE node, or the hostname.

Field	Description
cat_name	Logging category name preceded by the CISExxx string.
msg_id	Unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.
total_seg	Total number of segments in a log message. Long messages are divided into more than one segment. **Note** The *total_seg* depends on the Maximum Length setting in the remote logging targets page. See *Remote Logging Target Settings*.
seg_num	Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

The syslog message data or payload is the same as the Local Store Syslog Message Format. The remote syslog server targets are identified by the facility code names LOCAL0 to LOCAL7 (LOCAL6 is the default logging location.) Log messages that you assign to the remote syslog server are sent to the default location for Linux syslog (/var/log/messages), however; you can configure a different location on the server.



CHAPTER 2

List of Cisco ISE Syslogs

This document contains the syslogs generated in all Cisco ISE releases.

- List of Cisco ISE Syslogs, on page 6
- ACI Binding, on page 32
- AD Connector, on page 34
- Administrative and Operational Audit, on page 55
- Administrator Authentication and Authorization, on page 226
- Authentication Flow Diagnostics, on page 230
- Distributed Management, on page 250
- External MDM, on page 266
- Failed Attempts, on page 268
- Guest, on page 278
- Identity Stores Diagnostics, on page 286
- Internal MDM, on page 412
- Internal Operations Diagnostics, on page 422
- IPsec, on page 464
- Licensing, on page 465
- MDM Diagnostics, on page 479
- My Devices, on page 486
- Passed Authentications, on page 490
- Passive ID, on page 495
- Policy Diagnostics, on page 523
- Posture And Client Provisioning Audit, on page 539
- Posture And Client Provisioning Diagnostics, on page 546
- Profiler, on page 548
- RADIUS Accounting, on page 552
- RADIUS Diagnostics, on page 555
- System Statistics, on page 772
- TACACS Accounting, on page 774
- TACACS Diagnostics, on page 775
- Threat Centric NAC, on page 797

List of Cisco ISE Syslogs

The following sections include a comprehensive list of syslogs generated, what each of them means, and the format of the message in local and remote logging targets.

Cisco ISE Release 3.5: New System Messages

Category Name	Message Codes
AD Connector	25118
	25119
Administrative and Operational Audit	60477
	60478
	60479
	62018
	62019
	62020
	62021
	62022
	64011
	64013
Identity Stores Diagnostics	24910
	24911
	24912
	24913
	24914
	24915
	24916
	24917
	24918
	24919
	24920
	24921
	24922
Policy Diagnostics	15509

Category Name	Message Codes
Posture and Client Provisioning Audit	87007
	87008
Profiler	80020
TACACS Diagnostics	13079
	13080
	13081
	13082
	13083
	13084
	13085
	13086
	13087
	13088
	13089
	13090
	13091
	13092
	13093
	13094
	13095
	13096
	13097
	13098
	13099
	13100
	13101
	13102
	13103
	13104

Cisco ISE Release 3.5: Deleted System Messages

Category Name	Message Codes
RADIUS Diagnostics	13102
	13082
	13089
	13086
	13093
	13097
	13088
	13101
	13081
	13092
	13085
	13096
	13091
	13100
	11643
	13080
	13095
	13104
	13084
	13099
	13079
	13090
	13103
	13083
	13094
	13087
	13098

Cisco ISE Release 3.4: New System Messages

Category Name	Message Codes
AD Connector	25059
	25060
	25061
Administrative and Operational Audit	58046
	58047
	61304
	61305
	63001
	63002
	63003
	63004
	63005
	63006
	63007
	63008
	64010
	64012
Authentication Flow Diagnostics	22075
	22076
	22077
	22078
Failed Attempts	5453
Internal Operations Diagnostics	31505
	31506
	34165
	34166
	34167

Category Name	Message Codes
IPSec	93001
	93002
	93003
	93004
	93005
	93006
	93007
Passed Authentications	5207
	5208
Policy Diagnostics	15057
	15507
	15508

Category Name	Message Codes
RADIUS Diagnostics	11058
	11059
	11118
	11639
	11640
	11641
	11642
	11643
	11644
	11645
	12237
	12238
	12239
	12240
	12573
	12763
	12764
	12765
	12766
	12767
	12768
	12769
	12770
	12771
	12772
	12773
	12774
	12775
	12776
	12777
	12820
	12858

Category Name	Message Codes
	12859
	12860
	12861
	12862
	12863
	12864
	12865
	12866
	12867
	12868
	12869
	12870
	12871
	12872
	12902
	12903
	12904
	12905
	12906
	12907
	12908
	12909
	12910
	12911
	12912
	12913
	13079
	13080
	13081
	13082
	13083
	13084

Category Name	Message Codes
	13085
	13086
	13087
	13088
	13089
	13090
	13091
	13092
	13093
	13094
	13095
	13096
	13097
	13098
	13099
	13100
	13101
	13102
	13103
	13104

Cisco ISE Release 3.4: Deleted System Messages

Category Name	Message Codes
Administrative and Operational Audit	61025
	61026

Cisco ISE Release 3.3: New System Messages

Category Name	Message Codes

Administrative and Operational Audit	61083
	60469
	60472
	61092
	61084
	60470
	61088
	61085
	61089
	61086
	61090
	61087
	61091
Policy Diagnostics	15504
	15506
	15503
	15505
Identity Stores Diagnostics	24045
	24046
	24047

Cisco ISE Release 3.3: Deleted System Messages

No system messages were deleted in this release.

Cisco ISE Release 3.2: New System Messages

Category Name	Message Codes
Administrative and Operational Audit	60467 60468 60466 61081 61082 62007 62008 62009 62010 62011 62012 62013 62014 62015 62016 62017 80017 80018 80019 90503 90506 62006 61303
Profiler	80017 80018 80019
PassiveID	90503 90506

Category Name	Message Codes
RADIUS Diagnostics	11700 11701 11702 11703 11704 11705 11706 11707 11708 11709 11710 11711 11712 11713 11714 11715 11716 11717 11724 11725 11726 11721 11722 11718 11719 11720
Identity Stores Diagnostics	24797 24798 24799

Cisco ISE Release 3.2: Deleted System Messages

No system messages were deleted in this release.

Cisco ISE Release 3.1: New System Messages

Category Name	Message Codes
AD Connector	25113 25114 25115 25116 25117
Administrative and Operational Audit	61080 61238 61239 61240 61241 61242 61243 61244 61245 61237 61246 61300 61301 61302
Internal Operations Diagnostics	34170

Category Name	Message Codes
Licensing	35042 35043 35044 35045 35046 35047 35048 35049 35050 35051 35052 35053 35054 35055
PassiveID	90504 90505
Posture and Client Provisioning Audit	87005 87006

Cisco ISE Release 3.1: Deleted System Messages

No system messages were deleted in this release.

Cisco ISE Release 3.0: New System Messages

Category Name	Message Codes
ACI Binding	92001 92002 92003 92004 92005 92006

Category Name	Message Codes
AD Connector	25100 25101 25102 25103 25104 25105 25106 25107 25108 25109 25110 25111 25112

Category Name	Message Codes
Administrative and Operational Audit	

Category Name	Message Codes
	51025 61076 61077 61078 61079 61100 61101 61102 61103 61104 61105 61106 61107 61108 61109 61110 61111 61112 61113 61114 61115 61116 61117 61118 61119 61120 61121 61122 61123 61124 61125 61126

Category Name	Message Codes
	61127 61128 61129 61130 61131 61132 61133 61134 61135 61136 61137 61138 61139 61140 61141 61142 61143 61144 61145 61146 61147 61148 61149 61150 61151 61152 61153 61154 61156 61157 61158 61159

Category Name	Message Codes
	61160 61161 61162 61163 61164 61165 61166 61167 61168 61169 61170 61171 61172 61173 61174 61175 61176 61177 61178 61179 61180 61181 61182 61183 61184 61185 61186 61187 61188 61189 61190 61191

Category Name	Message Codes
	61192 61193 61194 61195 61196 61197 61198 61199 61200 61201 61202 61203 61204 61205 61206 61207 61208 61209 61210 61211 61212 61213 61214 61215 61216 61217 61218 61219 61220 61221 61222 61223

Category Name	Message Codes
	61224 61225 61226 61227 61228 61229 61230 61231 61232 61233 61234 61235 61236 62000 62001 62002 62003
Posture and Client Provisioning Audit	87901 87921

Cisco ISE Release 3.0: Deleted System Messages

Category Name	Message Codes
Administrative and Operational Audit	51106

Cisco ISE Release 2.7: New System Messages

Category Name	Message Codes
Administrative and Operational Audit	61059 61060 61061 61062 61063 61064 61065 61066 61067 61068 61069 61070 61071 61072 61073 61074 61075
Internal Operations Diagnostics	33511 33512 33513 33514 33515 33516 33517 33518

Category Name	Message Codes
RADIUS Diagnostics	

Category Name	Message Codes
	11525
	11526
	11527
	11528
	11529
	11530
	11531
	11532
	11533
	11534
	11535
	11536
	11537
	11538
	11539
	11540
	11541
	11542
	11543
	11544
	11545
	11546
	11547
	11548
	11549
	11550
	11551
	11552
	11553
	11554
	11555
	11556

Category Name	Message Codes
	11557
	11558
	11559
	11560
	11561
	11562
	11563
	11564
	11565
	11566
	11567
	11568
	11569
	11570
	11571
	11572
	11573
	11574
	11575
	11576
	11577
	11578
	11579
	11580
	11581
	11582
	11583
	11584
	11585
	11586
	11587
	11588

Category Name	Message Codes
	11589
	11590
	11591
	11592
	11593
	11594
	11595
	11596
	11597
	11598
	11599
	11600
	11601
	11602
	11603
	11604
	11605
	11606
	11607
	11608
	11609
	11610
	11611
	11612
	11613
	11614
	11615
	11616
	11617
	11618
	11619
	11620

Category Name	Message Codes
	11621 11622 11623 11624 11625 11626 11627 11628 11629 11630 11631 11632 11633 11634 11635 11636 11637 11638 12756 12757 12758 12759 12760 12761 12762 12920 12921 12928

Cisco ISE Release 2.7: Deleted System Messages

No system messages were deleted in this release.

Cisco ISE Release 2.6: New System Messages

Category Name	Message Codes
RADIUS Diagnostics	12968
Administrative and Operational Audit	61054 61055 61056 61057 61058

Cisco ISE Release 2.6: Deleted System Messages

No system messages were deleted in this release.

ACI Binding

- **Message Code:** 92001

  Severity: INFO

  Message Text: ACI binding created

  Message Description: Got ACI binding create message

  Local Target Message Format: <timestamp> <seq_num>92001 INFO TrustSec ACI binding created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>92001 INFO TrustSec ACI binding created, <log details>

- **Message Code:** 92002

  Severity: INFO

  Message Text: ACI binding updated

  Message Description: Got ACI binding update message

  Local Target Message Format: <timestamp> <seq_num>92002 INFO TrustSec ACI binding updated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>92002 INFO TrustSec ACI binding updated, <log details>

- **Message Code:** 92003

  Severity: INFO

Message Text: ACI binding deleted

Message Description: Got ACI binding delete message

Local Target Message Format: <timestamp> <seq_num>92003 INFO TrustSec ACI binding deleted, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>92003 INFO TrustSec ACI binding deleted, <log details>

- **Message Code:** 92004

  Severity: INFO

  Message Text: ISE informed ACI about binding created

  Message Description: ISE informed ACI about binding created

  Local Target Message Format: <timestamp> <seq_num>92004 INFO TrustSec ISE informed ACI about binding created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>92004 INFO TrustSec ISE informed ACI about binding created, <log details>

- **Message Code:** 92005

  Severity: INFO

  Message Text: ISE informed ACI about binding updated

  Message Description: ISE informed ACI about binding updated

  Local Target Message Format: <timestamp> <seq_num>92005 INFO TrustSec ISE informed ACI about binding updated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>92005 INFO TrustSec ISE informed ACI about binding updated, <log details>

- **Message Code:** 92006

  Severity: INFO

  Message Text: ISE informed ACI about binding deleted

  Message Description: ISE informed ACI about binding deleted

  Local Target Message Format: <timestamp> <seq_num>92006 INFO TrustSec ISE informed ACI about binding deleted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>92006 INFO TrustSec ISE informed ACI about binding deleted, <log details>

AD Connector

- **Message Code:** 25000

  Severity: INFO

  Message Text: ISE server password update succeeded

  Message Description: ISE server password update succeeded

  Local Target Message Format: <timestamp> <seq_num> 25000 INFO AD-Connector: ISE server password update succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25000 INFO AD-Connector: ISE server password update succeeded, <log details>

- **Message Code:** 25001

  Severity: ERROR

  Message Text: AD: ISE account password update failed.

  Message Description: ISE server has failed to update its AD machine account password.

  Local Target Message Format: <timestamp> <seq_num> 25001 ERROR AD-Connector: AD: ISE account password update failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25001 ERROR AD-Connector: AD: ISE account password update failed., <log details>

- **Message Code:** 25002

  Severity: INFO

  Message Text: ISE server TGT refresh succeeded

  Message Description: ISE server TGT refresh succeeded

  Local Target Message Format: <timestamp> <seq_num> 25002 INFO AD-Connector: ISE server TGT refresh succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25002 INFO AD-Connector: ISE server TGT refresh succeeded, <log details>

- **Message Code:** 25003

  Severity: ERROR

  Message Text: AD: Machine TGT refresh failed.

  Message Description: ISE server TGT (Ticket Granting Ticket) refresh has failed; it is used for AD connectivity and services.

  Local Target Message Format: <timestamp> <seq_num> 25003 ERROR AD-Connector: AD: Machine TGT refresh failed., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25003 ERROR AD-Connector: AD: Machine TGT refresh failed., <log details>

- **Message Code:** 25004

  Severity: INFO

  Message Text: AD Connector started

  Message Description: AD Connector started

  Local Target Message Format: <timestamp> <seq_num> 25004 INFO AD-Connector: AD Connector started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25004 INFO AD-Connector: AD Connector started, <log details>

- **Message Code:** 25005

  Severity: INFO

  Message Text: AD Connector stopped

  Message Description: AD Connector stopped

  Local Target Message Format: <timestamp> <seq_num> 25005 INFO AD-Connector: AD Connector stopped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25005 INFO AD-Connector: AD Connector stopped, <log details>

- **Message Code:** 25006

  Severity: WARN

  Message Text: AD Connector had to be restarted.

  Message Description: AD Connector had to be automatically restarted as it stopped unexpectedly.

  Local Target Message Format: <timestamp> <seq_num> 25006 WARN AD-Connector: AD Connector had to be restarted., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25006 WARN AD-Connector: AD Connector had to be restarted., <log details>

- **Message Code:** 25007

  Severity: INFO

  Message Text: Join point connector started

  Message Description: Join point connector started

  Local Target Message Format: <timestamp> <seq_num> 25007 INFO AD-Connector: Join point connector started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25007 INFO AD-Connector: Join point connector started, <log details>

- **Message Code:** 25008

  Severity: INFO

  Message Text: Join point connector stopped

  Message Description: Join point connector stopped

  Local Target Message Format: <timestamp> <seq_num> 25008 INFO AD-Connector: Join point connector stopped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25008 INFO AD-Connector: Join point connector stopped, <log details>

- **Message Code:** 25009

  Severity: INFO

  Message Text: Trusted domains discovery succeeded

  Message Description: Trusted domains discovery succeeded

  Local Target Message Format: <timestamp> <seq_num> 25009 INFO AD-Connector: Trusted domains discovery succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25009 INFO AD-Connector: Trusted domains discovery succeeded, <log details>

- **Message Code:** 25010

  Severity: ERROR

  Message Text: Trusted domains discovery failed

  Message Description: Trusted domains discovery failed

  Local Target Message Format: <timestamp> <seq_num> 25010 ERROR AD-Connector: Trusted domains discovery failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25010 ERROR AD-Connector: Trusted domains discovery failed, <log details>

- **Message Code:** 25011

  Severity: INFO

  Message Text: Domain join succeeded

  Message Description: Domain join succeeded

  Local Target Message Format: <timestamp> <seq_num> 25011 INFO AD-Connector: Domain join succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25011 INFO AD-Connector: Domain join succeeded, <log details>

- **Message Code:** 25012

  Severity: WARN

  Message Text: Domain join failed

  Message Description: Domain join failed

  Local Target Message Format: <timestamp> <seq_num> 25012 WARN AD-Connector: Domain join failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25012 WARN AD-Connector: Domain join failed, <log details>

- **Message Code:** 25013

  Severity: INFO

  Message Text: Domain leave succeeded

  Message Description: Domain leave succeeded

  Local Target Message Format: <timestamp> <seq_num> 25013 INFO AD-Connector: Domain leave succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25013 INFO AD-Connector: Domain leave succeeded, <log details>

- **Message Code:** 25014

  Severity: WARN

  Message Text: Domain leave failed

  Message Description: Domain leave failed

  Local Target Message Format: <timestamp> <seq_num> 25014 WARN AD-Connector: Domain leave failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25014 WARN AD-Connector: Domain leave failed, <log details>

- **Message Code:** 25015

  Severity: INFO

  Message Text: DNS SRV query succeeded

  Message Description: DNS SRV query succeeded

  Local Target Message Format: <timestamp> <seq_num> 25015 INFO AD-Connector: DNS SRV query succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25015 INFO AD-Connector: DNS SRV query succeeded, <log details>

- **Message Code:** 25016

  Severity: ERROR

  Message Text: DNS SRV query failed

  Message Description: DNS SRV query failed

  Local Target Message Format: <timestamp> <seq_num> 25016 ERROR AD-Connector: DNS SRV query failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25016 ERROR AD-Connector: DNS SRV query failed, <log details>

- **Message Code:** 25017

  Severity: INFO

  Message Text: DC discovery succeeded

  Message Description: DC discovery succeeded

  Local Target Message Format: <timestamp> <seq_num> 25017 INFO AD-Connector: DC discovery succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25017 INFO AD-Connector: DC discovery succeeded, <log details>

- **Message Code:** 25018

  Severity: ERROR

  Message Text: DC discovery failed

  Message Description: DC discovery failed

  Local Target Message Format: <timestamp> <seq_num> 25018 ERROR AD-Connector: DC discovery failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25018 ERROR AD-Connector: DC discovery failed, <log details>

- **Message Code:** 25019

  Severity: INFO

  Message Text: KDC discovery succeeded

  Message Description: KDC discovery succeeded

  Local Target Message Format: <timestamp> <seq_num> 25019 INFO AD-Connector: KDC discovery succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25019 INFO AD-Connector: KDC discovery succeeded, <log details>

- **Message Code:** 25020

  Severity: ERROR

  Message Text: KDC discovery failed

  Message Description: KDC discovery failed

  Local Target Message Format: <timestamp> <seq_num> 25020 ERROR AD-Connector: KDC discovery failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25020 ERROR AD-Connector: KDC discovery failed, <log details>

- **Message Code:** 25021

  Severity: INFO

  Message Text: GC discovery succeeded

  Message Description: GC discovery succeeded

  Local Target Message Format: <timestamp> <seq_num> 25021 INFO AD-Connector: GC discovery succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25021 INFO AD-Connector: GC discovery succeeded, <log details>

- **Message Code:** 25022

  Severity: ERROR

  Message Text: GC discovery failed

  Message Description: GC discovery failed

  Local Target Message Format: <timestamp> <seq_num> 25022 ERROR AD-Connector: GC discovery failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25022 ERROR AD-Connector: GC discovery failed, <log details>

- **Message Code:** 25023

  Severity: INFO

  Message Text: LDAP connect to domain controller succeeded

  Message Description: LDAP connect to domain controller succeeded

  Local Target Message Format: <timestamp> <seq_num> 25023 INFO AD-Connector: LDAP connect to domain controller succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25023 INFO AD-Connector: LDAP connect to domain controller succeeded, <log details>

- **Message Code:** 25024

  Severity: ERROR

  Message Text: LDAP connect to domain controller failed

  Message Description: LDAP connect to domain controller failed

  Local Target Message Format: <timestamp> <seq_num> 25024 ERROR AD-Connector: LDAP connect to domain controller failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25024 ERROR AD-Connector: LDAP connect to domain controller failed, <log details>

- **Message Code:** 25025

  Severity: INFO

  Message Text: LDAP connect to global catalog succeeded

  Message Description: LDAP connect to domain controller succeeded

  Local Target Message Format: <timestamp> <seq_num> 25025 INFO AD-Connector: LDAP connect to global catalog succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25025 INFO AD-Connector: LDAP connect to global catalog succeeded, <log details>

- **Message Code:** 25026

  Severity: ERROR

  Message Text: LDAP connect to global catalog failed

  Message Description: LDAP connect to domain controller failed

  Local Target Message Format: <timestamp> <seq_num> 25026 ERROR AD-Connector: LDAP connect to global catalog failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25026 ERROR AD-Connector: LDAP connect to global catalog failed, <log details>

- **Message Code:** 25027

  Severity: INFO

  Message Text: RPC connect to domain controller succeeded

  Message Description: RPC connect to domain controller succeeded

  Local Target Message Format: <timestamp> <seq_num> 25027 INFO AD-Connector: RPC connect to domain controller succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25027 INFO AD-Connector: RPC connect to domain controller succeeded, <log details>

- **Message Code:** 25028

  Severity: ERROR

  Message Text: RPC connect to domain controller failed

  Message Description: RPC connect to domain controller failed

  Local Target Message Format: <timestamp> <seq_num> 25028 ERROR AD-Connector: RPC connect to domain controller failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25028 ERROR AD-Connector: RPC connect to domain controller failed, <log details>

- **Message Code:** 25029

  Severity: INFO

  Message Text: KDC connect to domain controller succeeded

  Message Description: KDC connect to domain controller succeeded

  Local Target Message Format: <timestamp> <seq_num> 25029 INFO AD-Connector: KDC connect to domain controller succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25029 INFO AD-Connector: KDC connect to domain controller succeeded, <log details>

- **Message Code:** 25030

  Severity: ERROR

  Message Text: KDC connect to domain controller failed

  Message Description: KDC connect to domain controller failed

  Local Target Message Format: <timestamp> <seq_num> 25030 ERROR AD-Connector: KDC connect to domain controller failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25030 ERROR AD-Connector: KDC connect to domain controller failed, <log details>

- **Message Code:** 25031

  Severity: ERROR

  Message Text: AD Provider failed to start

  Message Description: AD Provider failed to start

  Local Target Message Format: <timestamp> <seq_num> 25031 ERROR AD-Connector: AD Provider failed to start, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25031 ERROR AD-Connector: AD Provider failed to start, <log details>

- **Message Code:** 25032

  Severity: INFO

  Message Text: Trusted domain discovered

  Message Description: Trusted domain discovered

  Local Target Message Format: <timestamp> <seq_num> 25032 INFO AD-Connector: Trusted domain discovered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25032 INFO AD-Connector: Trusted domain discovered, <log details>

- **Message Code:** 25033

  Severity: INFO

  Message Text: DNS A/AAAA query succeeded

  Message Description: DNS A/AAAA query succeeded

  Local Target Message Format: <timestamp> <seq_num> 25033 INFO AD-Connector: DNS A/AAAA query succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25033 INFO AD-Connector: DNS A/AAAA query succeeded, <log details>

- **Message Code:** 25034

  Severity: ERROR

  Message Text: DNS A/AAAA query failed

  Message Description: DNS A/AAAA query failed

  Local Target Message Format: <timestamp> <seq_num> 25034 ERROR AD-Connector: DNS A/AAAA query failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25034 ERROR AD-Connector: DNS A/AAAA query failed, <log details>

- **Message Code:** 25035

  Severity: INFO

  Message Text: Writeable DC discovery succeeded

  Message Description: Writeable DC discovery succeeded

  Local Target Message Format: <timestamp> <seq_num> 25035 INFO AD-Connector: Writeable DC discovery succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25035 INFO AD-Connector: Writeable DC discovery succeeded, <log details>

- **Message Code:** 25036

  Severity: ERROR

  Message Text: Writeable DC discovery failed

  Message Description: Writeable DC discovery failed

  Local Target Message Format: <timestamp> <seq_num> 25036 ERROR AD-Connector: Writeable DC discovery failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25036 ERROR AD-Connector: Writeable DC discovery failed, <log details>

- **Message Code:** 25037

  Severity: INFO

  Message Text: DC record cached

  Message Description: DC record cached

  Local Target Message Format: <timestamp> <seq_num> 25037 INFO AD-Connector: DC record cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25037 INFO AD-Connector: DC record cached, <log details>

- **Message Code:** 25038

  Severity: INFO

  Message Text: GC record cached

  Message Description: GC record cached

  Local Target Message Format: <timestamp> <seq_num> 25038 INFO AD-Connector: GC record cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25038 INFO AD-Connector: GC record cached, <log details>

- **Message Code:** 25039

  Severity: ERROR

  Message Text: LDAP SASL bind failed

  Message Description: LDAP SASL bind failed

  Local Target Message Format: <timestamp> <seq_num> 25039 ERROR AD-Connector: LDAP SASL bind failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25039 ERROR AD-Connector: LDAP SASL bind failed, <log details>

- **Message Code:** 25040

  Severity: ERROR

  Message Text: RPC secure channel establishment failed

  Message Description: RPC secure channel establishment failed

  Local Target Message Format: <timestamp> <seq_num> 25040 ERROR AD-Connector: RPC secure channel establishment failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25040 ERROR AD-Connector: RPC secure channel establishment failed, <log details>

- **Message Code:** 25041

  Severity: INFO

  Message Text: ISE Server site discovered

  Message Description: ISE Server site discovered

  Local Target Message Format: <timestamp> <seq_num> 25041 INFO AD-Connector: ISE Server site discovered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25041 INFO AD-Connector: ISE Server site discovered, <log details>

- **Message Code:** 25042

  Severity: WARN

  Message Text: ISE Server is not assigned to any AD site

  Message Description: ISE Server is not assigned to any AD site

  Local Target Message Format: <timestamp> <seq_num> 25042 WARN AD-Connector: ISE Server is not assigned to any AD site, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25042 WARN AD-Connector: ISE Server is not assigned to any AD site, <log details>

- **Message Code:** 25043

  Severity: WARN

  Message Text: No domain controller found in ISE Server site

  Message Description: No domain controller found in ISE Server site

  Local Target Message Format: <timestamp> <seq_num> 25043 WARN AD-Connector: No domain controller found in ISE Server site, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25043 WARN AD-Connector: No domain controller found in ISE Server site, <log details>

- **Message Code:** 25044

  Severity: ERROR

  Message Text: Communication to domain failed

  Message Description: Communication to domain failed

  Local Target Message Format: <timestamp> <seq_num> 25044 ERROR AD-Connector: Communication to domain failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25044 ERROR AD-Connector: Communication to domain failed, <log details>

- **Message Code:** 25045

  Severity: ERROR

  Message Text: Configured nameserver is down

  Message Description: The configured nameserver is down. As a result AD operations will fail.

  Local Target Message Format: <timestamp> <seq_num> 25045 ERROR AD-Connector: Configured nameserver is down, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25045 ERROR AD-Connector: Configured nameserver is down, <log details>

- **Message Code:** 25046

  Severity: ERROR

  Message Text: Joined domain is unavailable

  Message Description: Joined domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval

  Local Target Message Format: <timestamp> <seq_num> 25046 ERROR AD-Connector: Joined domain is unavailable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25046 ERROR AD-Connector: Joined domain is unavailable, <log details>

- **Message Code:** 25047

  Severity: ERROR

  Message Text: Authentication domain is unavailable

  Message Description: Authentication domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval

  Local Target Message Format: <timestamp> <seq_num> 25047 ERROR AD-Connector: Authentication domain is unavailable, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25047 ERROR AD-Connector: Authentication domain is unavailable, <log details>

- **Message Code:** 25048

  Severity: ERROR

  Message Text: Active-Directory forest is unavailable

  Message Description: Active Directory forest GC (Global Catalog) is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval

  Local Target Message Format: <timestamp> <seq_num> 25048 ERROR AD-Connector: Active-Directory forest is unavailable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25048 ERROR AD-Connector: Active-Directory forest is unavailable, <log details>

- **Message Code:** 25049

  Severity: WARN

  Message Text: Machine account was not found

  Message Description: Machine account was not found during leave opeartion with credentials.

  Local Target Message Format: <timestamp> <seq_num> 25049 WARN AD-Connector: Machine account was not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25049 WARN AD-Connector: Machine account was not found, <log details>

- **Message Code:** 25050

  Severity: INFO

  Message Text: Machine account was deleted from AD

  Message Description: Machine account was deleted from AD

  Local Target Message Format: <timestamp> <seq_num> 25050 INFO AD-Connector: Machine account was deleted from AD, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25050 INFO AD-Connector: Machine account was deleted from AD, <log details>

- **Message Code:** 25051

  Severity: ERROR

  Message Text: Machine account deletion was failed

  Message Description: User credentials permissions is insufficient to delete the machine account

  Local Target Message Format: <timestamp> <seq_num> 25051 ERROR AD-Connector: Machine account deletion was failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25051 ERROR AD-Connector: Machine account deletion was failed, <log details>

- **Message Code:** 25052

  Severity: INFO

  Message Text: Periodic trusts discovery started

  Message Description: Periodic trusts discovery started

  Local Target Message Format: <timestamp> <seq_num> 25052 INFO AD-Connector: Periodic trusts discovery started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25052 INFO AD-Connector: Periodic trusts discovery started, <log details>

- **Message Code:** 25053

  Severity: INFO

  Message Text: Detected offline forest

  Message Description: Detected offline forest

  Local Target Message Format: <timestamp> <seq_num> 25053 INFO AD-Connector: Detected offline forest, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25053 INFO AD-Connector: Detected offline forest, <log details>

- **Message Code:** 25054

  Severity: INFO

  Message Text: Trust removed by discovery

  Message Description: Trust removed bt discovery

  Local Target Message Format: <timestamp> <seq_num> 25054 INFO AD-Connector: Trust removed by discovery, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25054 INFO AD-Connector: Trust removed by discovery, <log details>

- **Message Code:** 25055

  Severity: INFO

  Message Text: DC added to black list

  Message Description: Domain Controller added to black list

  Local Target Message Format: <timestamp> <seq_num> 25055 INFO AD-Connector: DC added to black list, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25055 INFO AD-Connector: DC added to black list, <log details>

- **Message Code:** 25056

  Severity: INFO

  Message Text: DC removed from black list

  Message Description: Domain Controller removed from black list

  Local Target Message Format: <timestamp> <seq_num> 25056 INFO AD-Connector: DC removed from black list, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25056 INFO AD-Connector: DC removed from black list, <log details>

- **Message Code:** 25057

  Severity: ERROR

  Message Text: The ISE machine account does not have the required privileges to fetch groups.

  Message Description: The ISE machine account does not have the required privileges to fetch groups.

  Local Target Message Format: <timestamp> <seq_num> 25057 ERROR AD-Connector: The ISE machine account does not have the required privileges to fetch groups., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25057 ERROR AD-Connector: The ISE machine account does not have the required privileges to fetch groups., <log details>

- **Message Code:** 25058

  Severity: ERROR

  Message Text: ISE is not joined to an Active Directory Domain Controller

  Message Description: ISE is not joined to an Active Directory Domain Controller

  Local Target Message Format: <timestamp> <seq_num> 25058 ERROR AD-Connector: ISE is not joined to an Active Directory Domain Controller, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 25058 ERROR AD-Connector: ISE is not joined to an Active Directory Domain Controller, <log details>

- **Message Code:** 25059

  Severity: WARN

  Message Text: Domain Controller services are unavailable

  Message Description: Domain Controller services are unavailable

  Local Target Message Format: <timestamp> <seq_num>AD-Connector Domain Controller services are unavailable WARN Domain Controller services are unavailable, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>AD-Connector Domain Controller services are unavailable WARN Domain Controller services are unavailable, <log details>

- **Message Code:** 25060

  Severity: INFO

  Message Text: Domain Controller was skipped - Unstable

  Message Description: Domain Controller was skipped - Unstable

  Local Target Message Format: <timestamp> <seq_num>AD-Connector Domain Controller was skipped - Unstable INFO Domain Controller was skipped - Unstable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>AD-Connector Domain Controller was skipped - Unstable INFO Domain Controller was skipped - Unstable, <log details>

- **Message Code:** 25061

  Severity: INFO

  Message Text: Domain Controller lookup failed - Name or service not known

  Message Description: Domain Controller lookup failed - Name or service not known

  Local Target Message Format: <timestamp> <seq_num>AD-Connector Domain Controller lookup failed - Name or service not known INFO Domain Controller lookup failed - Name or service not known, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>AD-Connector Domain Controller lookup failed - Name or service not known INFO Domain Controller lookup failed - Name or service not known, <log details>

- **Message Code:** 25100

  Severity: DEBUG

  Message Text: Connecting to external REST ID store server

  Message Description: ISE is going to establish a new connection to external REST ID store server

  Local Target Message Format: <timestamp> <seq_num>25100 DEBUG External-REST Connecting to external REST ID store server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25100 DEBUG External-REST Connecting to external REST ID store server, <log details>

- **Message Code:** 25101

  Severity: DEBUG

  Message Text: Successfully connected to external REST ID store server

  Message Description: ISE successfully connect to external REST ID store server

  Local Target Message Format: <timestamp> <seq_num>25101 DEBUG External-REST Successfully connected to external REST ID store server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25101 DEBUG External-REST Successfully connected to external REST ID store server, <log details>

- **Message Code:** 25102

  Severity: DEBUG

  Message Text: Connection to external REST database failed

  Message Description: ISE failed to establish a new connection to external REST database

  Local Target Message Format: <timestamp> <seq_num>25102 DEBUG External-REST Connection to external REST database failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25102 DEBUG External-REST Connection to external REST database failed, <log details>

- **Message Code:** 25103

  Severity: DEBUG

  Message Text: Perform plain text password authentication in external REST ID store server

  Message Description: ISE is starting plain text password authentication against the external REST ID store server

  Local Target Message Format: <timestamp> <seq_num>25103 DEBUG External-REST Perform plain text password authentication in external REST ID store server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25103 DEBUG External-REST Perform plain text password authentication in external REST ID store server, <log details>

- **Message Code:** 25104

  Severity: DEBUG

  Message Text: Plain text password authentication in external REST ID store server succeeded

  Message Description: Plain text password authentication in external REST ID store server succeeded

  Local Target Message Format: <timestamp> <seq_num>25104 DEBUG External-REST Plain text password authentication in external REST ID store server succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25104 DEBUG External-REST Plain text password authentication in external REST ID store server succeeded, <log details>

- **Message Code:** 25105

  Severity: DEBUG

  Message Text: Plain text password authentication in external REST ID store server failed

  Message Description: Plain text password authentication in external REST ID store server failed

  Local Target Message Format: <timestamp> <seq_num>25105 DEBUG External-REST Plain text password authentication in external REST ID store server failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25105 DEBUG External-REST Plain text password authentication in external REST ID store server failed, <log details>

- **Message Code:** 25106

  Severity: DEBUG

  Message Text: REST ID Store server indicated plain text password authentication failure

  Message Description: REST ID store server indicated plain text password authentication failure

  Local Target Message Format: <timestamp> <seq_num>25106 DEBUG External-REST REST ID Store server indicated plain text password authentication failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25106 DEBUG External-REST REST ID Store server indicated plain text password authentication failure, <log details>

- **Message Code:** 25107

  Severity: DEBUG

  Message Text: REST ID store server respond with groups

  Message Description: REST ID store server respond with groups in authentication as part of authentication

  Local Target Message Format: <timestamp> <seq_num>25107 DEBUG External-REST REST ID store server respond with groups, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25107 DEBUG External-REST REST ID store server respond with groups, <log details>

- **Message Code:** 25108

  Severity: DEBUG

  Message Text: REST ID store server does not include any user groups

  Message Description: REST ID store server does not include any user groups as part of authentication response

  Local Target Message Format: <timestamp> <seq_num>25108 DEBUG External-REST REST ID store server does not include any user groups, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25108 DEBUG External-REST REST ID store server does not include any user groups, <log details>

- **Message Code:** 25109

  Severity: DEBUG

  Message Text: ISE starts set user groups in session cache

  Message Description: ISE starts set user groups in session cache to be used later in authorization process

  Local Target Message Format: <timestamp> <seq_num>25109 DEBUG External-REST ISE starts set user groups in session cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25109 DEBUG External-REST ISE starts set user groups in session cache, <log details>

- **Message Code:** 25110

  Severity: DEBUG

  Message Text: User groups inserted to session cache

  Message Description: ISE succeed to set user groups for current session in cache

  Local Target Message Format: <timestamp> <seq_num>25110 DEBUG External-REST User groups inserted to session cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25110 DEBUG External-REST User groups inserted to session cache, <log details>

- **Message Code:** 25111

  Severity: DEBUG

  Message Text: Failed to set user groups in session cache

  Message Description: ISE failed to set user groups in session cache, groups will not be used in authorization process

  Local Target Message Format: <timestamp> <seq_num>25111 DEBUG External-REST Failed to set user groups in session cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25111 DEBUG External-REST Failed to set user groups in session cache, <log details>

- **Message Code:** 25112

  Severity: DEBUG

  Message Text: REST database indicated plain text password authentication failure

  Message Description: REST database indicated plain text password authentication failure

  Local Target Message Format: <timestamp> <seq_num>25112 DEBUG External-REST REST database indicated plain text password authentication failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25112 DEBUG External-REST REST database indicated plain text password authentication failure, <log details>

- **Message Code:** 25113

  Severity: WARN

  Message Text: Number of bad password attempts for AD instance is higher than the configuration in Active Directory, Skipping the AD authentication.

  Message Description: Number of bad password attempts for AD instance is higher than the configuration in Active Directory, Skipping the AD authentication.

Local Target Message Format: <timestamp> <seq_num>25113 WARN External-Active-Directory Number of bad password attempts for AD instance is higher than the configuration in Active Directory, Skipping the AD authentication., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25113 WARN External-Active-Directory Number of bad password attempts for AD instance is higher than the configuration in Active Directory, Skipping the AD authentication., <log details>

- **Message Code:** 25114

  Severity: INFO

  Message Text: Number of bad password attempts for AD instance is lower than the configuration in Active Directory, Continuing to AD authentication.

  Message Description: Number of bad password attempts for AD instance is lower than the configuration in Active Directory, Continuing to AD authentication.

  Local Target Message Format: <timestamp> <seq_num>25114 INFO External-Active-Directory Number of bad password attempts for AD instance is lower than the configuration in Active Directory, Continuing to AD authentication., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25114 INFO External-Active-Directory Number of bad password attempts for AD instance is lower than the configuration in Active Directory, Continuing to AD authentication., <log details>

- **Message Code:** 25115

  Severity: ERROR

  Message Text: Cannot fetch user attributes from AD instance to determine current bad password count, Continuing to AD authentication.

  Message Description: Cannot fetch user attributes from AD instance to determine current bad password count, Continuing to AD authentication.

  Local Target Message Format: <timestamp> <seq_num>25115 ERROR External-Active-Directory Cannot fetch user attributes from AD instance to determine current bad password count, Continuing to AD authentication., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25115 ERROR External-Active-Directory Cannot fetch user attributes from AD instance to determine current bad password count, Continuing to AD authentication., <log details>

- **Message Code:** 25116

  Severity: ERROR

  Message Text: Cannot determine current bad password count, no Bad-Pwd-Count attribute in AD instance, Continuing to AD authentication.

  Message Description: Cannot determine current bad password count, no Bad-Pwd-Count attribute in AD instance, Continuing to AD authentication.

Local Target Message Format: <timestamp> <seq_num>25116 ERROR External-Active-Directory Cannot determine current bad password count, no Bad-Pwd-Count attribute in AD instance, Continuing to AD authentication., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25116 ERROR External-Active-Directory Cannot determine current bad password count, no Bad-Pwd-Count attribute in AD instance, Continuing to AD authentication., <log details>

- **Message Code:** 25117

  Severity: WARN

  Message Text: Prevent AD account lockout due to too many bad password attempts feature does not work when AD is part of ID Sequence or in a Scope Mode.

  Message Description: Prevent AD account lockout due to too many bad password attempts feature does not work when AD is part of ID Sequence or in a Scope Mode.

  Local Target Message Format: <timestamp> <seq_num>25117 WARN External-Active-Directory Prevent AD account lockout due to too many bad password attempts feature does not work when AD is part of ID Sequence or in a Scope Mode., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25117 WARN External-Active-Directory Prevent AD account lockout due to too many bad password attempts feature does not work when AD is part of ID Sequence or in a Scope Mode., <log details>

- **Message Code:** 25118

  Severity: DEBUG

  Message Text: Entra ID Device Certificate Identification Pattern is not matched

  Message Description: Entra ID Device Certificate Identification Pattern is not matched

  Local Target Message Format: <timestamp> <seq_num>25118 DEBUG External-REST Entra ID Device Certificate Identification Pattern is not matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25118 DEBUG External-REST Entra ID Device Certificate Identification Pattern is not matched, <log details>

- **Message Code:** 25119

  Severity: DEBUG

  Message Text: From the Certificate parameters, Either UPN format is not correct OR misconfigured to identify whether it is device flow or user flow

  Message Description: From the Certificate parameters, Either UPN format is not correct OR misconfigured to identify whether it is device flow or user flow

  Local Target Message Format: <timestamp> <seq_num>25119 DEBUG External-REST From the Certificate parameters, Either UPN format is not correct OR misconfigured to identify whether it is device flow or user flow, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>25119 DEBUG External-REST

From the Certificate parameters, Either UPN format is not correct OR misconfigured to identify whether it is device flow or user flow, <log details>

Administrative and Operational Audit

- **Message Code:** 51000

  Severity: NOTICE

  Message Text: Administrator authentication failed

  Message Description: Administrator authentication failed

  Local Target Message Format: <timestamp> <seq_num> 51000 NOTICE Administrator-Login: Administrator authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51000 NOTICE Administrator-Login: Administrator authentication failed, <log details>

- **Message Code:** 51001

  Severity: NOTICE

  Message Text: Administrator authentication succeeded

  Message Description: Administrator authentication succeeded

  Local Target Message Format: <timestamp> <seq_num> 51001 NOTICE Administrator-Login: Administrator authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num> <timestamp> <seq_num> 51001 NOTICE Administrator-Login: Administrator authentication succeeded, <log details>

- **Message Code:** 51002

  Severity: NOTICE

  Message Text: Administrator logged off

  Message Description: Administrator logged off

  Local Target Message Format: <timestamp> <seq_num> 51002 NOTICE Administrator-Login: Administrator logged off, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num> <timestamp> <seq_num> 51002 NOTICE Administrator-Login: Administrator logged off, <log details>

- **Message Code:** 51003

  Severity: NOTICE

  Message Text: Session Timeout

  Message Description: Administrator had a session timeout

Local Target Message Format: <timestamp> <seq_num> 51003 NOTICE Administrator-Login: Session Timeout, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num> <timestamp> <seq_num> 51003 NOTICE Administrator-Login: Session Timeout,<log details>

- **Message Code:** 51004

  Severity: NOTICE

  Message Text: Rejected administrator session from unauthorized client IP address

  Message Description: An attempt to start an administration session from an unauthorized client IP address was rejected. Check the client's administration access setting.

  Local Target Message Format: <timestamp> <seq_num> 51004 NOTICE Administrator-Login: Rejected administrator session from unauthorized client IP address, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51004 NOTICE Administrator-Login: Rejected administrator session from unauthorized client IP address, <log details>

- **Message Code:** 51005

  Severity: NOTICE

  Message Text: Administrator authentication failed. Administrator account is disabled

  Message Description: Administrator authentication failed. Administrator account is disabled.

  Local Target Message Format: <timestamp> <seq_num> 51005 NOTICE Administrator-Login: Administrator authentication failed. Administrator account is disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51005 NOTICE Administrator-Login: Administrator authentication failed. Administrator account is disabled, <log details>

- **Message Code:** 51006

  Severity: NOTICE

  Message Text: Administrator authentication failed. Account is disabled due to inactivity

  Message Description: Administrator authentication failed. Account is disabled due to inactivity.

  Local Target Message Format: <timestamp> <seq_num> 51006 NOTICE Administrator-Login: Administrator authentication failed. Account is disabled due to inactivity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51006 NOTICE Administrator-Login: Administrator authentication failed. Account is disabled due to inactivity, <log details>

- **Message Code:** 51007

  Severity: NOTICE

  Message Text: Authentication failed. Account is disabled due to password expiration

  Message Description: Authentication failed. Account is disabled due to password expiration

Local Target Message Format: <timestamp> <seq_num> 51007 NOTICE Administrator-Login: Authentication failed. Account is disabled due to password expiration, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51007 NOTICE Administrator-Login: Authentication failed. Account is disabled due to password expiration, <log details>

- **Message Code:** 51008

  Severity: NOTICE

  Message Text: Administrator authentication failed. Account is disabled due to excessive failed authentication attempts

  Message Description: Administrator authentication failed. Account is disabled due to excessive failed authentication attempts.

  Local Target Message Format: <timestamp> <seq_num> 51008 NOTICE Administrator-Login: Administrator authentication failed. Account is disabled due to excessive failed authentication attempts, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51008 NOTICE Administrator-Login: Administrator authentication failed. Account is disabled due to excessive failed authentication attempts, <log details>

- **Message Code:** 51009

  Severity: NOTICE

  Message Text: Authentication failed. ISE Runtime is not running

  Message Description: Authentication failed. ISE Runtime is not running

  Local Target Message Format: <timestamp> <seq_num> 51009 NOTICE Administrator-Login: Authentication failed. ISE Runtime is not running, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51009 NOTICE Administrator-Login: Authentication failed. ISE Runtime is not running, <log details>

- **Message Code:** 51020

  Severity: NOTICE

  Message Text: Administrator authentication failed. Login username does not exist.

  Message Description: Administrator authentication failed. Login username does not exist.

  Local Target Message Format: <timestamp> <seq_num> 51020 NOTICE Administrator-Login: Administrator authentication failed. Login username does not exist., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51020 NOTICE Administrator-Login: Administrator authentication failed. Login username does not exist., <log details>

- **Message Code:** 51021

  Severity: NOTICE

Message Text: Administrator authentication failed. Wrong password.

Message Description: Administrator authentication failed. Wrong password.

Local Target Message Format: <timestamp> <seq_num> 51021 NOTICE Administrator-Login: Administrator authentication failed. Wrong password., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51021 NOTICE Administrator-Login: Administrator authentication failed. Wrong password., <log details>

- **Message Code:** 51022

  Severity: NOTICE

  Message Text: Administrator authentication failed. System Error

  Message Description: Administrator authentication failed. System Error

  Local Target Message Format: <timestamp> <seq_num> 51022 NOTICE Administrator-Login: Administrator authentication failed. System Error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51022 NOTICE Administrator-Login: Administrator authentication failed. System Error, <log details>

- **Message Code:** 51023

  Severity: NOTICE

  Message Text: Administrator account is unlocked

  Message Description: Administrator account is unlocked

  Local Target Message Format: <timestamp> <seq_num> 51023 NOTICE Administrator-Login: Administrator account is unlocked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51023 NOTICE Administrator-Login: Administrator account is unlocked, <log details>

- **Message Code:** 51100

  Severity: NOTICE

  Message Text: Password changed successfully

  Message Description: The password has been changed successfully

  Local Target Message Format: <timestamp> <seq_num> 51100 NOTICE User change password: Password changed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51100 NOTICE User change password: Password changed successfully, <log details>

- **Message Code:** 51101

  Severity: NOTICE

  Message Text: Invalid new password. Password is too short

Message Description: Invalid new password. Password too short.

Local Target Message Format: <timestamp> <seq_num> 51101 NOTICE User change password: Invalid new password. Password is too short, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51101 NOTICE User change password: Invalid new password. Password is too short, <log details>

- **Message Code:** 51102

  Severity: NOTICE

  Message Text: Invalid new password. Too many repeating characters

  Message Description: Invalid new password. Too many repeating characters.

  Local Target Message Format: <timestamp> <seq_num> 51102 NOTICE User change password: Invalid new password. Too many repeating characters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51102 NOTICE User change password: Invalid new password. Too many repeating characters, <log details>

- **Message Code:** 51103

  Severity: NOTICE

  Message Text: Invalid new password. Missing required character type

  Message Description: Invalid new password. Missing required character type.

  Local Target Message Format: <timestamp> <seq_num> 51103 NOTICE User change password: Invalid new password. Missing required character type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51103 NOTICE User change password: Invalid new password. Missing required character type, <log details>

- **Message Code:** 51104

  Severity: NOTICE

  Message Text: Invalid new password. Contains username

  Message Description: Invalid new password. A password cannot contain a username.

  Local Target Message Format: <timestamp> <seq_num> 51104 NOTICE User change password: Invalid new password. Contains username, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51104 NOTICE User change password: Invalid new password. Contains username, <log details>

- **Message Code:** 51105

  Severity: NOTICE

  Message Text: Invalid new password. Contains reserved word

  Message Description: Invalid new password. A password cannot contain a reserved word.

Local Target Message Format: <timestamp> <seq_num> 51105 NOTICE User change password: Invalid new password. Contains reserved word, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51105 NOTICE User change password: Invalid new password. Contains reserved word, <log details>

- **Message Code:** 51106

  Severity: NOTICE

  Message Text: Authentication for web services failed

  Message Description: Authentication for web services failed.

  Local Target Message Format: <timestamp> <seq_num> 51106 NOTICE User change password: Authentication for web services failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51106 NOTICE User change password: Authentication for web services failed, <log details>

- **Message Code:** 51107

  Severity: NOTICE

  Message Text: Invalid new password

  Message Description: Invalid new password

  Local Target Message Format: <timestamp> <seq_num> 51107 NOTICE User change password: Invalid new password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51107 NOTICE User change password: Invalid new password, <log details>

- **Message Code:** 51115

  Severity: NOTICE

  Message Text: The new password is invalid. This password has been previously used.

  Message Description: The new password is invalid. This password has been previously used.

  Local Target Message Format: <timestamp> <seq_num> 51115 NOTICE User change password: The new password is invalid. This password has been previously used., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51115 NOTICE User change password: The new password is invalid. This password has been previously used., <log details>

- **Message Code:** 51116

  Severity: NOTICE

  Message Text: Invalid new password. Password must not contain dictionary words or their characters in reverse order

  Message Description: Invalid new password. Password must not contain dictionary words or their characters in reverse order

Local Target Message Format: <timestamp> <seq_num> 51116 NOTICE User change password: Invalid new password. Password must not contain dictionary words or their characters in reverse order, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 51116 NOTICE User change password: Invalid new password. Password must not contain dictionary words or their characters in reverse order, <log details>

- **Message Code:** 52000

  Severity: NOTICE

  Message Text: Added configuration

  Message Description: Added configuration

  Local Target Message Format: <timestamp> <seq_num> 52000 NOTICE Configuration-Changes: Added configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52000 NOTICE Configuration-Changes: Added configuration, <log details>

- **Message Code:** 52001

  Severity: NOTICE

  Message Text: Changed configuration

  Message Description: Changed configuration

  Local Target Message Format: <timestamp> <seq_num> 52001 NOTICE Configuration-Changes: Changed configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52001 NOTICE Configuration-Changes: Changed configuration, <log details>

- **Message Code:** 52002

  Severity: NOTICE

  Message Text: Deleted configuration

  Message Description: Deleted configuration

  Local Target Message Format: <timestamp> <seq_num> 52002 NOTICE Configuration-Changes: Deleted configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52002 NOTICE Configuration-Changes: Deleted configuration, <log details>

- **Message Code:** 52003

  Severity: NOTICE

  Message Text: Deregister Node

  Message Description: One of the ISE instances in the deployment has been de-registered.

Local Target Message Format: <timestamp> <seq_num> 52003 NOTICE Distributed-Management: Deregister Node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52003 NOTICE Distributed-Management: Deregister Node, <log details>

- **Message Code:** 52004

  Severity: NOTICE

  Message Text: Register Node

  Message Description: A new ISE instance has been registered and has joined the deployment.

  Local Target Message Format: <timestamp> <seq_num> 52004 NOTICE Distributed-Management: Register Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52004 NOTICE Distributed-Management: Register Node, <log details>

- **Message Code:** 52005

  Severity: NOTICE

  Message Text: Activate Node

  Message Description: An ISE instance has been activated to receive updates from the Primary node.

  Local Target Message Format: <timestamp> <seq_num> 52005 NOTICE Distributed-Management: Activate Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52005 NOTICE Distributed-Management: Activate Node, <log details>

- **Message Code:** 52006

  Severity: NOTICE

  Message Text: Deactivate ISE Node

  Message Description: An ISE instance has been deactivated and will no longer receive updates from the Primary node.

  Local Target Message Format: <timestamp> <seq_num> 52006 NOTICE Distributed-Management: Deactivate ISE Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52006 NOTICE Distributed-Management: Deactivate ISE Node, <log details>

- **Message Code:** 52007

  Severity: NOTICE

  Message Text: Force Full replication

  Message Description: A Force Full replication has been issued for an ISE instance.

Local Target Message Format: <timestamp> <seq_num> 52007 NOTICE Distributed-Management: Force Full replication, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52007 NOTICE Distributed-Management: Force Full replication, <log details>

- **Message Code:** 52008

  Severity: NOTICE

  Message Text: Replacement Register Handler

  Message Description: A new ISE instance has joined the deployment through hardware replacement.

  Local Target Message Format: <timestamp> <seq_num> 52008 NOTICE Distributed-Management: Replacement Register Handler, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52008 NOTICE Distributed-Management: Replacement Register Handler, <log details>

- **Message Code:** 52009

  Severity: NOTICE

  Message Text: Promote Node

  Message Description: A Secondary node has been promoted to be the Primary node of the deployment.

  Local Target Message Format: <timestamp> <seq_num> 52009 NOTICE Distributed-Management: Promote Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52009 NOTICE Distributed-Management: Promote Node, <log details>

- **Message Code:** 52010

  Severity: NOTICE

  Message Text: Promote Node Handler

  Message Description: A Secondary node has been promoted to be the Primary node of the deployment.

  Local Target Message Format: <timestamp> <seq_num> 52010 NOTICE Distributed-Management: Promote Node Handler, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52010 NOTICE Distributed-Management: Promote Node Handler, <log details>

- **Message Code:** 52011

  Severity: NOTICE

  Message Text: Local Mode

  Message Description: An ISE instance has been switched to Local Mode operation and is no longer receiving updates from the Primary node.

Local Target Message Format: <timestamp> <seq_num> 52011 NOTICE Distributed-Management: Local Mode, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52011 NOTICE Distributed-Management: Local Mode, <log details>

- **Message Code:** 52012

  Severity: NOTICE

  Message Text: Local Mode Handler

  Message Description: An ISE instance has been switched to Local Mode operation and is no longer receiving updates from the Primary node.

  Local Target Message Format: <timestamp> <seq_num> 52012 NOTICE Distributed-Management: Local Mode Handler, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52012 NOTICE Distributed-Management: Local Mode Handler, <log details>

- **Message Code:** 52013

  Severity: NOTICE

  Message Text: Hardware Replacement

  Message Description: A new ISE instance has joined the deployment through hardware replacement.

  Local Target Message Format: <timestamp> <seq_num> 52013 NOTICE Distributed-Management: Hardware Replacement, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52013 NOTICE Distributed-Management: Hardware Replacement, <log details>

- **Message Code:** 52014

  Severity: NOTICE

  Message Text: Deregister Handler

  Message Description: One of the ISE instances in the deployment has been de-registered.

  Local Target Message Format: <timestamp> <seq_num> 52014 NOTICE Distributed-Management: Deregister Handler, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52014 NOTICE Distributed-Management: Deregister Handler, <log details>

- **Message Code:** 52015

  Severity: NOTICE

  Message Text: Enable LogCollector Target

  Message Description: Enable the deployment Log Collector target.

Local Target Message Format: <timestamp> <seq_num> 52015 NOTICE Distributed-Management: Enable LogCollector Target, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52015 NOTICE Distributed-Management: Enable LogCollector Target, <log details>

- **Message Code:** 52016

  Severity: NOTICE

  Message Text: Select LogCollector Node

  Message Description: The Log Collector node for the deployment has been selected.

  Local Target Message Format: <timestamp> <seq_num> 52016 NOTICE Distributed-Management: Select LogCollector Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52016 NOTICE Distributed-Management: Select LogCollector Node, <log details>

- **Message Code:** 52017

  Severity: NOTICE

  Message Text: Apply software update

  Message Description: Apply a software update to the selected ISE instances.

  Local Target Message Format: <timestamp> <seq_num> 52017 NOTICE Distributed-Management: Apply software update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52017 NOTICE Distributed-Management: Apply software update, <log details>

- **Message Code:** 52018

  Severity: NOTICE

  Message Text: Overriding an ISE Instances Log Categories

  Message Description: An ISE Instance has had its Log Categories overridden to allow it to be configured separately from the Global Log Categories configuration.

  Local Target Message Format: <timestamp> <seq_num> 52018 NOTICE Distributed-Management: Overriding an ISE Instances Log Categories, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52018 NOTICE Distributed-Management: Overriding an ISE Instances Log Categories, <log details>

- **Message Code:** 52019

  Severity: NOTICE

  Message Text: Restoring an ISE Instances Log Categories to Global

  Message Description: An ISE Instance has had its Log Categories restored to use the Global Log Categories configuration.

Local Target Message Format: <timestamp> <seq_num> 52019 NOTICE Distributed-Management: Restoring an ISE Instances Log Categories to Global, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52019 NOTICE Distributed-Management: Restoring an ISE Instances Log Categories to Global, <log details>

- **Message Code:** 52020

  Severity: NOTICE

  Message Text: Full Replication

  Message Description: The primary requested full replication

  Local Target Message Format: <timestamp> <seq_num> 52020 NOTICE Distributed-Management: Full Replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52020 NOTICE Distributed-Management: Full Replication, <log details>

- **Message Code:** 52021

  Severity: NOTICE

  Message Text: Full replication request

  Message Description: The secondary requested full replication

  Local Target Message Format: <timestamp> <seq_num> 52021 NOTICE Distributed-Management: Full replication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52021 NOTICE Distributed-Management: Full replication request, <log details>

- **Message Code:** 52022

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Creating a link between the primary and secondary nodes

  Local Target Message Format: <timestamp> <seq_num> 52022 NOTICE Distributed-Management: Full replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52022 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52023

  Severity: NOTICE

  Message Text: Full replication failed

  Message Description: Failed to create a link between the primary and secondary nodes

Local Target Message Format: <timestamp> <seq_num> 52023 NOTICE Distributed-Management: Full replication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52023 NOTICE Distributed-Management: Full replication failed, <log details>

- **Message Code:** 52024

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Creating a local credential file on the node

  Local Target Message Format: <timestamp> <seq_num> 52024 NOTICE Distributed-Management: Full replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52024 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52025

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Retrieving the remote database key

  Local Target Message Format: <timestamp> <seq_num> 52025 NOTICE Distributed-Management: Full replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52025 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52026

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Retrieving the database from the primary over the secure Sybase channel

  Local Target Message Format: <timestamp> <seq_num> 52026 NOTICE Distributed-Management: Full replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52026 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52027

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Stopping the message bus heartbeat channel

Local Target Message Format: <timestamp> <seq_num> 52027 NOTICE Distributed-Management: Full replication, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52027 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52028

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Deleting backup files

  Local Target Message Format: <timestamp> <seq_num> 52028 NOTICE Distributed-Management: Full replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52028 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52029

  Severity: NOTICE

  Message Text: Full replication

  Message Description: Running the cleanup script and restarting ISE services

  Local Target Message Format: <timestamp> <seq_num> 52029 NOTICE Distributed-Management: Full replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52029 NOTICE Distributed-Management: Full replication, <log details>

- **Message Code:** 52030

  Severity: NOTICE

  Message Text: Full replication succeeded

  Message Description: Full replication was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52030 NOTICE Distributed-Management: Full replication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52030 NOTICE Distributed-Management: Full replication succeeded, <log details>

- **Message Code:** 52031

  Severity: NOTICE

  Message Text: Full replication failed

  Message Description: Failed to complete full replication

Local Target Message Format: <timestamp> <seq_num> 52031 NOTICE Distributed-Management: Full replication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52031 NOTICE Distributed-Management: Full replication failed, <log details>

- **Message Code:** 52032

  Severity: NOTICE

  Message Text: Registration request

  Message Description: An ISE instance requested to join a distributed environment

  Local Target Message Format: <timestamp> <seq_num> 52032 NOTICE Distributed-Management: Registration request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52032 NOTICE Distributed-Management: Registration request, <log details>

- **Message Code:** 52033

  Severity: NOTICE

  Message Text: Registration succeeded

  Message Description: Registration with the primary node was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52033 NOTICE Distributed-Management: Registration succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52033 NOTICE Distributed-Management: Registration succeeded, <log details>

- **Message Code:** 52034

  Severity: NOTICE

  Message Text: Registration request

  Message Description: The primary instance has requested full replication

  Local Target Message Format: <timestamp> <seq_num> 52034 NOTICE Distributed-Management: Registration request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52034 NOTICE Distributed-Management: Registration request, <log details>

- **Message Code:** 52035

  Severity: NOTICE

  Message Text: Registration failed

  Message Description: Failed to perform the full replication requested by the primary instance

Local Target Message Format: <timestamp> <seq_num> 52035 NOTICE Distributed-Management: Registration failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52035 NOTICE Distributed-Management: Registration failed, <log details>

- **Message Code:** 52036

  Severity: NOTICE

  Message Text: Registration

  Message Description: Changing an ISE instance from primary to secondary

  Local Target Message Format: <timestamp> <seq_num> 52036 NOTICE Distributed-Management: Registration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52036 NOTICE Distributed-Management: Registration, <log details>

- **Message Code:** 52037

  Severity: NOTICE

  Message Text: Registration

  Message Description: Updating the primary instance to secondary in the database

  Local Target Message Format: <timestamp> <seq_num> 52037 NOTICE Distributed-Management: Registration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52037 NOTICE Distributed-Management: Registration, <log details>

- **Message Code:** 52038

  Severity: NOTICE

  Message Text: Registration succeeded

  Message Description: The ISE instance was successfully joined to a distributed ISE deployment

  Local Target Message Format: <timestamp> <seq_num> 52038 NOTICE Distributed-Management: Registration succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52038 NOTICE Distributed-Management: Registration succeeded, <log details>

- **Message Code:** 52039

  Severity: NOTICE

  Message Text: Registration failed

  Message Description: The ISE instance was unable to join a distributed deployment

Local Target Message Format: <timestamp> <seq_num> 52039 NOTICE Distributed-Management: Registration failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52039 NOTICE Distributed-Management: Registration failed, <log details>

- **Message Code:** 52040

  Severity: NOTICE

  Message Text: Promotion request

  Message Description: Issued a request to promote a secondary instance

  Local Target Message Format: <timestamp> <seq_num> 52040 NOTICE Distributed-Management: Promotion request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52040 NOTICE Distributed-Management: Promotion request, <log details>

- **Message Code:** 52041

  Severity: NOTICE

  Message Text: Promotion request

  Message Description: A secondary instance requested to be promoted to be the primary instance

  Local Target Message Format: <timestamp> <seq_num> 52041 NOTICE Distributed-Management: Promotion request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52041 NOTICE Distributed-Management: Promotion request, <log details>

- **Message Code:** 52042

  Severity: NOTICE

  Message Text: Demotion succeeded

  Message Description: Demotion of the existing primary instance was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52042 NOTICE Distributed-Management: Demotion succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52042 NOTICE Distributed-Management: Demotion succeeded, <log details>

- **Message Code:** 52043

  Severity: NOTICE

  Message Text: Demotion failed

  Message Description: Demotion of the existing primary instance failed

Local Target Message Format: <timestamp> <seq_num> 52043 NOTICE Distributed-Management: Demotion failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52043 NOTICE Distributed-Management: Demotion failed, <log details>

- **Message Code:** 52044

  Severity: NOTICE

  Message Text: Promotion

  Message Description: The global deployment ID was successfully updated

  Local Target Message Format: <timestamp> <seq_num> 52044 NOTICE Distributed-Management: Promotion, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52044 NOTICE Distributed-Management: Promotion, <log details>

- **Message Code:** 52045

  Severity: NOTICE

  Message Text: Promotion succeeded

  Message Description: Promotion of the secondary instance was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52045 NOTICE Distributed-Management: Promotion succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52045 NOTICE Distributed-Management: Promotion succeeded, <log details>

- **Message Code:** 52046

  Severity: NOTICE

  Message Text: Promotion failed

  Message Description: Promotion of a secondary instance failed

  Local Target Message Format: <timestamp> <seq_num> 52046 NOTICE Distributed-Management: Promotion failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52046 NOTICE Distributed-Management: Promotion failed, <log details>

- **Message Code:** 52047

  Severity: NOTICE

  Message Text: Local mode reconnect request

  Message Description: The ISE instance in local mode issued a request to reconnect to the deployment

Local Target Message Format: <timestamp> <seq_num> 52047 NOTICE Distributed-Management: Local mode reconnect request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52047 NOTICE Distributed-Management: Local mode reconnect request, <log details>

- **Message Code:** 52048

  Severity: NOTICE

  Message Text: Local mode start

  Message Description: The ISE instance in local mode issued a remote call to the primary to reconnect to the deployment

  Local Target Message Format: <timestamp> <seq_num> 52048 NOTICE Distributed-Management: Local mode start, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52048 NOTICE Distributed-Management: Local mode start, <log details>

- **Message Code:** 52049

  Severity: NOTICE

  Message Text: Local mode reconnect

  Message Description: Initiating full replication for an ISE instance in local mode

  Local Target Message Format: <timestamp> <seq_num> 52049 NOTICE Distributed-Management: Local mode reconnect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52049 NOTICE Distributed-Management: Local mode reconnect, <log details>

- **Message Code:** 52050

  Severity: NOTICE

  Message Text: Local mode reconnect

  Message Description: Changing ISE instance status to secondary

  Local Target Message Format: <timestamp> <seq_num> 52050 NOTICE Distributed-Management: Local mode reconnect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52050 NOTICE Distributed-Management: Local mode reconnect, <log details>

- **Message Code:** 52051

  Severity: NOTICE

  Message Text: Local mode reconnect

  Message Description: Updating instance status to secondary in the database

Local Target Message Format: <timestamp> <seq_num> 52051 NOTICE Distributed-Management: Local mode reconnect, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52051 NOTICE Distributed-Management: Local mode reconnect, <log details>

- **Message Code:** 52052

  Severity: NOTICE

  Message Text: Local mode reconnect succeeded

  Message Description: Reconnecting a local mode instance to the deployment was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52052 NOTICE Distributed-Management: Local mode reconnect succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52052 NOTICE Distributed-Management: Local mode reconnect succeeded, <log details>

- **Message Code:** 52053

  Severity: NOTICE

  Message Text: Local mode reconnect failed

  Message Description: Reconnect a local mode instance to the deployment failed

  Local Target Message Format: <timestamp> <seq_num> 52053 NOTICE Distributed-Management: Local mode reconnect failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52053 NOTICE Distributed-Management: Local mode reconnect failed, <log details>

- **Message Code:** 52054

  Severity: NOTICE

  Message Text: Local mode request

  Message Description: Issued a request to local mode

  Local Target Message Format: <timestamp> <seq_num> 52054 NOTICE Distributed-Management: Local mode request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52054 NOTICE Distributed-Management: Local mode request, <log details>

- **Message Code:** 52055

  Severity: NOTICE

  Message Text: Local mode request

  Message Description: The secondary instance requested to be placed in local mode

Local Target Message Format: <timestamp> <seq_num> 52055 NOTICE Distributed-Management: Local mode request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52055 NOTICE Distributed-Management: Local mode request, <log details>

- **Message Code:** 52056

  Severity: NOTICE

  Message Text: Local mode

  Message Description: Changing the ISE instance status to local mode

  Local Target Message Format: <timestamp> <seq_num> 52056 NOTICE Distributed-Management: Local mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52056 NOTICE Distributed-Management: Local mode, <log details>

- **Message Code:** 52057

  Severity: NOTICE

  Message Text: Local mode

  Message Description: Updating the instance status to local mode in the database

  Local Target Message Format: <timestamp> <seq_num> 52057 NOTICE Distributed-Management: Local mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52057 NOTICE Distributed-Management: Local mode, <log details>

- **Message Code:** 52058

  Severity: NOTICE

  Message Text: Local mode succeeded

  Message Description: Local mode request was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52058 NOTICE Distributed-Management: Local mode succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52058 NOTICE Distributed-Management: Local mode succeeded, <log details>

- **Message Code:** 52059

  Severity: NOTICE

  Message Text: Local mode failed

  Message Description: Local mode request failed

Local Target Message Format: <timestamp> <seq_num> 52059 NOTICE Distributed-Management: Local mode failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52059 NOTICE Distributed-Management: Local mode failed, <log details>

- **Message Code:** 52060

  Severity: NOTICE

  Message Text: Deregister request

  Message Description: A primary requested to deregister a secondary from the distributed deployment

  Local Target Message Format: <timestamp> <seq_num> 52060 NOTICE Distributed-Management: Deregister request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52060 NOTICE Distributed-Management: Deregister request, <log details>

- **Message Code:** 52061

  Severity: NOTICE

  Message Text: Deregister request

  Message Description: A secondary requested to deregister from the distributed deployment

  Local Target Message Format: <timestamp> <seq_num> 52061 NOTICE Distributed-Management: Deregister request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52061 NOTICE Distributed-Management: Deregister request, <log details>

- **Message Code:** 52062

  Severity: NOTICE

  Message Text: Deregister

  Message Description: Removing the connection between the secondary and the primary

  Local Target Message Format: <timestamp> <seq_num> 52062 NOTICE Distributed-Management: Deregister, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52062 NOTICE Distributed-Management: Deregister, <log details>

- **Message Code:** 52063

  Severity: NOTICE

  Message Text: Deregister

  Message Description: Restarting registration heartbeat channel

Local Target Message Format: <timestamp> <seq_num> 52063 NOTICE Distributed-Management: Deregister, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52063 NOTICE Distributed-Management: Deregister, <log details>

- **Message Code:** 52070

  Severity: NOTICE

  Message Text: Deregister request

  Message Description: The secondary requested that the primary deregister itself

  Local Target Message Format: <timestamp> <seq_num> 52070 NOTICE Distributed-Management: Deregister request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52070 NOTICE Distributed-Management: Deregister request, <log details>

- **Message Code:** 52071

  Severity: NOTICE

  Message Text: Deregister

  Message Description: The primary deleted the secondary certificate information

  Local Target Message Format: <timestamp> <seq_num> 52071 NOTICE Distributed-Management: Deregister, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52071 NOTICE Distributed-Management: Deregister, <log details>

- **Message Code:** 52072

  Severity: NOTICE

  Message Text: Deregister succeeded

  Message Description: Deregistration was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52072 NOTICE Distributed-Management: Deregister succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52072 NOTICE Distributed-Management: Deregister succeeded, <log details>

- **Message Code:** 52073

  Severity: NOTICE

  Message Text: Deregister failed

  Message Description: Deregistration failed

Local Target Message Format: <timestamp> <seq_num> 52073 NOTICE Distributed-Management: Deregister failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52073 NOTICE Distributed-Management: Deregister failed, <log details>

- **Message Code:** 52074

  Severity: NOTICE

  Message Text: Delete node request

  Message Description: The ISE secondary instance in inactive mode requested to disconnect from the deployment

  Local Target Message Format: <timestamp> <seq_num> 52074 NOTICE Distributed-Management: Delete node request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52074 NOTICE Distributed-Management: Delete node request, <log details>

- **Message Code:** 52075

  Severity: NOTICE

  Message Text: Delete node request

  Message Description: The ISE secondary instance in inactive mode requested to disconnect from the primary instance

  Local Target Message Format: <timestamp> <seq_num> 52075 NOTICE Distributed-Management: Delete node request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52075 NOTICE Distributed-Management: Delete node request, <log details>

- **Message Code:** 52076

  Severity: NOTICE

  Message Text: Delete node request

  Message Description: The ISE primary instance requested to delete the secondary instance in inactive mode

  Local Target Message Format: <timestamp> <seq_num> 52076 NOTICE Distributed-Management: Delete node request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52076 NOTICE Distributed-Management: Delete node request, <log details>

- **Message Code:** 52077

  Severity: NOTICE

  Message Text: Delete node

Message Description: The ISE secondary instance in inactive mode successfully disconnected from the deployment

Local Target Message Format: <timestamp> <seq_num> 52077 NOTICE Distributed-Management: Delete node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52077 NOTICE Distributed-Management: Delete node, <log details>

- **Message Code:** 52078

  Severity: NOTICE

  Message Text: Delete node failed

  Message Description: Failed to delete the ISE secondary instance in inactive mode from the deployment

  Local Target Message Format: <timestamp> <seq_num> 52078 NOTICE Distributed-Management: Delete node failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52078 NOTICE Distributed-Management: Delete node failed, <log details>

- **Message Code:** 52079

  Severity: NOTICE

  Message Text: Delete node succeeded

  Message Description: The ISE primary instance successfully deleted the secondary instance in inactive mode

  Local Target Message Format: <timestamp> <seq_num> 52079 NOTICE Distributed-Management: Delete node succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52079 NOTICE Distributed-Management: Delete node succeeded, <log details>

- **Message Code:** 52080

  Severity: NOTICE

  Message Text: Delete node failed

  Message Description: Failed to delete the ISE secondary instance in inactive mode from the primary instance

  Local Target Message Format: <timestamp> <seq_num> 52080 NOTICE Distributed-Management: Delete node failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52080 NOTICE Distributed-Management: Delete node failed, <log details>

- **Message Code:** 52081

  Severity: NOTICE

Message Text: Backup request

Message Description: An immediate backup for the secondary instance was requested

Local Target Message Format: <timestamp> <seq_num> 52081 NOTICE DB-Management: Backup request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52081 NOTICE DB-Management: Backup request, <log details>

- **Message Code:** 52082

  Severity: NOTICE

  Message Text: Backup failed

  Message Description: An immediate backup for the secondary instance failed

  Local Target Message Format: <timestamp> <seq_num> 52082 NOTICE DB-Management: Backup failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52082 NOTICE DB-Management: Backup failed, <log details>

- **Message Code:** 52083

  Severity: NOTICE

  Message Text: Backup request

  Message Description: An immediate backup for the primary instance was requested

  Local Target Message Format: <timestamp> <seq_num> 52083 NOTICE DB-Management: Backup request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52083 NOTICE DB-Management: Backup request, <log details>

- **Message Code:** 52084

  Severity: NOTICE

  Message Text: Backup succeeded

  Message Description: An immediate backup for the primary instance was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52084 NOTICE DB-Management: Backup succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52084 NOTICE DB-Management: Backup succeeded, <log details>

- **Message Code:** 52085

  Severity: NOTICE

  Message Text: Backup failed

Message Description: An immediate backup for the primary failed

Local Target Message Format: <timestamp> <seq_num> 52085 NOTICE DB-Management: Backup failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52085 NOTICE DB-Management: Backup failed, <log details>

- **Message Code:** 52086

  Severity: NOTICE

  Message Text: Software update request

  Message Description: A software update was requested

  Local Target Message Format: <timestamp> <seq_num> 52086 NOTICE Software-Management: Software update request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52086 NOTICE Software-Management: Software update request, <log details>

- **Message Code:** 52088

  Severity: NOTICE

  Message Text: Software update

  Message Description: Applying software update

  Local Target Message Format: <timestamp> <seq_num> 52088 NOTICE Software-Management: Software update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52088 NOTICE Software-Management: Software update, <log details>

- **Message Code:** 52089

  Severity: NOTICE

  Message Text: Software update

  Message Description: Software update requires backup before the update

  Local Target Message Format: <timestamp> <seq_num> 52089 NOTICE Software-Management: Software update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52089 NOTICE Software-Management: Software update, <log details>

- **Message Code:** 52090

  Severity: NOTICE

  Message Text: Software update

  Message Description: The software update is downloading the update bundle from the primary instance

Local Target Message Format: <timestamp> <seq_num> 52090 NOTICE Software-Management: Software update, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52090 NOTICE Software-Management: Software update, <log details>

- **Message Code:** 52091

  Severity: NOTICE

  Message Text: Software update failed

  Message Description: Software update download of update bundle failed

  Local Target Message Format: <timestamp> <seq_num> 52091 NOTICE Software-Management: Software update failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52091 NOTICE Software-Management: Software update failed, <log details>

- **Message Code:** 52092

  Severity: NOTICE

  Message Text: Software update succeeded

  Message Description: The software update was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 52092 NOTICE Software-Management: Software update succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52092 NOTICE Software-Management: Software update succeeded, <log details>

- **Message Code:** 52093

  Severity: NOTICE

  Message Text: Software update failed

  Message Description: The software update failed

  Local Target Message Format: <timestamp> <seq_num> 52093 NOTICE Software-Management: Software update failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52093 NOTICE Software-Management: Software update failed, <log details>

- **Message Code:** 52094

  Severity: NOTICE

  Message Text: Activate request

  Message Description: Request to activate a secondary instance

Local Target Message Format: <timestamp> <seq_num> 52094 NOTICE Distributed-Management: Activate request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52094 NOTICE Distributed-Management: Activate request, <log details>

- **Message Code:** 52095

  Severity: NOTICE

  Message Text: Register

  Message Description: Request to perform hardware replacement of secondary instance in the deployment

  Local Target Message Format: <timestamp> <seq_num> 52095 NOTICE Distributed-Management: Register, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52095 NOTICE Distributed-Management: Register, <log details>

- **Message Code:** 52096

  Severity: NOTICE

  Message Text: Activate

  Message Description: Unable to retrieve the primary instance information

  Local Target Message Format: <timestamp> <seq_num> 52096 NOTICE Distributed-Management: Activate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52096 NOTICE Distributed-Management: Activate, <log details>

- **Message Code:** 52097

  Severity: NOTICE

  Message Text: Activate

  Message Description: Requested the secondary to initiate full replication

  Local Target Message Format: <timestamp> <seq_num> 52097 NOTICE Distributed-Management: Activate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52097 NOTICE Distributed-Management: Activate, <log details>

- **Message Code:** 52098

  Severity: NOTICE

  Message Text: Activate

  Message Description: Request to activate a secondary instance completed successfully

Local Target Message Format: <timestamp> <seq_num> 52098 NOTICE Distributed-Management: Activate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52098 NOTICE Distributed-Management: Activate, <log details>

- **Message Code:** 52099

  Severity: NOTICE

  Message Text: Activate

  Message Description: Request to activate a secondary instance failed

  Local Target Message Format: <timestamp> <seq_num> 52099 NOTICE Distributed-Management: Activate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52099 NOTICE Distributed-Management: Activate, <log details>

- **Message Code:** 52100

  Severity: NOTICE

  Message Text: Deregister

  Message Description: Check status process on secondary detected that it is now deregistered on the primary.

  Local Target Message Format: <timestamp> <seq_num> 52100 NOTICE Distributed-Management: Deregister, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52100 NOTICE Distributed-Management: Deregister, <log details>

- **Message Code:** 52101

  Severity: NOTICE

  Message Text: Deregister

  Message Description: Check status process on primary detected that a secondary instance has deregistered itself.

  Local Target Message Format: <timestamp> <seq_num> 52101 NOTICE Distributed-Management: Deregister, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52101 NOTICE Distributed-Management: Deregister, <log details>

- **Message Code:** 52102

  Severity: NOTICE

  Message Text: SCHEDULED BACKUP

  Message Description: Scheduled backup starting on primary instance.

Local Target Message Format: <timestamp> <seq_num> 52102 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52102 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

- **Message Code:** 52103

  Severity: NOTICE

  Message Text: SCHEDULED BACKUP

  Message Description: Scheduled backup failed to start due to invalid character in backup name.

  Local Target Message Format: <timestamp> <seq_num> 52103 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52103 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

- **Message Code:** 52104

  Severity: NOTICE

  Message Text: SCHEDULED BACKUP

  Message Description: Scheduled backup failed to start due to invalid repository.

  Local Target Message Format: <timestamp> <seq_num> 52104 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52104 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

- **Message Code:** 52105

  Severity: NOTICE

  Message Text: SCHEDULED BACKUP

  Message Description: Scheduled backup failed due to internal error.

  Local Target Message Format: <timestamp> <seq_num> 52105 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52105 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

- **Message Code:** 52106

  Severity: NOTICE

  Message Text: SCHEDULED BACKUP

  Message Description: Scheduled backup successfully completed.

Local Target Message Format: <timestamp> <seq_num> 52106 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 52106 NOTICE DB-Management: SCHEDULED BACKUP, <log details>

- **Message Code:** 57000

  Severity: NOTICE

  Message Text: Deleted rolled-over local log file(s)

  Message Description: Deleted rolled-over local log file(s)

  Local Target Message Format: <timestamp> <seq_num> 57000 NOTICE Configuration-changes: Deleted rolled-over local log file(s), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 57000 NOTICE Configuration-changes: Deleted rolled-over local log file(s), <log details>

- **Message Code:** 58001

  Severity: NOTICE

  Message Text: ISE process started

  Message Description: An ISE process has started

  Local Target Message Format: <timestamp> <seq_num> 58001 NOTICE Process-Management: ISE process started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58001 NOTICE Process-Management: ISE process started, <log details>

- **Message Code:** 58002

  Severity: NOTICE

  Message Text: ISE process stopped

  Message Description: An ISE process has stopped

  Local Target Message Format: <timestamp> <seq_num> 58002 NOTICE Process-Management: ISE process stopped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58002 NOTICE Process-Management: ISE process stopped, <log details>

- **Message Code:** 58003

  Severity: NOTICE

  Message Text: ISE processes started

  Message Description: All ISE processes have started

Local Target Message Format: <timestamp> <seq_num> 58003 NOTICE Process-Management: ISE processes started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58003 NOTICE Process-Management: ISE processes started, <log details>

- **Message Code:** 58004

  Severity: NOTICE

  Message Text: ISE processes stopped

  Message Description: All ISE processes have stopped

  Local Target Message Format: <timestamp> <seq_num> 58004 NOTICE Process-Management: ISE processes stopped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58004 NOTICE Process-Management: ISE processes stopped, <log details>

- **Message Code:** 58005

  Severity: NOTICE

  Message Text: ISE process was restarted by watchdog service

  Message Description: The watchdog service has restarted an ISE process

  Local Target Message Format: <timestamp> <seq_num> 58005 NOTICE Process-Management: ISE process was restarted by watchdog service, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58005 NOTICE Process-Management: ISE process was restarted by watchdog service, <log details>

- **Message Code:** 58006

  Severity: NOTICE

  Message Text: Watchdog configuration reloaded

  Message Description: The watchdog configuration has been reloaded

  Local Target Message Format: <timestamp> <seq_num> 58006 NOTICE Process-Management: Watchdog configuration reloaded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58006 NOTICE Process-Management: Watchdog configuration reloaded, <log details>

- **Message Code:** 58007

  Severity: NOTICE

  Message Text: ISE process reported start/stop error

  Message Description: An ISE process has reported a start or stop

Local Target Message Format: <timestamp> <seq_num> 58007 NOTICE Process-Management: ISE process reported start/stop error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58007 NOTICE Process-Management: ISE process reported start/stop error, <log details>

- **Message Code:** 58008

  Severity: NOTICE

  Message Text: CARS backup complete

  Message Description: The CARS backup was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 58008 NOTICE DB-Management: CARS backup complete, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58008 NOTICE DB-Management: CARS backup complete, <log details>

- **Message Code:** 58009

  Severity: NOTICE

  Message Text: CARS restore complete

  Message Description: The CARS restore was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 58009 NOTICE DB-Management: CARS restore complete, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58009 NOTICE DB-Management: CARS restore complete, <log details>

- **Message Code:** 58010

  Severity: NOTICE

  Message Text: ISE database backup

  Message Description: The ISE database backup was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 58010 NOTICE DB-Management: ISE database backup, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58010 NOTICE DB-Management: ISE database backup, <log details>

- **Message Code:** 58011

  Severity: NOTICE

  Message Text: ISE database restore

  Message Description: The ISE database restore was completed successfully

Local Target Message Format: <timestamp> <seq_num> 58011 NOTICE DB-Management: ISE database restore, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58011 NOTICE DB-Management: ISE database restore, <log details>

- **Message Code:** 58012

  Severity: NOTICE

  Message Text: ISE support bundle collected

  Message Description: The ISE support bundle has been collected

  Local Target Message Format: <timestamp> <seq_num> 58012 NOTICE DB-Management: ISE support bundle collected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58012 NOTICE DB-Management: ISE support bundle collected, <log details>

- **Message Code:** 58013

  Severity: NOTICE

  Message Text: ISE database reset

  Message Description: The ISE database has been reset

  Local Target Message Format: <timestamp> <seq_num> 58013 NOTICE DB-Management: ISE database reset, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58013 NOTICE DB-Management: ISE database reset, <log details>

- **Message Code:** 58014

  Severity: NOTICE

  Message Text: ISE core files deleted

  Message Description: The ISE core files have been deleted

  Local Target Message Format: <timestamp> <seq_num> 58014 NOTICE File-Management: ISE core files deleted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58014 NOTICE File-Management: ISE core files deleted, <log details>

- **Message Code:** 58015

  Severity: NOTICE

  Message Text: ISE log files deleted

  Message Description: The ISE log files have been deleted

Local Target Message Format: <timestamp> <seq_num> 58015 NOTICE File-Management: ISE log files deleted, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58015 NOTICE File-Management: ISE log files deleted, <log details>

- **Message Code:** 58016

  Severity: NOTICE

  Message Text: ISE upgrade

  Message Description: The ISE upgrade was completed successfully

  Local Target Message Format: <timestamp> <seq_num> 58016 NOTICE Software-Management: ISE upgrade, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58016 NOTICE Software-Management: ISE upgrade, <log details>

- **Message Code:** 58017

  Severity: NOTICE

  Message Text: ISE patch install

  Message Description: The ISE patch was successfully installed

  Local Target Message Format: <timestamp> <seq_num> 58017 NOTICE Software-Management: ISE patch install, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58017 NOTICE Software-Management: ISE patch install, <log details>

- **Message Code:** 58018

  Severity: NOTICE

  Message Text: ISE migration interface enabled/disabled

  Message Description: The ISE migration interface has been enabled or disabled

  Local Target Message Format: <timestamp> <seq_num> 58018 NOTICE System-Management: ISE migration interface enabled/disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58018 NOTICE System-Management: ISE migration interface enabled/disabled, <log details>

- **Message Code:** 58019

  Severity: NOTICE

  Message Text: ISE administrator password reset

  Message Description: The ISE administrator password has been reset

Local Target Message Format: <timestamp> <seq_num> 58019 NOTICE System-Management: ISE administrator password reset, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58019 NOTICE System-Management: ISE administrator password reset, <log details>

- **Message Code:** 58020

  Severity: NOTICE

  Message Text: Clock set

  Message Description: The clock has been set

  Local Target Message Format: <timestamp> <seq_num> 58020 NOTICE System-Management: Clock set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58020 NOTICE System-Management: Clock set, <log details>

- **Message Code:** 58021

  Severity: NOTICE

  Message Text: Time zone set

  Message Description: The time zone has been set

  Local Target Message Format: <timestamp> <seq_num> 58021 NOTICE System-Management: Time zone set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58021 NOTICE System-Management: Time zone set, <log details>

- **Message Code:** 58022

  Severity: NOTICE

  Message Text: NTP Server set

  Message Description: The NTP Server has been set

  Local Target Message Format: <timestamp> <seq_num> 58022 NOTICE System-Management: NTP Server set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58022 NOTICE System-Management: NTP Server set, <log details>

- **Message Code:** 58023

  Severity: NOTICE

  Message Text: Hostname set

  Message Description: The hostname has been set

Local Target Message Format: <timestamp> <seq_num> 58023 NOTICE System-Management: Hostname set, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58023 NOTICE System-Management: Hostname set, <log details>

- **Message Code:** 58024

  Severity: NOTICE

  Message Text: IP address set

  Message Description: The IP address has been set

  Local Target Message Format: <timestamp> <seq_num> 58024 NOTICE System-Management: IP address set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58024 NOTICE System-Management: IP address set, <log details>

- **Message Code:** 58025

  Severity: NOTICE

  Message Text: IP address state

  Message Description: IP address state

  Local Target Message Format: <timestamp> <seq_num> 58025 NOTICE System-Management: IP address state, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58025 NOTICE System-Management: IP address state, <log details>

- **Message Code:** 58026

  Severity: NOTICE

  Message Text: Default gateway set

  Message Description: The default gateway has been set

  Local Target Message Format: <timestamp> <seq_num> 58026 NOTICE System-Management: Default gateway set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58026 NOTICE System-Management: Default gateway set, <log details>

- **Message Code:** 58027

  Severity: NOTICE

  Message Text: Name server set

  Message Description: The name server has been set

Local Target Message Format: <timestamp> <seq_num> 58027 NOTICE System-Management: Name server set, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58027 NOTICE System-Management: Name server set, <log details>

- **Message Code:** 58028

  Severity: NOTICE

  Message Text: ADE OS Xfer library error

  Message Description: An error occurred in the ADE OS Xfer library

  Local Target Message Format: <timestamp> <seq_num> 58028 NOTICE System-Management: ADE OS Xfer library error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58028 NOTICE System-Management: ADE OS Xfer library error, <log details>

- **Message Code:** 58029

  Severity: NOTICE

  Message Text: ADE OS install library error

  Message Description: An error occurred in the ADE OS install library

  Local Target Message Format: <timestamp> <seq_num> 58029 NOTICE System-Management: ADE OS install library error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58029 NOTICE System-Management: ADE OS install library error, <log details>

- **Message Code:** 58030

  Severity: NOTICE

  Message Text: ISE upgrade - schema change

  Message Description: The ISE schema upgrade is complete

  Local Target Message Format: <timestamp> <seq_num> 58030 NOTICE Software-Management: ISE upgrade - schema change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58030 NOTICE Software-Management: ISE upgrade - schema change, <log details>

- **Message Code:** 58031

  Severity: NOTICE

  Message Text: ISE upgrade - dictionary

  Message Description: The ISE dictionary upgrade is complete

Local Target Message Format: <timestamp> <seq_num> 58031 NOTICE Software-Management: ISE upgrade - dictionary, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58031 NOTICE Software-Management: ISE upgrade - dictionary, <log details>

- **Message Code:** 58032

  Severity: NOTICE

  Message Text: ISE upgrade - data manipulation

  Message Description: ISE upgrade - data manipulation stage complete

  Local Target Message Format: <timestamp> <seq_num> 58032 NOTICE Software-Management: ISE upgrade - data manipulation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58032 NOTICE Software-Management: ISE upgrade - data manipulation, <log details>

- **Message Code:** 58033

  Severity: NOTICE

  Message Text: ISE upgrade - AAC

  Message Description: The ISE AAC upgrade is complete

  Local Target Message Format: <timestamp> <seq_num> 58033 NOTICE Software-Management: ISE upgrade - AAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58033 NOTICE Software-Management: ISE upgrade - AAC, <log details>

- **Message Code:** 58034

  Severity: NOTICE

  Message Text: ISE upgrade - PKI

  Message Description: The ISE PKI upgrade is complete

  Local Target Message Format: <timestamp> <seq_num> 58034 NOTICE Software-Management: ISE upgrade - PKI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58034 NOTICE Software-Management: ISE upgrade - PKI, <log details>

- **Message Code:** 58035

  Severity: NOTICE

  Message Text: ISE upgrade - MnT

  Message Description: The MnT upgrade is complete

Local Target Message Format: <timestamp> <seq_num> 58035 NOTICE Software-Management: ISE upgrade - MnT, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58035 NOTICE Software-Management: ISE upgrade - MnT, <log details>

- **Message Code:** 58036

  Severity: NOTICE

  Message Text: ISE upgrade

  Message Description: The ISE upgrade has been started

  Local Target Message Format: <timestamp> <seq_num> 58036 NOTICE Software-Management: ISE upgrade, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58036 NOTICE Software-Management: ISE upgrade, <log details>

- **Message Code:** 58037

  Severity: NOTICE

  Message Text: ISE install

  Message Description: The ISE installation has been started

  Local Target Message Format: <timestamp> <seq_num> 58037 NOTICE Software-Management: ISE install, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58037 NOTICE Software-Management: ISE install, <log details>

- **Message Code:** 58038

  Severity: NOTICE

  Message Text: Failed to join to AD

  Message Description: The AD agent failed to join the AD domain

  Local Target Message Format: <timestamp> <seq_num> 58038 NOTICE System-Management: Failed to join to AD, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58038 NOTICE System-Management: Failed to join to AD, <log details>

- **Message Code:** 58039

  Severity: NOTICE

  Message Text: AD join

  Message Description: The AD agent has joined the AD domain

Local Target Message Format: <timestamp> <seq_num> 58039 NOTICE System-Management: AD join, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58039 NOTICE System-Management: AD join, <log details>

- **Message Code:** 58040

  Severity: NOTICE

  Message Text: AD leave

  Message Description: The AD agent has left the AD domain

  Local Target Message Format: <timestamp> <seq_num> 58040 NOTICE System-Management: AD leave, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58040 NOTICE System-Management: AD leave, <log details>

- **Message Code:** 58041

  Severity: NOTICE

  Message Text: Import/export process aborted

  Message Description: The import/export process has aborted

  Local Target Message Format: <timestamp> <seq_num> 58041 NOTICE System-Management: Import/export process aborted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58041 NOTICE System-Management: Import/export process aborted, <log details>

- **Message Code:** 58042

  Severity: NOTICE

  Message Text: Import/export process started

  Message Description: The import/export process has started

  Local Target Message Format: <timestamp> <seq_num> 58042 NOTICE System-Management: Import/export process started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58042 NOTICE System-Management: Import/export process started, <log details>

- **Message Code:** 58043

  Severity: NOTICE

  Message Text: Import/export process complete

  Message Description: The import/export process is complete

Local Target Message Format: <timestamp> <seq_num> 58043 NOTICE System-Management: Import/export process complete, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58043 NOTICE System-Management: Import/export process complete, <log details>

- **Message Code:** 58044

  Severity: NOTICE

  Message Text: Error in import/export process

  Message Description: An error occurred during the import/export process

  Local Target Message Format: <timestamp> <seq_num> 58044 NOTICE System-Management: Error in import/export process, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58044 NOTICE System-Management: Error in import/export process, <log details>

- **Message Code:** 58045

  Severity: NOTICE

  Message Text: Only single network interface is allowed

  Message Description: Only single network interface is allowed

  Local Target Message Format: <timestamp> <seq_num> 58045 NOTICE System-Management: Only single network interface is allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 58045 NOTICE System-Management: Only single network interface is allowed, <log details>

- **Message Code:** 58046

  Severity: NOTICE

  Message Text: NTP successfully sync with configured server

  Message Description: NTP successfully sync with configured server

  Local Target Message Format: <timestamp> <seq_num>58046 NOTICE System-Management NTP successfully sync with configured server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>58046 NOTICE System-Management NTP successfully sync with configured server, <log details>

- **Message Code:** 58047

  Severity: NOTICE

  Message Text: NTP time jump was detected

  Message Description: NTP time jump was detected

Local Target Message Format: <timestamp> <seq_num>58047 NOTICE System-Management NTP time jump was detected, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>58047 NOTICE System-Management NTP time jump was detected, <log details>

- **Message Code:** 59000

  Severity: NOTICE

  Message Text: Received request to revoke all PACs

  Message Description: The administrator requested to revoke all previously issued EAP-FAST-related keys and PACs by generating a new EAP-FAST seed key.

  Local Target Message Format: <timestamp> <seq_num> 59000 NOTICE EAP-FAST: Received request to revoke all PACs, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59000 NOTICE EAP-FAST: Received request to revoke all PACs, <log details>

- **Message Code:** 59001

  Severity: NOTICE

  Message Text: Generated new EAP-FAST seed key

  Message Description: A new EAP-FAST seed key was successfully generated. All EAP-FAST-related keys and PACs will be revoked.

  Local Target Message Format: <timestamp> <seq_num> 59001 NOTICE EAP-FAST: Generated new EAP-FAST seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59001 NOTICE EAP-FAST: Generated new EAP-FAST seed key, <log details>

- **Message Code:** 59002

  Severity: NOTICE

  Message Text: Successfully updated EAP-FAST seed key

  Message Description: Successfully updated the EAP-FAST seed key, which will be used to derive master keys. All previously generated EAP-FAST keys and PACs have been revoked.

  Local Target Message Format: <timestamp> <seq_num> 59002 NOTICE EAP-FAST: Successfully updated EAP-FAST seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59002 NOTICE EAP-FAST: Successfully updated EAP-FAST seed key, <log details>

- **Message Code:** 59003

  Severity: NOTICE

  Message Text: User not authorized to revoke all EAP-FAST PACs

Message Description: The user is not authorized to revoke all EAP-FAST PACs.

Local Target Message Format: <timestamp> <seq_num> 59003 NOTICE EAP-FAST: User not authorized to revoke all EAP-FAST PACs, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59003 NOTICE EAP-FAST: User not authorized to revoke all EAP-FAST PACs, <log details>

- **Message Code:** 59004

  Severity: NOTICE

  Message Text: Timed out during attempt to revoke EAP-FAST keys and PACs

  Message Description: The ISE runtime experienced a timeout while attempting to revoke previously generated EAP-FAST keys and PACs.

  Local Target Message Format: <timestamp> <seq_num> 59004 NOTICE EAP-FAST: Timed out during attempt to revoke EAP-FAST keys and PACs, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59004 NOTICE EAP-FAST: Timed out during attempt to revoke EAP-FAST keys and PACs, <log details>

- **Message Code:** 59005

  Severity: NOTICE

  Message Text: Received request to generate Tunnel PAC

  Message Description: The administrator requested to manually issue an out-of-band EAP-FAST Tunnel PAC.

  Local Target Message Format: <timestamp> <seq_num> 59005 NOTICE EAP-FAST: Received request to generate Tunnel PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59005 NOTICE EAP-FAST: Received request to generate Tunnel PAC, <log details>

- **Message Code:** 59006

  Severity: NOTICE

  Message Text: Received request to generate Machine PAC

  Message Description: The administrator requested to manually issue an out-of-band EAP-FAST Machine PAC.

  Local Target Message Format: <timestamp> <seq_num> 59006 NOTICE EAP-FAST: Received request to generate Machine PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59006 NOTICE EAP-FAST: Received request to generate Machine PAC, <log details>

- **Message Code:** 59007

  Severity: NOTICE

Message Text: Failed to generate PAC

Message Description: Encountered an error while attempting to issue an out-of-band EAP-FAST PAC.

Local Target Message Format: <timestamp> <seq_num> 59007 NOTICE EAP-FAST: Failed to generate PAC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59007 NOTICE EAP-FAST: Failed to generate PAC, <log details>

- **Message Code:** 59008

  Severity: NOTICE

  Message Text: Successfully generated PAC

  Message Description: Succeeded in manually issuing an out-of-band EAP-FAST PAC.

  Local Target Message Format: <timestamp> <seq_num> 59008 NOTICE EAP-FAST: Successfully generated PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59008 NOTICE EAP-FAST: Successfully generated PAC, <log details>

- **Message Code:** 59009

  Severity: NOTICE

  Message Text: Received request to generate TrustSec PAC

  Message Description: The administrator requested to manually issue an out-of-band EAP-FAST TrustSec PAC.

  Local Target Message Format: <timestamp> <seq_num> 59009 NOTICE SGA-PAC: Received request to generate TrustSec PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59009 NOTICE SGA-PAC: Received request to generate TrustSec PAC, <log details>

- **Message Code:** 59010

  Severity: NOTICE

  Message Text: Failed to generate TrustSec PAC

  Message Description: Encountered an error while attempting to issue an out-of-band EAP-FAST TrustSec PAC.

  Local Target Message Format: <timestamp> <seq_num> 59010 NOTICE SGA-PAC: Failed to generate TrustSec PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59010 NOTICE SGA-PAC: Failed to generate TrustSec PAC, <log details>

- **Message Code:** 59011

  Severity: NOTICE

Message Text: Successfully generated TrustSec PAC

Message Description: Succeeded in manually issuing an out-of-band EAP-FAST TrustSec PAC.

Local Target Message Format: <timestamp> <seq_num> 59011 NOTICE SGA-PAC: Successfully generated TrustSec PAC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59011 NOTICE SGA-PAC: Successfully generated TrustSec PAC, <log details>

- **Message Code:** 59050

  Severity: NOTICE

  Message Text: Received request to revoke all Tickets

  Message Description: The administrator requested to revoke all previously issued EAP-TLS-related keys and Tickets by generating a new EAP-TLS seed key.

  Local Target Message Format: <timestamp> <seq_num> 59050 NOTICE EAP-TLS: Received request to revoke all Tickets, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59050 NOTICE EAP-TLS: Received request to revoke all Tickets, <log details>

- **Message Code:** 59051

  Severity: NOTICE

  Message Text: Generated new EAP-TLS seed key

  Message Description: A new EAP-TLS seed key was successfully generated. All EAP-TLS-related keys and Tickets will be revoked.

  Local Target Message Format: <timestamp> <seq_num> 59051 NOTICE EAP-TLS: Generated new EAP-TLS seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59051 NOTICE EAP-TLS: Generated new EAP-TLS seed key, <log details>

- **Message Code:** 59052

  Severity: NOTICE

  Message Text: Successfully updated EAP-TLS seed key

  Message Description: Successfully updated the EAP-TLS seed key, which will be used to derive master keys. All previously generated EAP-TLS keys and tickets have been revoked.

  Local Target Message Format: <timestamp> <seq_num> 59052 NOTICE EAP-TLS: Successfully updated EAP-TLS seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59052 NOTICE EAP-TLS: Successfully updated EAP-TLS seed key, <log details>

- **Message Code:** 59100

Severity: NOTICE

Message Text: Delete local store logs

Message Description: The admin requested to delete the local store logs

Local Target Message Format: <timestamp> <seq_num> 59100 NOTICE Log-Management: Delete local store logs, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59100 NOTICE Log-Management: Delete local store logs, <log details>

- **Message Code:** 59101

  Severity: NOTICE

  Message Text: Delete local store logs

  Message Description: The local store log file was deleted successfully

  Local Target Message Format: <timestamp> <seq_num> 59101 NOTICE Log-Management: Delete local store logs, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59101 NOTICE Log-Management: Delete local store logs, <log details>

- **Message Code:** 59102

  Severity: NOTICE

  Message Text: Delete local store logs

  Message Description: The local store log files were deleted successfully

  Local Target Message Format: <timestamp> <seq_num> 59102 NOTICE Log-Management: Delete local store logs, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59102 NOTICE Log-Management: Delete local store logs, <log details>

- **Message Code:** 59103

  Severity: NOTICE

  Message Text: Delete local store logs

  Message Description: Failed to delete the local store log files

  Local Target Message Format: <timestamp> <seq_num> 59103 NOTICE Log-Management: Delete local store logs, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59103 NOTICE Log-Management: Delete local store logs, <log details>

- **Message Code:** 59200

  Severity: NOTICE

Message Text: Set log collector

Message Description: The admin requested to set a log collector

Local Target Message Format: <timestamp> <seq_num> 59200 NOTICE Log-Management: Set log collector, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59200 NOTICE Log-Management: Set log collector, <log details>

- **Message Code:** 59201

  Severity: NOTICE

  Message Text: Set log collector

  Message Description: A log collector was set successfully

  Local Target Message Format: <timestamp> <seq_num> 59201 NOTICE Log-Management: Set log collector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59201 NOTICE Log-Management: Set log collector, <log details>

- **Message Code:** 59202

  Severity: NOTICE

  Message Text: Set log collector

  Message Description: An error occurred while setting a log collector

  Local Target Message Format: <timestamp> <seq_num> 59202 NOTICE Log-Management: Set log collector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59202 NOTICE Log-Management: Set log collector, <log details>

- **Message Code:** 59203

  Severity: NOTICE

  Message Text: Resume log collector

  Message Description: The admin requested to resume the log collector

  Local Target Message Format: <timestamp> <seq_num> 59203 NOTICE Log-Management: Resume log collector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59203 NOTICE Log-Management: Resume log collector, <log details>

- **Message Code:** 59204

  Severity: NOTICE

  Message Text: Resume log collector

Message Description: The log collector was resumed successfully

Local Target Message Format: <timestamp> <seq_num> 59204 NOTICE Log-Management: Resume log collector, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59204 NOTICE Log-Management: Resume log collector, <log details>

- **Message Code:** 59205

  Severity: NOTICE

  Message Text: Resume log collector

  Message Description: An error occurred while resuming the log collector

  Local Target Message Format: <timestamp> <seq_num> 59205 NOTICE Log-Management: Resume log collector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59205 NOTICE Log-Management: Resume log collector, <log details>

- **Message Code:** 59206

  Severity: NOTICE

  Message Text: Suspend log collector

  Message Description: The admin requested to suspend the log collector

  Local Target Message Format: <timestamp> <seq_num> 59206 NOTICE Log-Management: Suspend log collector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59206 NOTICE Log-Management: Suspend log collector, <log details>

- **Message Code:** 59207

  Severity: NOTICE

  Message Text: Suspend log collector

  Message Description: The log collector was suspended successfully

  Local Target Message Format: <timestamp> <seq_num> 59207 NOTICE Log-Management: Suspend log collector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59207 NOTICE Log-Management: Suspend log collector, <log details>

- **Message Code:** 59208

  Severity: NOTICE

  Message Text: Suspend log collector

  Message Description: An error occurred while suspending the log collector

Local Target Message Format: <timestamp> <seq_num> 59208 NOTICE Log-Management: Suspend log collector, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59208 NOTICE Log-Management: Suspend log collector, <log details>

- **Message Code:** 59250

  Severity: NOTICE

  Message Text: Administrator reset the access setting from CLI

  Message Description: The administrator successfully activated the access-setting command from the config-acs shell. See the command-line information within this message for details.

  Local Target Message Format: <timestamp> <seq_num> 59250 NOTICE CLI: Administrator reset the access setting from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59250 NOTICE CLI: Administrator reset the access setting from CLI, <log details>

- **Message Code:** 59251

  Severity: NOTICE

  Message Text: Administrator activated/deactivated AD debug level from CLI

  Message Description: The administrator has successfully activated the debug-adclient command from the config-acs shell. See the command-line information within this message for details.

  Local Target Message Format: <timestamp> <seq_num> 59251 NOTICE CLI: Administrator activated/deactivated AD debug level from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59251 NOTICE CLI: Administrator activated/deactivated AD debug level from CLI, <log details>

- **Message Code:** 59252

  Severity: NOTICE

  Message Text: Administrator changed component debug log level from CLI

  Message Description: The administrator has successfully activated the debug-log command from the config-acs shell. See the command-line information within this message for details.

  Local Target Message Format: <timestamp> <seq_num> 59252 NOTICE CLI: Administrator changed component debug log level from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59252 NOTICE CLI: Administrator changed component debug log level from CLI, <log details>

- **Message Code:** 59253

  Severity: NOTICE

  Message Text: Administrator started export configuration data process from CLI

Message Description: The administrator has successfully activated the export-data command from the config-acs shell. See the command-line information within this message for details.

Local Target Message Format: <timestamp> <seq_num> 59253 NOTICE CLI: Administrator started export configuration data process from CLI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59253 NOTICE CLI: Administrator started export configuration data process from CLI, <log details>

- **Message Code:** 59254

  Severity: NOTICE

  Message Text: Administrator started export configuration data process from CLI

  Message Description: The administrator has successfully activated the import-data command from the config-acs shell. See the command-line information within this message for details.

  Local Target Message Format: <timestamp> <seq_num> 59254 NOTICE CLI: Administrator started export configuration data process from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59254 NOTICE CLI: Administrator started export configuration data process from CLI, <log details>

- **Message Code:** 59255

  Severity: NOTICE

  Message Text: Administrator aborted import/export configuration data process from CLI

  Message Description: The administrator has successfully activated the import-export-abort command from the config-acs shell. See the command-line information within this message for details.

  Local Target Message Format: <timestamp> <seq_num> 59255 NOTICE CLI: Administrator aborted import/export configuration data process from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59255 NOTICE CLI: Administrator aborted import/export configuration data process from CLI, <log details>

- **Message Code:** 59256

  Severity: NOTICE

  Message Text: Administrator started replication process from CLI

  Message Description: The administrator has successfully activated the replication command from the config-acs shell. See the command-line information within this message for details.

  Local Target Message Format: <timestamp> <seq_num> 59256 NOTICE CLI: Administrator started replication process from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59256 NOTICE CLI: Administrator started replication process from CLI, <log details>

- **Message Code:** 59257

Severity: NOTICE

Message Text: Administrator reset management interface certificate from CLI

Message Description: The administrator has successfully activated the reset-management-interface-certificate command from the config-acs shell. See the command-line information within this message for details.

Local Target Message Format: <timestamp> <seq_num> 59257 NOTICE CLI: Administrator reset management interface certificate from CLI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59257 NOTICE CLI: Administrator reset management interface certificate from CLI, <log details>

- **Message Code:** 59258

  Severity: NOTICE

  Message Text: Administrator decrypted support bundle from CLI

  Message Description: The administrator has successfully activated the decrypt-support-bundle command from the config-acs shell. More details can be found in the command line information within this message

  Local Target Message Format: <timestamp> <seq_num> 59258 NOTICE CLI: Administrator decrypted support bundle from CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59258 NOTICE CLI: Administrator decrypted support bundle from CLI, <log details>

- **Message Code:** 59259

  Severity: WARN

  Message Text: Replication failed

  Message Description: Replicated failed and will stop applying new configuration changes

  Local Target Message Format: <timestamp> <seq_num> 59259 WARN Replication: Replication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 59259 WARN Replication: Replication failed, <log details>

- **Message Code:** 60000

  Severity: NOTICE

  Message Text: Patch installation completed successfully on the node

  Message Description: Patch installation completed successfully on the node

  Local Target Message Format: <timestamp> <seq_num> 60000 NOTICE Software-Management: Patch installation completed successfully on the node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60000 NOTICE Software-Management: Patch installation completed successfully on the node, <log details>

- **Message Code:** 60001

  Severity: NOTICE

  Message Text: Patch installation failed on the node

  Message Description: Patch installation failed on the node

  Local Target Message Format: <timestamp> <seq_num> 60001 NOTICE Software-Management: Patch installation failed on the node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60001 NOTICE Software-Management: Patch installation failed on the node, <log details>

- **Message Code:** 60002

  Severity: NOTICE

  Message Text: Patch rollback completed successfully on the node

  Message Description: Patch rollback completed successfully on the node

  Local Target Message Format: <timestamp> <seq_num> 60002 NOTICE Software-Management: Patch rollback completed successfully on the node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60002 NOTICE Software-Management: Patch rollback completed successfully on the node, <log details>

- **Message Code:** 60003

  Severity: NOTICE

  Message Text: Patch rollback failed on the node

  Message Description: Patch rollback failed on the node

  Local Target Message Format: <timestamp> <seq_num> 60003 NOTICE Software-Management: Patch rollback failed on the node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60003 NOTICE Software-Management: Patch rollback failed on the node, <log details>

- **Message Code:** 60050

  Severity: NOTICE

  Message Text: Node added to deployment successfully

  Message Description: Node added to deployment successfully

  Local Target Message Format: <timestamp> <seq_num> 60050 NOTICE Distributed-Management: Node added to deployment successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60050 NOTICE Distributed-Management: Node added to deployment successfully, <log details>

- **Message Code:** 60051

Severity: NOTICE

Message Text: Failed to add node to deployment

Message Description: Failed to add node to deployment

Local Target Message Format: <timestamp> <seq_num> 60051 NOTICE Distributed-Management: Failed to add node to deployment, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60051 NOTICE Distributed-Management: Failed to add node to deployment, <log details>

- **Message Code:** 60052

  Severity: NOTICE

  Message Text: Node removed from deployment

  Message Description: Node removed from deployment

  Local Target Message Format: <timestamp> <seq_num> 60052 NOTICE Distributed-Management: Node removed from deployment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60052 NOTICE Distributed-Management: Node removed from deployment, <log details>

- **Message Code:** 60053

  Severity: NOTICE

  Message Text: Failed to remove node from deployment

  Message Description: Failed to remove node from deployment

  Local Target Message Format: <timestamp> <seq_num> 60053 NOTICE Distributed-Management: Failed to remove node from deployment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60053 NOTICE Distributed-Management: Failed to remove node from deployment, <log details>

- **Message Code:** 60054

  Severity: NOTICE

  Message Text: Node updated successfully

  Message Description: Node updated successfully

  Local Target Message Format: <timestamp> <seq_num> 60054 NOTICE Distributed-Management: Node updated successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60054 NOTICE Distributed-Management: Node updated successfully, <log details>

- **Message Code:** 60055

  Severity: NOTICE

Message Text: Failed to update node

Message Description: Failed to update node

Local Target Message Format: <timestamp> <seq_num> 60055 NOTICE Distributed-Management: Failed to update node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60055 NOTICE Distributed-Management: Failed to update node, <log details>

- **Message Code:** 60056

  Severity: NOTICE

  Message Text: The runtime status of the node group has changed

  Message Description: There is a change in the cluster state

  Local Target Message Format: <timestamp> <seq_num> 60056 NOTICE PSN-Heartbeat: The runtime status of the node group has changed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60056 NOTICE PSN-Heartbeat: The runtime status of the node group has changed, <log details>

- **Message Code:** 60057

  Severity: NOTICE

  Message Text: A PSN node went down

  Message Description: One of the PSN nodes in the node group has gone down

  Local Target Message Format: <timestamp> <seq_num> 60057 NOTICE PSN-Heartbeat: A PSN node went down, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60057 NOTICE PSN-Heartbeat: A PSN node went down, <log details>

- **Message Code:** 60058

  Severity: NOTICE

  Message Text: The initial status of the heartbeat system

  Message Description: The initial status of the heartbeat system

  Local Target Message Format: <timestamp> <seq_num> 60058 NOTICE PSN-Heartbeat: The initial status of the heartbeat system, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60058 NOTICE PSN-Heartbeat: The initial status of the heartbeat system, <log details>

- **Message Code:** 60059

  Severity: NOTICE

  Message Text: Node has successfully registered with MnT

Message Description: Node has successfully registered with MnT

Local Target Message Format: <timestamp> <seq_num> 60059 NOTICE PSN-Heartbeat: Node has successfully registered with MnT, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60059 NOTICE PSN-Heartbeat: Node has successfully registered with MnT, <log details>

- **Message Code:** 60060

  Severity: NOTICE

  Message Text: Administrator invoked OCSP Clear Cache operation for all Policy Service nodes

  Message Description: The ISE Administrator invoked OCSP Clear Cache operation for all Policy Service nodes

  Local Target Message Format: <timestamp> <seq_num> 60060 NOTICE OCSP: Administrator invoked OCSP Clear Cache operation for all Policy Service nodes, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60060 NOTICE OCSP: Administrator invoked OCSP Clear Cache operation for all Policy Service nodes, <log details>

- **Message Code:** 60061

  Severity: NOTICE

  Message Text: OCSP Clear Cache operation completed successfully

  Message Description: OCSP Clear Cache operation completed successfully on all Policy Service nodes

  Local Target Message Format: <timestamp> <seq_num> 60061 NOTICE OCSP: OCSP Clear Cache operation completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60061 NOTICE OCSP: OCSP Clear Cache operation completed successfully, <log details>

- **Message Code:** 60062

  Severity: NOTICE

  Message Text: OCSP Clear Cache operation terminated with error

  Message Description: OCSP Clear Cache clear operation terminated with error on one or more Policy Service nodes

  Local Target Message Format: <timestamp> <seq_num> 60062 NOTICE OCSP: OCSP Clear Cache operation terminated with error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60062 NOTICE OCSP: OCSP Clear Cache operation terminated with error, <log details>

- **Message Code:** 60063

  Severity: NOTICE

  Message Text: Replication to node completed successfully

Message Description: Replication of data to secondary node completed successfully

Local Target Message Format: <timestamp> <seq_num> 60063 NOTICE Distributed-Management: Replication to node completed successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60063 NOTICE Distributed-Management: Replication to node completed successfully, <log details>

- **Message Code:** 60064

  Severity: NOTICE

  Message Text: Replication to node failed

  Message Description: Replication of data to secondary node failed

  Local Target Message Format: <timestamp> <seq_num> 60064 NOTICE Distributed-Management: Replication to node failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60064 NOTICE Distributed-Management: Replication to node failed, <log details>

- **Message Code:** 60065

  Severity: NOTICE

  Message Text: The maximum number of Administrative sessions have been exceeded

  Message Description: The maximum number of Administrative sessions have been exceeded

  Local Target Message Format: <timestamp> <seq_num> 60065 NOTICE Administrator-Login: The maximum number of Administrative sessions have been exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60065 NOTICE Administrator-Login: The maximum number of Administrative sessions have been exceeded, <log details>

- **Message Code:** 60066

  Severity: NOTICE

  Message Text: The delta between the old and the new is not matched

  Message Description: The delta between the old and the new is not matched

  Local Target Message Format: <timestamp> <seq_num> 60066 NOTICE Administrator-Login: The delta between the old and the new is not matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60066 NOTICE Administrator-Login: The delta between the old and the new is not matched, <log details>

- **Message Code:** 60067

  Severity: INFO

  Message Text: Profiler Feed Service - automatic download intitiated

Message Description: The Profiler Feed Service has begun the scheduled check and download of new and/or updated Profiles

Local Target Message Format: <timestamp> <seq_num> 60067 INFO FeedService: Profiler Feed Service - automatic download intitiated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60067 INFO FeedService: Profiler Feed Service - automatic download intitiated, <log details>

- **Message Code:** 60068

  Severity: INFO

  Message Text: Profiler Feed Service - manual download initiated

  Message Description: The Profiler Feed Service has begun the check and download of new and/or updated Profiles in response to Administrator's request

  Local Target Message Format: <timestamp> <seq_num> 60068 INFO FeedService: Profiler Feed Service - manual download initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60068 INFO FeedService: Profiler Feed Service - manual download initiated, <log details>

- **Message Code:** 60069

  Severity: INFO

  Message Text: Profiler Feed Service - Profiles Downloaded

  Message Description: The Profiler Feed Service has downloaded new and/or updated Profiles

  Local Target Message Format: <timestamp> <seq_num> 60069 INFO FeedService: Profiler Feed Service - Profiles Downloaded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60069 INFO FeedService: Profiler Feed Service - Profiles Downloaded, <log details>

- **Message Code:** 60070

  Severity: INFO

  Message Text: Profiler Feed Service - No Profiles Downloaded

  Message Description: The Profiler Feed Service found no new and/or updated Profiles to download

  Local Target Message Format: <timestamp> <seq_num> 60070 INFO FeedService: Profiler Feed Service - No Profiles Downloaded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60070 INFO FeedService: Profiler Feed Service - No Profiles Downloaded, <log details>

- **Message Code:** 60071

  Severity: WARN

  Message Text: Feed Server communication issue

Message Description: The Profiler Feed Service could not be reached

Local Target Message Format: <timestamp> <seq_num> 60071 WARN FeedService: Feed Server communication issue, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60071 WARN FeedService: Feed Server communication issue, <log details>

- **Message Code:** 60072

  Severity: ERROR

  Message Text: Profiler Feed Service reported that the Feed is unavailable

  Message Description: The Feed that was queried for was not known by the Profiler Feed Service

  Local Target Message Format: <timestamp> <seq_num> 60072 ERROR FeedService: Profiler Feed Service reported that the Feed is unavailable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60072 ERROR FeedService: Profiler Feed Service reported that the Feed is unavailable, <log details>

- **Message Code:** 60073

  Severity: ERROR

  Message Text: Querying the Profiler Feed Service resulted in an unexpected error

  Message Description: Received an unexpected error when querying the the Profiler Feed Service

  Local Target Message Format: <timestamp> <seq_num> 60073 ERROR FeedService: Querying the Profiler Feed Service resulted in an unexpected error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60073 ERROR FeedService: Querying the Profiler Feed Service resulted in an unexpected error, <log details>

- **Message Code:** 60074

  Severity: ERROR

  Message Text: Importing downloaded profiles from the Profiler Feed Service resulted in an unexpected error

  Message Description: Received an unexpected error when importing downloaded profiles from the Profiler Feed Service

  Local Target Message Format: <timestamp> <seq_num> 60074 ERROR FeedService: Importing downloaded profiles from the Profiler Feed Service resulted in an unexpected error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60074 ERROR FeedService: Importing downloaded profiles from the Profiler Feed Service resulted in an unexpected error, <log details>

- **Message Code:** 60075

  Severity: NOTICE

Message Text: Sponsor has successfully authenticated

Message Description: Sponsor has successfully authenticated

Local Target Message Format: <timestamp> <seq_num> 60075 NOTICE Sponsor: Sponsor has successfully authenticated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60075 NOTICE Sponsor: Sponsor has successfully authenticated, <log details>

- **Message Code:** 60076

  Severity: NOTICE

  Message Text: Sponsor authentication has failed

  Message Description: Sponsor authentication has failed; please see Failure Code for more details

  Local Target Message Format: <timestamp> <seq_num> 60076 NOTICE Sponsor: Sponsor authentication has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60076 NOTICE Sponsor: Sponsor authentication has failed, <log details>

- **Message Code:** 60077

  Severity: NOTICE

  Message Text: MyDevices user authentication has failed

  Message Description: MyDevices user authentication has failed

  Local Target Message Format: <timestamp> <seq_num> 60077 NOTICE MyDevices: MyDevices user authentication has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60077 NOTICE MyDevices: MyDevices user authentication has failed, <log details>

- **Message Code:** 60078

  Severity: INFO

  Message Text: MyDevices user has successfully authenticated

  Message Description: MyDevices user has successfully authenticated

  Local Target Message Format: <timestamp> <seq_num> 60078 INFO MyDevices: MyDevices user has successfully authenticated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60078 INFO MyDevices: MyDevices user has successfully authenticated, <log details>

- **Message Code:** 60079

  Severity: INFO

  Message Text: A failure to establish an SSL session was detected

Message Description: A failure to establish an SSL session was detected

Local Target Message Format: <timestamp> <seq_num> 60079 INFO Administrator-Login: A failure to establish an SSL session was detected, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60079 INFO Administrator-Login: A failure to establish an SSL session was detected, <log details>

- **Message Code:** 60080

  Severity: INFO

  Message Text: A SSH CLI user has successfully logged in

  Message Description: A SSH CLI User has successfully logged in

  Local Target Message Format: <timestamp> <seq_num> 60080 INFO Administrator-Login: A SSH CLI user has successfully logged in, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60080 INFO Administrator-Login: A SSH CLI user has successfully logged in, <log details>

- **Message Code:** 60081

  Severity: INFO

  Message Text: A SSH CLI user has attempted unsuccessfully to login

  Message Description: A SSH CLI user has attempted unsuccessfully to login

  Local Target Message Format: <timestamp> <seq_num> 60081 INFO Administrator-Login: A SSH CLI user has attempted unsuccessfully to login, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60081 INFO Administrator-Login: A SSH CLI user has attempted unsuccessfully to login, <log details>

- **Message Code:** 60082

  Severity: INFO

  Message Text: A SSH CLI user has attempted to login, however account is locked out

  Message Description: A SSH CLI user has attempted to login, however account is locked out

  Local Target Message Format: <timestamp> <seq_num> 60082 INFO Administrator-Login: A SSH CLI user has attempted to login, however account is locked out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60082 INFO Administrator-Login: A SSH CLI user has attempted to login, however account is locked out, <log details>

- **Message Code:** 60083

  Severity: INFO

  Message Text: Syslog Server configuration change

  Message Description: Syslog Server configuration change has occurred

Local Target Message Format: <timestamp> <seq_num> 60083 INFO System-Management: Syslog Server configuration change, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60083 INFO System-Management: Syslog Server configuration change, <log details>

- **Message Code:** 60084

  Severity: INFO

  Message Text: ADEOS CLI user configuration change

  Message Description: Configuration change occurred for ADEOS CLI user

  Local Target Message Format: <timestamp> <seq_num> 60084 INFO System-Management: ADEOS CLI user configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60084 INFO System-Management: ADEOS CLI user configuration change, <log details>

- **Message Code:** 60085

  Severity: INFO

  Message Text: ADEOS Repository configuration change

  Message Description: Configuration change occurred for ADEOS repository

  Local Target Message Format: <timestamp> <seq_num> 60085 INFO System-Management: ADEOS Repository configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60085 INFO System-Management: ADEOS Repository configuration change, <log details>

- **Message Code:** 60086

  Severity: INFO

  Message Text: ADEOS SSH Service configuration change

  Message Description: Configuration change occurred for ADEOS SSH Service

  Local Target Message Format: <timestamp> <seq_num> 60086 INFO System-Management: ADEOS SSH Service configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60086 INFO System-Management: ADEOS SSH Service configuration change, <log details>

- **Message Code:** 60087

  Severity: INFO

  Message Text: ADEOS Maximum SSH CLI sessions configuration change

  Message Description: Configuration change occurred for ADEOS Maximum CLI sessions

Local Target Message Format: <timestamp> <seq_num> 60087 INFO System-Management: ADEOS Maximum SSH CLI sessions configuration change, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60087 INFO System-Management: ADEOS Maximum SSH CLI sessions configuration change, <log details>

- **Message Code:** 60088

  Severity: INFO

  Message Text: ADEOS SNMP agent configuration change

  Message Description: Configuration change occurred for ADEOS SNMP agent

  Local Target Message Format: <timestamp> <seq_num> 60088 INFO System-Management: ADEOS SNMP agent configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60088 INFO System-Management: ADEOS SNMP agent configuration change, <log details>

- **Message Code:** 60089

  Severity: INFO

  Message Text: ADEOS CLI kron scheduler policy configuration change

  Message Description: Configuration change occurred for ADEOS CLI kron scheduler policy

  Local Target Message Format: <timestamp> <seq_num> 60089 INFO System-Management: ADEOS CLI kron scheduler policy configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60089 INFO System-Management: ADEOS CLI kron scheduler policy configuration change, <log details>

- **Message Code:** 60090

  Severity: INFO

  Message Text: ADEOS CLI kron scheduler occurence configuration change

  Message Description: Configuration change occurred for ADEOS CLI kron scheduler occurence

  Local Target Message Format: <timestamp> <seq_num> 60090 INFO System-Management: ADEOS CLI kron scheduler occurence configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60090 INFO System-Management: ADEOS CLI kron scheduler occurence configuration change, <log details>

- **Message Code:** 60091

  Severity: INFO

  Message Text: ADEOS CLI pre-login banner configuration change

  Message Description: Configuration change occurred for ADEOS CLI pre-login banner

Local Target Message Format: <timestamp> <seq_num> 60091 INFO System-Management: ADEOS CLI pre-login banner configuration change, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60091 INFO System-Management: ADEOS CLI pre-login banner configuration change, <log details>

- **Message Code:** 60092

  Severity: INFO

  Message Text: ADEOS CLI post-login banner configuration change

  Message Description: Configuration change occurred for ADEOS CLI post-login banner

  Local Target Message Format: <timestamp> <seq_num> 60092 INFO System-Management: ADEOS CLI post-login banner configuration change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60092 INFO System-Management: ADEOS CLI post-login banner configuration change, <log details>

- **Message Code:** 60093

  Severity: INFO

  Message Text: ISE Backup has started

  Message Description: ISE Backup has started

  Local Target Message Format: <timestamp> <seq_num> 60093 INFO System-Management: ISE Backup has started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60093 INFO System-Management: ISE Backup has started, <log details>

- **Message Code:** 60094

  Severity: INFO

  Message Text: ISE Backup has completed successfully

  Message Description: ISE Backup has completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60094 INFO System-Management: ISE Backup has completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60094 INFO System-Management: ISE Backup has completed successfully, <log details>

- **Message Code:** 60095

  Severity: ERROR

  Message Text: ISE Backup has failed

  Message Description: ISE Backup has failed

Local Target Message Format: <timestamp> <seq_num> 60095 ERROR System-Management: ISE Backup has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60095 ERROR System-Management: ISE Backup has failed, <log details>

- **Message Code:** 60096

  Severity: INFO

  Message Text: ISE Log backup has started

  Message Description: ISE Log Backup has started

  Local Target Message Format: <timestamp> <seq_num> 60096 INFO System-Management: ISE Log backup has started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60096 INFO System-Management: ISE Log backup has started, <log details>

- **Message Code:** 60097

  Severity: INFO

  Message Text: ISE Log Backup has completed successfully

  Message Description: ISE Log Backup has completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60097 INFO System-Management: ISE Log Backup has completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60097 INFO System-Management: ISE Log Backup has completed successfully, <log details>

- **Message Code:** 60098

  Severity: ERROR

  Message Text: ISE Log Backup has failed

  Message Description: ISE Log Backup has failed

  Local Target Message Format: <timestamp> <seq_num> 60098 ERROR System-Management: ISE Log Backup has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60098 ERROR System-Management: ISE Log Backup has failed, <log details>

- **Message Code:** 60099

  Severity: INFO

  Message Text: ISE Restore has started

  Message Description: ISE Restore has started

Local Target Message Format: <timestamp> <seq_num> 60099 INFO System-Management: ISE Restore has started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60099 INFO System-Management: ISE Restore has started, <log details>

- **Message Code:** 60100

  Severity: INFO

  Message Text: ISE Restore has completed successfully

  Message Description: ISE Restore has completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60100 INFO System-Management: ISE Restore has completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60100 INFO System-Management: ISE Restore has completed successfully, <log details>

- **Message Code:** 60101

  Severity: ERROR

  Message Text: ISE Restore has failed

  Message Description: ISE Restore has failed

  Local Target Message Format: <timestamp> <seq_num> 60101 ERROR System-Management: ISE Restore has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60101 ERROR System-Management: ISE Restore has failed, <log details>

- **Message Code:** 60102

  Severity: INFO

  Message Text: Application installation completed successfully

  Message Description: Application installation completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60102 INFO System-Management: Application installation completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60102 INFO System-Management: Application installation completed successfully, <log details>

- **Message Code:** 60103

  Severity: ERROR

  Message Text: Application installation failed

  Message Description: Application installation failed

Local Target Message Format: <timestamp> <seq_num> 60103 ERROR System-Management: Application installation failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60103 ERROR System-Management: Application installation failed, <log details>

- **Message Code:** 60104

  Severity: INFO

  Message Text: Application remove started

  Message Description: Application remove started

  Local Target Message Format: <timestamp> <seq_num> 60104 INFO System-Management: Application remove started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60104 INFO System-Management: Application remove started, <log details>

- **Message Code:** 60105

  Severity: INFO

  Message Text: Application remove completed successfully

  Message Description: Application remove completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60105 INFO System-Management: Application remove completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60105 INFO System-Management: Application remove completed successfully, <log details>

- **Message Code:** 60106

  Severity: ERROR

  Message Text: Application remove failed

  Message Description: Application remove failed

  Local Target Message Format: <timestamp> <seq_num> 60106 ERROR System-Management: Application remove failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60106 ERROR System-Management: Application remove failed, <log details>

- **Message Code:** 60107

  Severity: ERROR

  Message Text: Application upgrade failed

  Message Description: Application upgrade failed

Local Target Message Format: <timestamp> <seq_num> 60107 ERROR System-Management: Application upgrade failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60107 ERROR System-Management: Application upgrade failed, <log details>

- **Message Code:** 60108

  Severity: INFO

  Message Text: Application patch started

  Message Description: Application patch started

  Local Target Message Format: <timestamp> <seq_num> 60108 INFO System-Management: Application patch started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60108 INFO System-Management: Application patch started, <log details>

- **Message Code:** 60109

  Severity: INFO

  Message Text: Application patch remove has started

  Message Description: Application patch remove has started

  Local Target Message Format: <timestamp> <seq_num> 60109 INFO System-Management: Application patch remove has started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60109 INFO System-Management: Application patch remove has started, <log details>

- **Message Code:** 60111

  Severity: INFO

  Message Text: Application patch remove has completed successfully

  Message Description: Application patch remove has completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60111 INFO System-Management: Application patch remove has completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60111 INFO System-Management: Application patch remove has completed successfully, <log details>

- **Message Code:** 60112

  Severity: ERROR

  Message Text: Application patch remove has failed

  Message Description: Application patch remove has failed

Local Target Message Format: <timestamp> <seq_num> 60112 ERROR System-Management: Application patch remove has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60112 ERROR System-Management: Application patch remove has failed, <log details>

- **Message Code:** 60113

  Severity: WARNING

  Message Text: ISE server reload has been initiated

  Message Description: ISE server reload has been initiated

  Local Target Message Format: <timestamp> <seq_num> 60113 WARNING Startup-Shutdown: ISE server reload has been initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60113 WARNING Startup-Shutdown: ISE server reload has been initiated, <log details>

- **Message Code:** 60114

  Severity: WARNING

  Message Text: ISE server shutdown has been initiated

  Message Description: ISE server shutdown has been initiated

  Local Target Message Format: <timestamp> <seq_num> 60114 WARNING Startup-Shutdown: ISE server shutdown has been initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60114 WARNING Startup-Shutdown: ISE server shutdown has been initiated, <log details>

- **Message Code:** 60115

  Severity: INFO

  Message Text: A CLI user has logged in from SSH

  Message Description: A CLI user has logged in from SSH

  Local Target Message Format: <timestamp> <seq_num> 60115 INFO Administrator-Login: A CLI user has logged in from SSH, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60115 INFO Administrator-Login: A CLI user has logged in from SSH, <log details>

- **Message Code:** 60116

  Severity: INFO

  Message Text: A CLI user has logged out from SSH

  Message Description: A CLI user has logged out from SSH

Local Target Message Format: <timestamp> <seq_num> 60116 INFO Administrator-Login: A CLI user has logged out from SSH, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60116 INFO Administrator-Login: A CLI user has logged out from SSH, <log details>

- **Message Code:** 60117

  Severity: INFO

  Message Text: ADEOS CLI user has been force logged out

  Message Description: ADEOS CLI user has force logged out

  Local Target Message Format: <timestamp> <seq_num> 60117 INFO System-Management: ADEOS CLI user has been force logged out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60117 INFO System-Management: ADEOS CLI user has been force logged out, <log details>

- **Message Code:** 60118

  Severity: INFO

  Message Text: ADEOS CLI user has used delete CLI to delete file

  Message Description: ADEOS CLI user has used delete CLI to delete file

  Local Target Message Format: <timestamp> <seq_num> 60118 INFO System-Management: ADEOS CLI user has used delete CLI to delete file, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60118 INFO System-Management: ADEOS CLI user has used delete CLI to delete file, <log details>

- **Message Code:** 60119

  Severity: INFO

  Message Text: ADEOS CLI user has used copy CLI to copy file

  Message Description: ADEOS CLI user has used copy CLI to copy file

  Local Target Message Format: <timestamp> <seq_num> 60119 INFO System-Management: ADEOS CLI user has used copy CLI to copy file, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60119 INFO System-Management: ADEOS CLI user has used copy CLI to copy file, <log details>

- **Message Code:** 60120

  Severity: INFO

  Message Text: ADEOS CLI user has used mkdir CLI to create a directory

  Message Description: ADEOS CLI user has used mkdir CLI to create a directory

Local Target Message Format: <timestamp> <seq_num> 60120 INFO System-Management: ADEOS CLI user has used mkdir CLI to create a directory, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60120 INFO System-Management: ADEOS CLI user has used mkdir CLI to create a directory, <log details>

- **Message Code:** 60121

  Severity: INFO

  Message Text: ADEOS CLI user has copied out running system configuration

  Message Description: ADEOS CLI user has copied out running system configuration

  Local Target Message Format: <timestamp> <seq_num> 60121 INFO System-Management: ADEOS CLI user has copied out running system configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60121 INFO System-Management: ADEOS CLI user has copied out running system configuration, <log details>

- **Message Code:** 60122

  Severity: INFO

  Message Text: ADEOS CLI user has copied in system configuration

  Message Description: ADEOS CLI user has copied in system configuration

  Local Target Message Format: <timestamp> <seq_num> 60122 INFO System-Management: ADEOS CLI user has copied in system configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60122 INFO System-Management: ADEOS CLI user has copied in system configuration, <log details>

- **Message Code:** 60123

  Severity: INFO

  Message Text: ADEOS CLI user has saved running system configuration

  Message Description: ADEOS CLI user has saved running system configuration

  Local Target Message Format: <timestamp> <seq_num> 60123 INFO System-Management: ADEOS CLI user has saved running system configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60123 INFO System-Management: ADEOS CLI user has saved running system configuration, <log details>

- **Message Code:** 60124

  Severity: WARNING

  Message Text: ADEOS CLI user failed to login because password has expired

  Message Description: ADEOS CLI user failed to login because password has expired

Local Target Message Format: <timestamp> <seq_num> 60124 WARNING System-Management: ADEOS CLI user failed to login because password has expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60124 WARNING System-Management: ADEOS CLI user failed to login because password has expired, <log details>

- **Message Code:** 60125

  Severity: INFO

  Message Text: A malformed SSH requested has been detected

  Message Description: A malformed SSH requested has been detected

  Local Target Message Format: <timestamp> <seq_num> 60125 INFO Administrator-Login: A malformed SSH requested has been detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60125 INFO Administrator-Login: A malformed SSH requested has been detected, <log details>

- **Message Code:** 60126

  Severity: ERROR

  Message Text: Application patch installation failed

  Message Description: Application patch installation failed

  Local Target Message Format: <timestamp> <seq_num> 60126 ERROR System-Management: Application patch installation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60126 ERROR System-Management: Application patch installation failed, <log details>

- **Message Code:** 60127

  Severity: ERROR

  Message Text: Maximum number of concurrent CLI sessions has been reached

  Message Description: Maximum number of concurrent CLI sessions has been reached

  Local Target Message Format: <timestamp> <seq_num> 60127 ERROR System-Management: Maximum number of concurrent CLI sessions has been reached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60127 ERROR System-Management: Maximum number of concurrent CLI sessions has been reached, <log details>

- **Message Code:** 60128

  Severity: ERROR

  Message Text: Failure occurred trying to copy file in from ADEOS CLI

  Message Description: Failure occurred trying to copy file in from ADEOS CLI

Local Target Message Format: <timestamp> <seq_num> 60128 ERROR System-Management: Failure occurred trying to copy file in from ADEOS CLI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60128 ERROR System-Management: Failure occurred trying to copy file in from ADEOS CLI, <log details>

- **Message Code:** 60129

  Severity: ERROR

  Message Text: Failure occurred trying to copy file out from ADEOS CLI

  Message Description: Failure occurred trying to copy file out from ADEOS CLI

  Local Target Message Format: <timestamp> <seq_num> 60129 ERROR System-Management: Failure occurred trying to copy file out from ADEOS CLI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60129 ERROR System-Management: Failure occurred trying to copy file out from ADEOS CLI, <log details>

- **Message Code:** 60130

  Severity: INFO

  Message Text: ISE Scheduled Backup has been configured

  Message Description: ISE Scheduled Backup has been configured

  Local Target Message Format: <timestamp> <seq_num> 60130 INFO System-Management: ISE Scheduled Backup has been configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60130 INFO System-Management: ISE Scheduled Backup has been configured, <log details>

- **Message Code:** 60131

  Severity: INFO

  Message Text: ISE Support bundle has been created from web UI

  Message Description: ISE Support bundle has been created from web UI

  Local Target Message Format: <timestamp> <seq_num> 60131 INFO System-Management: ISE Support bundle has been created from web UI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60131 INFO System-Management: ISE Support bundle has been created from web UI, <log details>

- **Message Code:** 60132

  Severity: INFO

  Message Text: ISE Support bundle has been deleted from web UI

  Message Description: ISE Support bundle has been deleted from web UI

Local Target Message Format: <timestamp> <seq_num> 60132 INFO System-Management: ISE Support bundle has been deleted from web UI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60132 INFO System-Management: ISE Support bundle has been deleted from web UI, <log details>

- **Message Code:** 60133

  Severity: ERROR

  Message Text: ISE Support bundle generation from web UI has failed

  Message Description: ISE Support bundle generation from web UI has failed

  Local Target Message Format: <timestamp> <seq_num> 60133 ERROR System-Management: ISE Support bundle generation from web UI has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60133 ERROR System-Management: ISE Support bundle generation from web UI has failed, <log details>

- **Message Code:** 60134

  Severity: FATAL

  Message Text: DNS Resolution failure

  Message Description: DNS Resolution failure on node

  Local Target Message Format: <timestamp> <seq_num> 60134 FATAL System-Management: DNS Resolution failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60134 FATAL System-Management: DNS Resolution failure, <log details>

- **Message Code:** 60135

  Severity: INFO

  Message Text: MyDevices user SSO logout has failed

  Message Description: MyDevices user SSO logout has failed

  Local Target Message Format: <timestamp> <seq_num> 60135 INFO MyDevices: MyDevices user SSO logout has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60135 INFO MyDevices: MyDevices user SSO logout has failed, <log details>

- **Message Code:** 60136

  Severity: INFO

  Message Text: Sponsor user SSO logout has failed

  Message Description: Sponsor user SSO logout has failed

Local Target Message Format: <timestamp> <seq_num> 60136 INFO Sponsor: Sponsor user SSO logout has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60136 INFO Sponsor: Sponsor user SSO logout has failed, <log details>

- **Message Code:** 60150

  Severity: INFO

  Message Text: Slow Replication

  Message Description: Replication is slow

  Local Target Message Format: <timestamp> <seq_num> 60150 INFO Replication: Slow Replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60150 INFO Replication: Slow Replication, <log details>

- **Message Code:** 60151

  Severity: WARN

  Message Text: Slow Replication

  Message Description: Replication is slow

  Local Target Message Format: <timestamp> <seq_num> 60151 WARN Replication: Slow Replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60151 WARN Replication: Slow Replication, <log details>

- **Message Code:** 60152

  Severity: ERROR

  Message Text: Slow Replication

  Message Description: Replication is slow

  Local Target Message Format: <timestamp> <seq_num> 60152 ERROR Replication: Slow Replication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60152 ERROR Replication: Slow Replication, <log details>

- **Message Code:** 60153

  Severity: INFO

  Message Text: Certificate has been exported

  Message Description: Certificate has been exported

Local Target Message Format: <timestamp> <seq_num> 60153 INFO System-Management: Certificate has been exported, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60153 INFO System-Management: Certificate has been exported, <log details>

- **Message Code:** 60154

  Severity: INFO

  Message Text: Application patch install has completed successfully

  Message Description: Application patch install has completed successfully

  Local Target Message Format: <timestamp> <seq_num> 60154 INFO System-Management: Application patch install has completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60154 INFO System-Management: Application patch install has completed successfully, <log details>

- **Message Code:** 60155

  Severity: INFO

  Message Text: Secure communication with syslog server established

  Message Description: Secure communication with syslog server established

  Local Target Message Format: <timestamp> <seq_num> 60155 INFO System-Management: Secure communication with syslog server established, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60155 INFO System-Management: Secure communication with syslog server established, <log details>

- **Message Code:** 60156

  Severity: WARN

  Message Text: Secure communication establishment with syslog server failed

  Message Description: Secure communication establishment with syslog server failed

  Local Target Message Format: <timestamp> <seq_num> 60156 WARN System-Management: Secure communication establishment with syslog server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60156 WARN System-Management: Secure communication establishment with syslog server failed, <log details>

- **Message Code:** 60157

  Severity: ERROR

  Message Text: Unable to copy the exported report file to configured repository

  Message Description: Copying the exported report file to configured repository failed

Local Target Message Format: <timestamp> <seq_num> 60157 ERROR System-Management: Unable to copy the exported report file to configured repository, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60157 ERROR System-Management: Unable to copy the exported report file to configured repository, <log details>

- **Message Code:** 60158

  Severity: INFO

  Message Text: All xGrid administrator actions are logged using this message

  Message Description: All xGrid administrator actions are logged using this message

  Local Target Message Format: <timestamp> <seq_num> 60158 INFO System-Management: All xGrid administrator actions are logged using this message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60158 INFO System-Management: All xGrid administrator actions are logged using this message, <log details>

- **Message Code:** 60159

  Severity: INFO

  Message Text: Posture requirements update has started from the remote feed URL

  Message Description: The system received a request to check for posture requirement updates on remote feed URL. Update started.

  Local Target Message Format: <timestamp> <seq_num> 60159 INFO System-Management: Posture requirements update has started from the remote feed URL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60159 INFO System-Management: Posture requirements update has started from the remote feed URL, <log details>

- **Message Code:** 60160

  Severity: NOTICE

  Message Text: Successfully finished updating posture requirements from remote feed URL

  Message Description: The posture update from the remote feed URL has finished successfully

  Local Target Message Format: <timestamp> <seq_num> 60160 NOTICE System-Management: Successfully finished updating posture requirements from remote feed URL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60160 NOTICE System-Management: Successfully finished updating posture requirements from remote feed URL, <log details>

- **Message Code:** 60161

  Severity: ERROR

  Message Text: Failed to update Posture requirements from the remote feed URL

  Message Description: The Posture update from the remote feed URL has failed

Local Target Message Format: <timestamp> <seq_num> 60161 ERROR System-Management: Failed to update Posture requirements from the remote feed URL, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60161 ERROR System-Management: Failed to update Posture requirements from the remote feed URL, <log details>

- **Message Code:** 60162

  Severity: DEBUG

  Message Text: Checking for the updated Posture requirements on the remote feed URL

  Message Description: Starting the process of checking whether there are updated posture requirements on the remote feed URL

  Local Target Message Format: <timestamp> <seq_num> 60162 DEBUG System-Management: Checking for the updated Posture requirements on the remote feed URL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60162 DEBUG System-Management: Checking for the updated Posture requirements on the remote feed URL, <log details>

- **Message Code:** 60163

  Severity: DEBUG

  Message Text: Processing the updated Posture requirements received from the remote feed URL

  Message Description: Starting to process updated posture requirements received from the remote feed URL

  Local Target Message Format: <timestamp> <seq_num> 60163 DEBUG System-Management: Processing the updated Posture requirements received from the remote feed URL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60163 DEBUG System-Management: Processing the updated Posture requirements received from the remote feed URL, <log details>

- **Message Code:** 60164

  Severity: ERROR

  Message Text: NTP Service is down on the node

  Message Description: NTP Service is down on the node

  Local Target Message Format: <timestamp> <seq_num> 60164 ERROR System-Management: NTP Service is down on the node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60164 ERROR System-Management: NTP Service is down on the node, <log details>

- **Message Code:** 60165

  Severity: ERROR

Message Text: NTP failed to sync with configured servers

Message Description: NTP failed to sync with the configured servers

Local Target Message Format: <timestamp> <seq_num> 60165 ERROR System-Management: NTP failed to sync with configured servers, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60165 ERROR System-Management: NTP failed to sync with configured servers, <log details>

- **Message Code:** 60166

  Severity: WARN

  Message Text: Certificate will expire soon

  Message Description: Certificate Expiration warning

  Local Target Message Format: <timestamp> <seq_num> 60166 WARN Certificate: Certificate will expire soon, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60166 WARN Certificate: Certificate will expire soon, <log details>

- **Message Code:** 60167

  Severity: WARN

  Message Text: Certificate has expired

  Message Description: Certificate has expired

  Local Target Message Format: <timestamp> <seq_num> 60167 WARN Certificate: Certificate has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60167 WARN Certificate: Certificate has expired, <log details>

- **Message Code:** 60168

  Severity: INFO

  Message Text: Session Repeat Count has reset successfully

  Message Description: Session Repeat Count has reset successfully

  Local Target Message Format: <timestamp> <seq_num> 60168 INFO System-Management: Session Repeat Count has reset successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60168 INFO System-Management: Session Repeat Count has reset successfully, <log details>

- **Message Code:** 60169

  Severity: INFO

  Message Text: Session Repeat Count reset has failed

Message Description: Session Repeat Count reset has failed

Local Target Message Format: <timestamp> <seq_num> 60169 INFO System-Management: Session Repeat Count reset has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60169 INFO System-Management: Session Repeat Count reset has failed, <log details>

- **Message Code:** 60170

  Severity: INFO

  Message Text: Resetting Repeat Count is successful for all sessions

  Message Description: Resetting Repeat Count is successful for all sessions

  Local Target Message Format: <timestamp> <seq_num> 60170 INFO System-Management: Resetting Repeat Count is successful for all sessions, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60170 INFO System-Management: Resetting Repeat Count is successful for all sessions, <log details>

- **Message Code:** 60171

  Severity: INFO

  Message Text: Resetting Repeat Count has failed for all sessions

  Message Description: Resetting Repeat Count has failed for all sessions

  Local Target Message Format: <timestamp> <seq_num> 60171 INFO System-Management: Resetting Repeat Count has failed for all sessions, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60171 INFO System-Management: Resetting Repeat Count has failed for all sessions, <log details>

- **Message Code:** 60172

  Severity: INFO

  Message Text: Alarm(s) has/have been acknowledged

  Message Description: These alarms are acknowledged and will not be displayed on the Dashboard

  Local Target Message Format: <timestamp> <seq_num> 60172 INFO System-Management: Alarm(s) has/have been acknowledged, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60172 INFO System-Management: Alarm(s) has/have been acknowledged, <log details>

- **Message Code:** 60173

  Severity: INFO

  Message Text: Outdated alarms are purged

  Message Description: Only latest 15000 alarms would be retained and rest of them are purged

Local Target Message Format: <timestamp> <seq_num> 60173 INFO System-Management: Outdated alarms are purged, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60173 INFO System-Management: Outdated alarms are purged, <log details>

- **Message Code:** 60174

  Severity: ERROR

  Message Text: Could not add Certificate Revocation List

  Message Description: Could not add Certificate Revocation List. The Certificate Revocation List will not be used by ISE

  Local Target Message Format: <timestamp> <seq_num> 60174 ERROR CRL: Could not add Certificate Revocation List, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60174 ERROR CRL: Could not add Certificate Revocation List, <log details>

- **Message Code:** 60175

  Severity: ERROR

  Message Text: Could not download Certificate Revocation List

  Message Description: Could not download Certificate Revocation List. The Certificate Revocation List will not be used by ISE

  Local Target Message Format: <timestamp> <seq_num> 60175 ERROR CRL: Could not download Certificate Revocation List, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60175 ERROR CRL: Could not download Certificate Revocation List, <log details>

- **Message Code:** 60176

  Severity: INFO

  Message Text: Posture Update

  Message Description: Posture Update

  Local Target Message Format: <timestamp> <seq_num> 60176 INFO System-Management: Posture Update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60176 INFO System-Management: Posture Update, <log details>

- **Message Code:** 60177

  Severity: ERROR

  Message Text: Application upgrade preparation failed

  Message Description: Application upgrade preparation failed

Local Target Message Format: <timestamp> <seq_num> 60177 ERROR System-Management: Application upgrade preparation failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60177 ERROR System-Management: Application upgrade preparation failed, <log details>

- **Message Code:** 60178

  Severity: INFO

  Message Text: Application upgrade preparation successful

  Message Description: Application upgrade preparation successful

  Local Target Message Format: <timestamp> <seq_num> 60178 INFO System-Management: Application upgrade preparation successful, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60178 INFO System-Management: Application upgrade preparation successful, <log details>

- **Message Code:** 60179

  Severity: INFO

  Message Text: Application upgrade preparation started

  Message Description: Application upgrade preparation started

  Local Target Message Format: <timestamp> <seq_num> 60179 INFO System-Management: Application upgrade preparation started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60179 INFO System-Management: Application upgrade preparation started, <log details>

- **Message Code:** 60180

  Severity: WARN

  Message Text: Syslog server Identity check failed

  Message Description: Syslog server Identity check failed, Secure communication not established with syslog server

  Local Target Message Format: <timestamp> <seq_num> 60180 WARN System-Management: Syslog server Identity check failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60180 WARN System-Management: Syslog server Identity check failed, <log details>

- **Message Code:** 60184

  Severity: INFO

  Message Text: A console CLI user has successfully logged in

  Message Description: A console CLI User has successfully logged in

Local Target Message Format: <timestamp> <seq_num> 60184 INFO Administrator-Login: A console CLI user has successfully logged in, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60184 INFO Administrator-Login: A console CLI user has successfully logged in, <log details>

- **Message Code:** 60185

  Severity: INFO

  Message Text: A console CLI user has attempted unsuccessfully to login

  Message Description: A console CLI user has attempted unsuccessfully to login

  Local Target Message Format: <timestamp> <seq_num> 60185 INFO Administrator-Login: A console CLI user has attempted unsuccessfully to login, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60185 INFO Administrator-Login: A console CLI user has attempted unsuccessfully to login, <log details>

- **Message Code:** 60186

  Severity: INFO

  Message Text: A console CLI user has attempted to login, however account is locked out

  Message Description: A console CLI user has attempted to login, however account is locked out

  Local Target Message Format: <timestamp> <seq_num> 60186 INFO Administrator-Login: A console CLI user has attempted to login, however account is locked out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60186 INFO Administrator-Login: A console CLI user has attempted to login, however account is locked out, <log details>

- **Message Code:** 60187

  Severity: INFO

  Message Text: Application upgrade succeeded

  Message Description: Application upgrade succeeded

  Local Target Message Format: <timestamp> <seq_num> 60187 INFO System-Management: Application upgrade succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60187 INFO System-Management: Application upgrade succeeded, <log details>

- **Message Code:** 60188

  Severity: INFO

  Message Text: An attempted SSH connection has failed

  Message Description: An attempted SSH connection has failed

Local Target Message Format: <timestamp> <seq_num> 60188 INFO Administrator-Login: An attempted SSH connection has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60188 INFO Administrator-Login: An attempted SSH connection has failed, <log details>

- **Message Code:** 60189

  Severity: INFO

  Message Text: Terminal Session timeout has been modified

  Message Description: Configuration change occurred for ADEOS CLI Terminal Session timeout

  Local Target Message Format: <timestamp> <seq_num> 60189 INFO System-Management: Terminal Session timeout has been modified, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60189 INFO System-Management: Terminal Session timeout has been modified, <log details>

- **Message Code:** 60190

  Severity: INFO

  Message Text: xGrid Administrator Action

  Message Description: xGrid Administrator Action

  Local Target Message Format: <timestamp> <seq_num> 60190 INFO System-Management: xGrid Administrator Action, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60190 INFO System-Management: xGrid Administrator Action, <log details>

- **Message Code:** 60191

  Severity: ERROR

  Message Text: Insufficient Virtual Machine Resources on node

  Message Description: Insufficient Virtual Machine Resources on node

  Local Target Message Format: <timestamp> <seq_num> 60191 ERROR System-Management: Insufficient Virtual Machine Resources on node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60191 ERROR System-Management: Insufficient Virtual Machine Resources on node, <log details>

- **Message Code:** 60192

  Severity: ERROR

  Message Text: Firmware update required on node

  Message Description: Firmware update required on node

Local Target Message Format: <timestamp> <seq_num> 60192 ERROR System-Management: Firmware update required on node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60192 ERROR System-Management: Firmware update required on node, <log details>

- **Message Code:** 60193

  Severity: INFO

  Message Text: RSA key configuration has been modified

  Message Description: Configuration change occurred for ADEOS CLI RSA key

  Local Target Message Format: <timestamp> <seq_num> 60193 INFO System-Management: RSA key configuration has been modified, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60193 INFO System-Management: RSA key configuration has been modified, <log details>

- **Message Code:** 60194

  Severity: INFO

  Message Text: Host key configuration has been modified

  Message Description: Configuration change occurred for ADEOS CLI host key

  Local Target Message Format: <timestamp> <seq_num> 60194 INFO System-Management: Host key configuration has been modified, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60194 INFO System-Management: Host key configuration has been modified, <log details>

- **Message Code:** 60195

  Severity: INFO

  Message Text: CA Service started

  Message Description: CA Service started

  Local Target Message Format: <timestamp> <seq_num> 60195 INFO CA-Service: CA Service started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60195 INFO CA-Service: CA Service started, <log details>

- **Message Code:** 60196

  Severity: INFO

  Message Text: CA Service stopped

  Message Description: CA Service stopped

Local Target Message Format: <timestamp> <seq_num> 60196 INFO CA-Service: CA Service stopped, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60196 INFO CA-Service: CA Service stopped, <log details>

- **Message Code:** 60197

  Severity: NOTICE

  Message Text: Revoked ISE CA issued Certificate.

  Message Description: Certificate issued to Endpoint by ISE CA is revoked by Administrator

  Local Target Message Format: <timestamp> <seq_num> 60197 NOTICE CA-Service: Revoked ISE CA issued Certificate., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60197 NOTICE CA-Service: Revoked ISE CA issued Certificate., <log details>

- **Message Code:** 60198

  Severity: INFO

  Message Text: MnT purge event occurred

  Message Description: MnT purge event occurred

  Local Target Message Format: <timestamp> <seq_num> 60198 INFO System-Management: MnT purge event occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60198 INFO System-Management: MnT purge event occurred, <log details>

- **Message Code:** 60199

  Severity: INFO

  Message Text: An IP-SGT mapping was deployed successfully

  Message Description: An IP-SGT mapping was deployed successfully to a TrustSec device

  Local Target Message Format: <timestamp> <seq_num> 60199 INFO TrustSec: An IP-SGT mapping was deployed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60199 INFO TrustSec: An IP-SGT mapping was deployed successfully, <log details>

- **Message Code:** 60200

  Severity: INFO

  Message Text: An IP-SGT mapping has failed deploying

  Message Description: An IP-SGT mapping has failed deploying to a TrustSec device

Local Target Message Format: <timestamp> <seq_num> 60200 INFO TrustSec: An IP-SGT mapping has failed deploying, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60200 INFO TrustSec: An IP-SGT mapping has failed deploying, <log details>

- **Message Code:** 60201

  Severity: INFO

  Message Text: IP-SGT deployment to TrustSec device was successful

  Message Description: IP-SGT deployment to TrustSec device was successful

  Local Target Message Format: <timestamp> <seq_num> 60201 INFO TrustSec: IP-SGT deployment to TrustSec device was successful, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60201 INFO TrustSec: IP-SGT deployment to TrustSec device was successful, <log details>

- **Message Code:** 60202

  Severity: INFO

  Message Text: IP-SGT deployment to TrustSec device failed

  Message Description: IP-SGT deployment to TrustSec device failed

  Local Target Message Format: <timestamp> <seq_num> 60202 INFO TrustSec: IP-SGT deployment to TrustSec device failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60202 INFO TrustSec: IP-SGT deployment to TrustSec device failed, <log details>

- **Message Code:** 60203

  Severity: INFO

  Message Text: IP-SGT deployment to the TrustSec devices finished

  Message Description: IP-SGT deployment to the TrustSec devices finished

  Local Target Message Format: <timestamp> <seq_num> 60203 INFO TrustSec: IP-SGT deployment to the TrustSec devices finished, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60203 INFO TrustSec: IP-SGT deployment to the TrustSec devices finished, <log details>

- **Message Code:** 60204

  Severity: INFO

  Message Text: System root CLI account has successfully logged in

  Message Description: System root CLI account has successfully logged in

Local Target Message Format: <timestamp> <seq_num> 60204 INFO System-Management: System root CLI account has successfully logged in, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60204 INFO System-Management: System root CLI account has successfully logged in, <log details>

- **Message Code:** 60205

  Severity: INFO

  Message Text: A CLI user has logged in from console

  Message Description: A CLI user has logged in from console

  Local Target Message Format: <timestamp> <seq_num> 60205 INFO Administrator-Login: A CLI user has logged in from console, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60205 INFO Administrator-Login: A CLI user has logged in from console, <log details>

- **Message Code:** 60206

  Severity: INFO

  Message Text: A CLI user has logged out from console

  Message Description: A CLI user has logged out from console

  Local Target Message Format: <timestamp> <seq_num> 60206 INFO Administrator-Login: A CLI user has logged out from console, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60206 INFO Administrator-Login: A CLI user has logged out from console, <log details>

- **Message Code:** 60207

  Severity: INFO

  Message Text: logging loglevel configuration has been modified

  Message Description: Configuration change occurred for ADEOS CLI logging loglevel

  Local Target Message Format: <timestamp> <seq_num> 60207 INFO System-Management: logging loglevel configuration has been modified, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60207 INFO System-Management: logging loglevel configuration has been modified, <log details>

- **Message Code:** 60208

  Severity: INFO

  Message Text: Root CA certificate has been replaced

  Message Description: Root CA certificate has been replaced

Local Target Message Format: <timestamp> <seq_num> 60208 INFO System-Management: Root CA certificate has been replaced, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60208 INFO System-Management: Root CA certificate has been replaced, <log details>

- **Message Code:** 60209

  Severity: INFO

  Message Text: CA service enabled

  Message Description: CA service enabled

  Local Target Message Format: <timestamp> <seq_num> 60209 INFO System-Management: CA service enabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60209 INFO System-Management: CA service enabled, <log details>

- **Message Code:** 60210

  Severity: INFO

  Message Text: CA service disabled

  Message Description: CA service disabled

  Local Target Message Format: <timestamp> <seq_num> 60210 INFO System-Management: CA service disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60210 INFO System-Management: CA service disabled, <log details>

- **Message Code:** 60211

  Severity: INFO

  Message Text: ISE acquired subordinate certificate authority from 3rd party CA server

  Message Description: ISE acquired subordinate certificate authority from 3rd party CA server

  Local Target Message Format: <timestamp> <seq_num> 60211 INFO System-Management: ISE acquired subordinate certificate authority from 3rd party CA server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60211 INFO System-Management: ISE acquired subordinate certificate authority from 3rd party CA server, <log details>

- **Message Code:** 60212

  Severity: WARNING

  Message Text: Portal could not start on this node since Certificate tag is missing

  Message Description: Portal could not start on this node since Certificate tag is missing

Local Target Message Format: <timestamp> <seq_num> 60212 WARNING System-Management: Portal could not start on this node since Certificate tag is missing, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60212 WARNING System-Management: Portal could not start on this node since Certificate tag is missing, <log details>

- **Message Code:** 60213

  Severity: INFO

  Message Text: CA keys were replaced by import operation

  Message Description: CA keys were replaced by import operation

  Local Target Message Format: <timestamp> <seq_num> 60213 INFO System-Management: CA keys were replaced by import operation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60213 INFO System-Management: CA keys were replaced by import operation, <log details>

- **Message Code:** 60214

  Severity: INFO

  Message Text: CA keys were exported

  Message Description: CA keys were exported

  Local Target Message Format: <timestamp> <seq_num> 60214 INFO System-Management: CA keys were exported, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60214 INFO System-Management: CA keys were exported, <log details>

- **Message Code:** 60215

  Severity: INFO

  Message Text: Endpoint certs were marked expired

  Message Description: Endpoint certs were marked expired by daily scheduled job

  Local Target Message Format: <timestamp> <seq_num> 60215 INFO CA-Service: Endpoint certs were marked expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60215 INFO CA-Service: Endpoint certs were marked expired, <log details>

- **Message Code:** 60216

  Severity: INFO

  Message Text: Endpoint certs were purged

  Message Description: Endpoint certs were purged by daily scheduled job

Local Target Message Format: <timestamp> <seq_num> 60216 INFO CA-Service: Endpoint certs were purged, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60216 INFO CA-Service: Endpoint certs were purged, <log details>

- **Message Code:** 60217

  Severity: WARN

  Message Text: Certificate replication failed and will be retried

  Message Description: The PAP failed to push a replicated certificate, such as a wildcard certificate, to a secondary node

  Local Target Message Format: <timestamp> <seq_num> 60217 WARN Replication: Certificate replication failed and will be retried, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60217 WARN Replication: Certificate replication failed and will be retried, <log details>

- **Message Code:** 60218

  Severity: WARN

  Message Text: Certificate replication failed

  Message Description: The PAP failed to push a replicated certificate, such as a wildcard certificate, to a secondary node

  Local Target Message Format: <timestamp> <seq_num> 60218 WARN Replication: Certificate replication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60218 WARN Replication: Certificate replication failed, <log details>

- **Message Code:** 60219

  Severity: WARN

  Message Text: Administration Node has not received any PAN HA monitoring request from monitoring node

  Message Description: Administration Node has not received any PAN HA monitoring request from monitoring node

  Local Target Message Format: <timestamp> <seq_num> 60219 WARN Distributed-Management: Administration Node has not received any PAN HA monitoring request from monitoring node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60219 WARN Distributed-Management: Administration Node has not received any PAN HA monitoring request from monitoring node, <log details>

- **Message Code:** 60221

Severity: WARN

Message Text: Misconfiguration in PAN HA monitoring

Message Description: Misconfiguration in PAN HA monitoring

Local Target Message Format: <timestamp> <seq_num> 60221 WARN Distributed-Management: Misconfiguration in PAN HA monitoring, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60221 WARN Distributed-Management: Misconfiguration in PAN HA monitoring, <log details>

- **Message Code:** 60222

  Severity: WARN

  Message Text: PAN is not reachable or unhealthy

  Message Description: PAN is not reachable or unhealthy

  Local Target Message Format: <timestamp> <seq_num> 60222 WARN Distributed-Management: PAN is not reachable or unhealthy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60222 WARN Distributed-Management: PAN is not reachable or unhealthy, <log details>

- **Message Code:** 60223

  Severity: ERROR

  Message Text: PAN HA Promotion request failed

  Message Description: PAN HA Promotion request failed

  Local Target Message Format: <timestamp> <seq_num> 60223 ERROR Distributed-Management: PAN HA Promotion request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60223 ERROR Distributed-Management: PAN HA Promotion request failed, <log details>

- **Message Code:** 60224

  Severity: INFO

  Message Text: Automatic failover to the Secondary PAN is successfully triggered

  Message Description: Automatic failover to the Secondary PAN is successfully triggered

  Local Target Message Format: <timestamp> <seq_num> 60224 INFO Distributed-Management: Automatic failover to the Secondary PAN is successfully triggered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60224 INFO Distributed-Management: Automatic failover to the Secondary PAN is successfully triggered, <log details>

- **Message Code:** 60225

Severity: ERROR

Message Text: Unable to build the certificate chain

Message Description: Two or more certificates have been found with same value of CN attribute in the subject field leading to certificate chain building error

Local Target Message Format: <timestamp> <seq_num> 60225 ERROR Client Provisioning: Unable to build the certificate chain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60225 ERROR Client Provisioning: Unable to build the certificate chain, <log details>

- **Message Code:** 60226

  Severity: INFO

  Message Text: Successfully performed CoA termination(s) for a user certificate being revoked

  Message Description: Successfully performed CoA termination(s) for a user certificate being revoked

  Local Target Message Format: <timestamp> <seq_num> 60226 INFO Certificate: Successfully performed CoA termination(s) for a user certificate being revoked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60226 INFO Certificate: Successfully performed CoA termination(s) for a user certificate being revoked, <log details>

- **Message Code:** 60227

  Severity: INFO

  Message Text: Failed to perform a CoA termination

  Message Description: Please make sure that the NAD is configured to send the client MAC Address when making RADIUS access-requests to ISE

  Local Target Message Format: <timestamp> <seq_num> 60227 INFO Certificate: Failed to perform a CoA termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60227 INFO Certificate: Failed to perform a CoA termination, <log details>

- **Message Code:** 60228

  Severity: ERROR

  Message Text: MSE Server is unreachable

  Message Description: MSE Server is unreachable

  Local Target Message Format: <timestamp> <seq_num> 60228 ERROR System-Management: MSE Server is unreachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60228 ERROR System-Management: MSE Server is unreachable, <log details>

- **Message Code:** 60229

Severity: INFO

Message Text: MSE Server is back online

Message Description: MSE Server is back online

Local Target Message Format: <timestamp> <seq_num> 60229 INFO System-Management: MSE Server is back online, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60229 INFO System-Management: MSE Server is back online, <log details>

- **Message Code:** 60231

  Severity: INFO

  Message Text: Queried MSE server

  Message Description: MSE server was queried to get endpoint location

  Local Target Message Format: <timestamp> <seq_num> 60231 INFO System-Management: Queried MSE server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60231 INFO System-Management: Queried MSE server, <log details>

- **Message Code:** 60232

  Severity: INFO

  Message Text: Started ongoing sessions check against automatically retrieved CRL

  Message Description: Started all ongoing TLS sessions check as soon as the CRL is downloaded.

  Local Target Message Format: <timestamp> <seq_num> 60232 INFO System-Management: Started ongoing sessions check against automatically retrieved CRL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60232 INFO System-Management: Started ongoing sessions check against automatically retrieved CRL, <log details>

- **Message Code:** 60233

  Severity: INFO

  Message Text: The endpoint session is terminated due to the revoked certificate

  Message Description: The endpoint session is terminated due to the revoked endpoint certificate, following the ongoing sessions check against downloaded CRL

  Local Target Message Format: <timestamp> <seq_num> 60233 INFO Dynamic-Authorization: The endpoint session is terminated due to the revoked certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60233 INFO Dynamic-Authorization: The endpoint session is terminated due to the revoked certificate, <log details>

- **Message Code:** 60234

Severity: ERROR

Message Text: The SXP connection has been disconnected

Message Description: The SXP connection has been disconnected

Local Target Message Format: <timestamp> <seq_num> 60234 ERROR Sxp: The SXP connection has been disconnected, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60234 ERROR Sxp: The SXP connection has been disconnected, <log details>

- **Message Code:** 60235

  Severity: INFO

  Message Text: SXP connection succeeded

  Message Description: SXP connection succeeded

  Local Target Message Format: <timestamp> <seq_num> 60235 INFO SXP: SXP connection succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60235 INFO SXP: SXP connection succeeded, <log details>

- **Message Code:** 60236

  Severity: WARN

  Message Text: SXP connection failed

  Message Description: SXP connection failed

  Local Target Message Format: <timestamp> <seq_num> 60236 WARN SXP: SXP connection failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60236 WARN SXP: SXP connection failed, <log details>

- **Message Code:** 60237

  Severity: INFO

  Message Text: SXP binding is successful

  Message Description: SXP binding is successful

  Local Target Message Format: <timestamp> <seq_num> 60237 INFO SXP: SXP binding is successful, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60237 INFO SXP: SXP binding is successful, <log details>

- **Message Code:** 60238

  Severity: INFO

Message Text: SXP binding failed

Message Description: SXP binding failed

Local Target Message Format: <timestamp> <seq_num> 60238 INFO SXP: SXP binding failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60238 INFO SXP: SXP binding failed, <log details>

- **Message Code:** 60239

  Severity: WARN

  Message Text: SXP binding conflict has occurred

  Message Description: SXP binding conflict has occurred

  Local Target Message Format: <timestamp> <seq_num> 60239 WARN SXP: SXP binding conflict has occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60239 WARN SXP: SXP binding conflict has occurred, <log details>

- **Message Code:** 60400

  Severity: INFO

  Message Text: Policy elements have been generated based on network device profile configuration.

  Message Description: Policy elements have been generated based on network device profile configuration.

  Local Target Message Format: <timestamp> <seq_num> 60400 INFO Configuration-Changes: Policy elements have been generated based on network device profile configuration., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60400 INFO Configuration-Changes: Policy elements have been generated based on network device profile configuration., <log details>

- **Message Code:** 60401

  Severity: INFO

  Message Text: Reminder: Assign NAD Profiles.

  Message Description: Network Access Devices now have a NAD Profile which defines their capabilities. All existing devices have been assigned a default Cisco NAD Profile which should be changed for non-Cisco devices.

  Local Target Message Format: <timestamp> <seq_num> 60401 INFO Configuration-Changes: Reminder: Assign NAD Profiles., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60401 INFO Configuration-Changes: Reminder: Assign NAD Profiles., <log details>

- **Message Code:** 60451

Severity: INFO

Message Text: Telemetry is enabled on this deployment

Message Description: Telemetry is enabled on this deployment

Local Target Message Format: <timestamp> <seq_num> 60451 INFO System-Management: Telemetry is enabled on this deployment, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60451 INFO System-Management: Telemetry is enabled on this deployment, <log details>

- **Message Code:** 60452

  Severity: INFO

  Message Text: Telemetry is disabled on this deployment

  Message Description: Telemetry is disabled on this deployment

  Local Target Message Format: <timestamp> <seq_num> 60452 INFO System-Management: Telemetry is disabled on this deployment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60452 INFO System-Management: Telemetry is disabled on this deployment, <log details>

- **Message Code:** 60453

  Severity: INFO

  Message Text: Telemetry messages were sent successfully

  Message Description: Telemetry messages were sent successfully

  Local Target Message Format: <timestamp> <seq_num> 60453 INFO System-Management: Telemetry messages were sent successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60453 INFO System-Management: Telemetry messages were sent successfully, <log details>

- **Message Code:** 60454

  Severity: INFO

  Message Text: Telemetry messages were not sent successfully

  Message Description: Telemetry messages were not sent successfully

  Local Target Message Format: <timestamp> <seq_num> 60454 INFO System-Management: Telemetry messages were not sent successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60454 INFO System-Management: Telemetry messages were not sent successfully, <log details>

- **Message Code:** 60501

  Severity: WARN

Message Text: ERS xml input is a suspect for XSS or Injection attack

Message Description: Please review your xml input

Local Target Message Format: <timestamp> <seq_num> 60501 WARN ERS: ERS xml input is a suspect for XSS or Injection attack, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60501 WARN ERS: ERS xml input is a suspect for XSS or Injection attack, <log details>

- **Message Code:** 60502

  Severity: WARN

  Message Text: ERS identified deprecated url

  Message Description: The request url is deprecated and recommended avoid using it

  Local Target Message Format: <timestamp> <seq_num> 60502 WARN ERS: ERS identified deprecated url, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60502 WARN ERS: ERS identified deprecated url, <log details>

- **Message Code:** 60503

  Severity: WARN

  Message Text: ERS identified out-dated url

  Message Description: the request url is out-dated and recommended to use a newer one. This url will not be removed in future releases

  Local Target Message Format: <timestamp> <seq_num> 60503 WARN ERS: ERS identified out-dated url, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60503 WARN ERS: ERS identified out-dated url, <log details>

- **Message Code:** 60504

  Severity: WARN

  Message Text: ERS request content-type header is out-dated

  Message Description: The request resource version stated in the request content-type header is out-dated. That means that the resource schema has been modified. one or more attribute might been added or removed and to overcome that with out-dated schema, the ERS Engine will use default values

  Local Target Message Format: <timestamp> <seq_num> 60504 WARN ERS: ERS request content-type header is out-dated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60504 WARN ERS: ERS request content-type header is out-dated, <log details>

- **Message Code:** 11319

Severity: WARN

Message Text: TrustSec works only with TLS 1.0

Message Description: TrustSec works only with TLS1.0, if you plan to use TrustSec, make sure it is enabled

Local Target Message Format: <timestamp> <seq_num> 11319 WARN TrustSec: TrustSec works only with TLS 1.0, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11319 WARN TrustSec: TrustSec works only with TLS 1.0, <log details>

- **Message Code:** 60455

  Severity: INFO

  Message Text: Easy Wired is selected on Allowed Protocol but Identity Mapping has NOT been activated

  Message Description: Easy Wired is selected on Allowed Protocol but Identity Mapping has NOT been activated

  Local Target Message Format: <timestamp> <seq_num> 60455 INFO System-Management: Easy Wired is selected on Allowed Protocol but Identity Mapping has NOT been activated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60455 INFO System-Management: Easy Wired is selected on Allowed Protocol but Identity Mapping has NOT been activated, <log details>

- **Message Code:** 60456

  Severity: INFO

  Message Text: Started CRL/OCSP periodic certificate check

  Message Description: Started CRL/OCSP periodic certificate check

  Local Target Message Format: <timestamp> <seq_num> 60456 INFO System-Management: Started CRL/OCSP periodic certificate check, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60456 INFO System-Management: Started CRL/OCSP periodic certificate check, <log details>

- **Message Code:** 60457

  Severity: INFO

  Message Text: Authentication Type Method for Admin UI Access

  Message Description: Successful message for Authentication Type Method Configuration update

  Local Target Message Format: <timestamp> <seq_num> 60457 INFO Admin Access Authentication Method: Authentication Type Method for Admin UI Access, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60457 INFO Admin Access Authentication Method: Authentication Type Method for Admin UI Access, <log details>

- **Message Code:** 60458

Severity: INFO

Message Text: Authentication Type Method for Admin UI Access

Message Description: Unsuccessful message for Authentication Type Method Configuration update

Local Target Message Format: <timestamp> <seq_num> 60458 INFO Admin Access Authentication Method: Authentication Type Method for Admin UI Access, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60458 INFO Admin Access Authentication Method: Authentication Type Method for Admin UI Access, <log details>

- **Message Code:** 60459

  Severity: ERROR

  Message Text: SXP binding binding not propagated because binding threshold has been reached

  Message Description: SXP binding threshold reached

  Local Target Message Format: <timestamp> <seq_num> 60459 ERROR SXP: SXP binding binding not propagated because binding threshold has been reached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60459 ERROR SXP: SXP binding binding not propagated because binding threshold has been reached, <log details>

- **Message Code:** 60460

  Severity: INFO

  Message Text: Account disabled due to inactivity

  Message Description: Account disabled due to inactivity

  Local Target Message Format: <timestamp> <seq_num> 60460 INFO System-Management: Account disabled due to inactivity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60460 INFO System-Management: Account disabled due to inactivity, <log details>

- **Message Code:** 60461

  Severity: INFO

  Message Text: Account disabled due to user level date expiry

  Message Description: Account disabled due to user level date expiry

  Local Target Message Format: <timestamp> <seq_num> 60461 INFO System-Management: Account disabled due to user level date expiry, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60461 INFO System-Management: Account disabled due to user level date expiry, <log details>

- **Message Code:** 60462

  Severity: INFO

Message Text: Account disabled due to global level date expiry

Message Description: Account disabled due to global level date expiry

Local Target Message Format: <timestamp> <seq_num> 60462 INFO System-Management: Account disabled due to global level date expiry, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60462 INFO System-Management: Account disabled due to global level date expiry, <log details>

- **Message Code:** 60463

  Severity: INFO

  Message Text: Account disabled due to global level days expiry

  Message Description: Account disabled due to global level days expiry

  Local Target Message Format: <timestamp> <seq_num> 60463 INFO System-Management: Account disabled due to global level days expiry, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60463 INFO System-Management: Account disabled due to global level days expiry, <log details>

- **Message Code:** 60464

  Severity: INFO

  Message Text: Smart Call Home messages were sent successfully

  Message Description: Smart Call Home messages were sent successfully

  Local Target Message Format: <timestamp> <seq_num> 60464 INFO System-Management: Smart Call Home messages were sent successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60464 INFO System-Management: Smart Call Home messages were sent successfully, <log details>

- **Message Code:** 60465

  Severity: INFO

  Message Text: Smart Call Home messages were not sent successfully

  Message Description: Smart Call Home messages were not sent successfully

  Local Target Message Format: <timestamp> <seq_num> 60465 INFO System-Management: Smart Call Home messages were not sent successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 60465 INFO System-Management: Smart Call Home messages were not sent successfully, <log details>

- **Message Code:** 61001

  Severity: INFO

  Message Text: APIC self signed Certificate was used

Message Description: Self signed Certificate was used ? ISE verified APIC using a self signed certificate.

Local Target Message Format: <timestamp> <seq_num> 61001 INFO TrustSec: APIC self signed Certificate was used, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61001 INFO TrustSec: APIC self signed Certificate was used, <log details>

- **Message Code:** 61002

  Severity: INFO

  Message Text: ISE has learned a new SGT from IEPG

  Message Description: ISE has learned a new SGT from IEPG

  Local Target Message Format: <timestamp> <seq_num> 61002 INFO TrustSec: ISE has learned a new SGT from IEPG, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61002 INFO TrustSec: ISE has learned a new SGT from IEPG, <log details>

- **Message Code:** 61003

  Severity: INFO

  Message Text: ISE has propagated a new EEPG to APIC

  Message Description: ISE has propagated a new EEPG to APIC.

  Local Target Message Format: <timestamp> <seq_num> 61003 INFO TrustSec: ISE has propagated a new EEPG to APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61003 INFO TrustSec: ISE has propagated a new EEPG to APIC, <log details>

- **Message Code:** 61004

  Severity: INFO

  Message Text: ISE has learned a new SXP mapping from APIC endpoint

  Message Description: ISE has learned a new SXP mapping from APIC endpoint

  Local Target Message Format: <timestamp> <seq_num> 61004 INFO TrustSec: ISE has learned a new SXP mapping from APIC endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61004 INFO TrustSec: ISE has learned a new SXP mapping from APIC endpoint, <log details>

- **Message Code:** 61005

  Severity: INFO

  Message Text: ISE has propagated a new endpoint(SXP mapping) to APIC

  Message Description: ISE has propagated a new endpoint(SXP mapping) to APIC

Local Target Message Format: <timestamp> <seq_num> 61005 INFO TrustSec: ISE has propagated a new endpoint(SXP mapping) to APIC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61005 INFO TrustSec: ISE has propagated a new endpoint(SXP mapping) to APIC, <log details>

- **Message Code:** 61006

  Severity: INFO

  Message Text: ISE has removed an SGT due to deleted IEPG

  Message Description: ISE has removed an SGT due to deleted IEPG

  Local Target Message Format: <timestamp> <seq_num> 61006 INFO TrustSec: ISE has removed an SGT due to deleted IEPG, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61006 INFO TrustSec: ISE has removed an SGT due to deleted IEPG, <log details>

- **Message Code:** 61007

  Severity: INFO

  Message Text: ISE has removed EEPG from APIC due to SGT deletion

  Message Description: ISE has removed EEPG from APIC due to SGT deletion

  Local Target Message Format: <timestamp> <seq_num> 61007 INFO TrustSec: ISE has removed EEPG from APIC due to SGT deletion, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61007 INFO TrustSec: ISE has removed EEPG from APIC due to SGT deletion, <log details>

- **Message Code:** 61008

  Severity: INFO

  Message Text: ISE has removed an SXP mapping due to endpoint deletion on APIC

  Message Description: ISE has removed an SXP mapping due to endpoint deletion on APIC

  Local Target Message Format: <timestamp> <seq_num> 61008 INFO TrustSec: ISE has removed an SXP mapping due to endpoint deletion on APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61008 INFO TrustSec: ISE has removed an SXP mapping due to endpoint deletion on APIC, <log details>

- **Message Code:** 61009

  Severity: INFO

  Message Text: ISE has removed endpoint APIC due to SXP mapping removal a new SXP mapping to APIC

  Message Description: ISE has removed endpoint APIC due to SXP mapping removal a new SXP mapping to APIC

Local Target Message Format: <timestamp> <seq_num> 61009 INFO TrustSec: ISE has removed endpoint APIC due to SXP mapping removal a new SXP mapping to APIC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61009 INFO TrustSec: ISE has removed endpoint APIC due to SXP mapping removal a new SXP mapping to APIC, <log details>

- **Message Code:** 61010

  Severity: INFO

  Message Text: ISE has established connection to APIC

  Message Description: ISE has established connection to APIC

  Local Target Message Format: <timestamp> <seq_num> 61010 INFO TrustSec: ISE has established connection to APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61010 INFO TrustSec: ISE has established connection to APIC, <log details>

- **Message Code:** 61011

  Severity: INFO

  Message Text: ISE was disconnected from APIC

  Message Description: ISE was disconnected from APIC

  Local Target Message Format: <timestamp> <seq_num> 61011 INFO TrustSec: ISE was disconnected from APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61011 INFO TrustSec: ISE was disconnected from APIC, <log details>

- **Message Code:** 61012

  Severity: INFO

  Message Text: ISE has authenticated against APIC successfully

  Message Description: ISE has authenticated against APIC successfully

  Local Target Message Format: <timestamp> <seq_num> 61012 INFO TrustSec: ISE has authenticated against APIC successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61012 INFO TrustSec: ISE has authenticated against APIC successfully, <log details>

- **Message Code:** 61013

  Severity: INFO

  Message Text: ISE failed to authenticate against APIC

  Message Description: ISE failed to authenticate against APIC

Local Target Message Format: <timestamp> <seq_num> 61013 INFO TrustSec: ISE failed to authenticate against APIC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61013 INFO TrustSec: ISE failed to authenticate against APIC, <log details>

- **Message Code:** 61014

  Severity: INFO

  Message Text: ISE has refreshed authentication against APIC successfully

  Message Description: ISE has refreshed authentication against APIC successfully

  Local Target Message Format: <timestamp> <seq_num> 61014 INFO TrustSec: ISE has refreshed authentication against APIC successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61014 INFO TrustSec: ISE has refreshed authentication against APIC successfully, <log details>

- **Message Code:** 61015

  Severity: INFO

  Message Text: ISE failed to refresh authenticate against APIC

  Message Description: ISE failed to refresh authenticate against APIC

  Local Target Message Format: <timestamp> <seq_num> 61015 INFO TrustSec: ISE failed to refresh authenticate against APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61015 INFO TrustSec: ISE failed to refresh authenticate against APIC, <log details>

- **Message Code:** 61016

  Severity: INFO

  Message Text: ISE failed to refresh EPG subscriber against APIC

  Message Description: ISE failed to refresh EPG subscriber against APIC

  Local Target Message Format: <timestamp> <seq_num> 61016 INFO TrustSec: ISE failed to refresh EPG subscriber against APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61016 INFO TrustSec: ISE failed to refresh EPG subscriber against APIC, <log details>

- **Message Code:** 61017

  Severity: INFO

  Message Text: ISE failed to refresh endpoint subscriber against APIC

  Message Description: ISE failed to refresh endpoint subscriber against APIC

Local Target Message Format: <timestamp> <seq_num> 61017 INFO TrustSec: ISE failed to refresh endpoint subscriber against APIC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61017 INFO TrustSec: ISE failed to refresh endpoint subscriber against APIC, <log details>

- **Message Code:** 61018

  Severity: INFO

  Message Text: ISE failed to refresh EEPG subscriber against APIC

  Message Description: ISE failed to refresh EEPG subscriber against APIC

  Local Target Message Format: <timestamp> <seq_num> 61018 INFO TrustSec: ISE failed to refresh EEPG subscriber against APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61018 INFO TrustSec: ISE failed to refresh EEPG subscriber against APIC, <log details>

- **Message Code:** 61020

  Severity: INFO

  Message Text: ISE failed to refresh L3EXTOUT subscriber against APIC

  Message Description: ISE failed to refresh L3EXTOUT subscriber against APIC

  Local Target Message Format: <timestamp> <seq_num> 61020 INFO TrustSec: ISE failed to refresh L3EXTOUT subscriber against APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61020 INFO TrustSec: ISE failed to refresh L3EXTOUT subscriber against APIC, <log details>

- **Message Code:** 61021

  Severity: INFO

  Message Text: After 3 retries, ISE recieved EPG with class id: ANY. Ignoring this EPG

  Message Description: After 3 retries, ISE recieved EPG with class id: ANY. Ignoring this EPG

  Local Target Message Format: <timestamp> <seq_num> 61021 INFO TrustSec: After 3 retries, ISE recieved EPG with class id: ANY. Ignoring this EPG, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61021 INFO TrustSec: After 3 retries, ISE recieved EPG with class id: ANY. Ignoring this EPG, <log details>

- **Message Code:** 61022

  Severity: INFO

  Message Text: ISE has failed to propagate SGT to EEPG

  Message Description: ISE has failed to propagate SGT to EEPG

Local Target Message Format: <timestamp> <seq_num> 61022 INFO TrustSec: ISE has failed to propagate SGT to EEPG, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61022 INFO TrustSec: ISE has failed to propagate SGT to EEPG, <log details>

- **Message Code:** 61023

  Severity: INFO

  Message Text: ISE has failed to learn IEPG from APIC

  Message Description: ISE has failed to learn IEPG from APIC

  Local Target Message Format: <timestamp> <seq_num> 61023 INFO TrustSec: ISE has failed to learn IEPG from APIC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61023 INFO TrustSec: ISE has failed to learn IEPG from APIC, <log details>

- **Message Code:** 61024

  Severity: INFO

  Message Text: ISE has failed to parse VRF for EPG

  Message Description: ISE has failed to parse VRF for EPG

  Local Target Message Format: <timestamp> <seq_num> 61024 INFO TrustSec: ISE has failed to parse VRF for EPG, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61024 INFO TrustSec: ISE has failed to parse VRF for EPG, <log details>

- **Message Code:** 61025

  Severity: INFO

  Message Text: Open secure connection with TLS peer

  Message Description: Secure connection established with TLS peer

  Local Target Message Format: <timestamp> <seq_num> 61025 INFO System-Management: Open secure connection with TLS peer, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61025 INFO System-Management: Open secure connection with TLS peer, <log details>

- **Message Code:** 61026

  Severity: INFO

  Message Text: Shutdown secure connection with TLS peer

  Message Description: Secure connection with TLS peer shutdown

Local Target Message Format: <timestamp> <seq_num> 61026 INFO System-Management: Shutdown secure connection with TLS peer, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 61026 INFO System-Management: Shutdown secure connection with TLS peer, <log details>

- **Message Code:** 60505

  Severity: ERROR

  Message Text: ERS request rejected due to invalid input.

  Message Description: The ERS request was rejected because the input was invalid

  Local Target Message Format: <timestamp> <seq_num>60505 ERROR ERS ERS request rejected due to invalid input., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60505 ERROR ERS ERS request rejected due to invalid input., <log details>

- **Message Code:** 60506

  Severity: ERROR

  Message Text: ERS request suspicious of malicious attack

  Message Description: The ERS request is suspicious of a malicious attack.

  Local Target Message Format: <timestamp> <seq_num>60506 ERROR ERS ERS request suspicious of malicious attack, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60506 ERROR ERS ERS request suspicious of malicious attack, <log details>

- **Message Code:** 60507

  Severity: ERROR

  Message Text: ERS request rejected due to unauthorized user.

  Message Description: ERS request was rejected because the user who sent the request is unauthorized.

  Local Target Message Format: <timestamp> <seq_num>60507 ERROR ERS ERS request rejected due to unauthorized user., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60507 ERROR ERS ERS request rejected due to unauthorized user., <log details>

- **Message Code:** 60508

  Severity: ERROR

  Message Text: ERS request was rejected due to illegal request on a non-primary node

  Message Description: The ERS request was rejected because an illegal request was sent to a non-primary node

Local Target Message Format: <timestamp> <seq_num>60508 ERROR ERS ERS request was rejected due to illegal request on a non-primary node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60508 ERROR ERS ERS request was rejected due to illegal request on a non-primary node, <log details>

- **Message Code:** 60509

  Severity: ERROR

  Message Text: ERS request was denied as maximum possible connection was exceeded

  Message Description: ERS request was denied as maximum possible connection was exceeded

  Local Target Message Format: <timestamp> <seq_num>60509 ERROR ERS ERS request was denied as maximum possible connection was exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60509 ERROR ERS ERS request was denied as maximum possible connection was exceeded, <log details>

- **Message Code:** 61027

  Severity: WARN

  Message Text: Received Invalid or Bad HTTP request

  Message Description: The system detected an invalid or bad HTTP request. This could be an attempted security attack

  Local Target Message Format: <timestamp> <seq_num>61027 WARN Bad-HTTP-Request Received Invalid or Bad HTTP request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61027 WARN Bad-HTTP-Request Received Invalid or Bad HTTP request, <log details>

- **Message Code:** 61028

  Severity: INFO

  Message Text: TrustSec deploy verification has started.

  Message Description: TrustSec deployment verification process has started.

  Local Target Message Format: <timestamp> <seq_num>61028 INFO TrustSec TrustSec deploy verification has started., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61028 INFO TrustSec TrustSec deploy verification has started., <log details>

- **Message Code:** 61029

  Severity: INFO

  Message Text: TrustSec deploy verification has finished.

  Message Description: TrustSec deployment verification process has finished.

Local Target Message Format: <timestamp> <seq_num>61029 INFO TrustSec TrustSec deploy verification has finished., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61029 INFO TrustSec TrustSec deploy verification has finished., <log details>

- **Message Code:** 61030

  Severity: INFO

  Message Text: TrustSec deploy verification was canceled.

  Message Description: TrustSec deployment verification process was canceled as a new TrustSec deploy started.

  Local Target Message Format: <timestamp> <seq_num>61030 INFO TrustSec TrustSec deploy verification was canceled., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61030 INFO TrustSec TrustSec deploy verification was canceled., <log details>

- **Message Code:** 61031

  Severity: WARN

  Message Text: TrustSec deploy verification failed to reach NAD.

  Message Description: TrustSec deployment verification process failed to connect to a network access device.

  Local Target Message Format: <timestamp> <seq_num>61031 WARN TrustSec TrustSec deploy verification failed to reach NAD., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61031 WARN TrustSec TrustSec deploy verification failed to reach NAD., <log details>

- **Message Code:** 61032

  Severity: WARN

  Message Text: TrustSec deploy verification - policy difference.

  Message Description: TrustSec deploy verification process found a difference between a network access device and ISE TrustSec configuration.

  Local Target Message Format: <timestamp> <seq_num>61032 WARN TrustSec TrustSec deploy verification - policy difference., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61032 WARN TrustSec TrustSec deploy verification - policy difference., <log details>

- **Message Code:** 61033

  Severity: INFO

  Message Text: TrustSec deployment verification process succeeded.

Message Description: ISE trustsec configuration was successfully deployed to all network access devices.

Local Target Message Format: <timestamp> <seq_num>61033 INFO TrustSec TrustSec deployment verification process succeeded., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61033 INFO TrustSec TrustSec deployment verification process succeeded., <log details>

- **Message Code:** 61034

  Severity: INFO

  Message Text: Maximum resource limit reached.

  Message Description: Maximum resource limit reached.

  Local Target Message Format: <timestamp> <seq_num>61034 INFO ResourceLimits Maximum resource limit reached., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61034 INFO ResourceLimits Maximum resource limit reached., <log details>

- **Message Code:** 61035

  Severity: INFO

  Message Text: IP SGT static mapping has been sent to the NAD.

  Message Description: IP SGT static mapping has been sent to the NAD.

  Local Target Message Format: <timestamp> <seq_num>61035 INFO TrustSec IP SGT static mapping has been sent to the NAD., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61035 INFO TrustSec IP SGT static mapping has been sent to the NAD., <log details>

- **Message Code:** 61051

  Severity: INFO

  Message Text: Synflood-limit configured

  Message Description: Synflood-limit configured

  Local Target Message Format: <timestamp> <seq_num>61051 INFO SynfloodLimitConfigured Synflood-limit configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61051 INFO SynfloodLimitConfigured Synflood-limit configured, <log details>

- **Message Code:** 61052

  Severity: INFO

  Message Text: rate-limit configured

  Message Description: rate-limit configured

Local Target Message Format: <timestamp> <seq_num>61052 INFO RateLimitConfigured rate-limit configured, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61052 INFO RateLimitConfigured rate-limit configured, <log details>

- **Message Code:** 61053

  Severity: WARN

  Message Text: Invalid user input detected. * \ $ @ characters are not allowed

  Message Description: Invalid user input detected. * \ $ @ characters are not allowed

  Local Target Message Format: <timestamp> <seq_num>61053 WARN UserInputControl Invalid user input detected. * \ $ @ characters are not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61053 WARN UserInputControl Invalid user input detected. * \ $ @ characters are not allowed, <log details>

- **Message Code:** 61054

  Severity: ERROR

  Message Text: ISE found Invalid authorization profile

  Message Description: ISE found Invalid authorization profile

  Local Target Message Format: <timestamp> <seq_num>61054 ERROR Configuration-Changes ISE found Invalid authorization profile, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61054 ERROR Configuration-Changes ISE found Invalid authorization profile, <log details>

- **Message Code:** 61055

  Severity: ERROR

  Message Text: The memory consumed by the queue is high

  Message Description: The memory consumed by the queue is high

  Local Target Message Format: <timestamp> <seq_num>61055 ERROR System-Management The memory consumed by the queue is high, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61055 ERROR System-Management The memory consumed by the queue is high, <log details>

- **Message Code:** 61056

  Severity: ERROR

  Message Text: The federation link was down

  Message Description: The federation link was down

Local Target Message Format: <timestamp> <seq_num>61056 ERROR System-Management The federation link was down, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61056 ERROR System-Management The federation link was down, <log details>

- **Message Code:** 61057

  Severity: ERROR

  Message Text: The space available to the queue is low

  Message Description: The space available to the queue is low

  Local Target Message Format: <timestamp> <seq_num>61057 ERROR System-Management The space available to the queue is low, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61057 ERROR System-Management The space available to the queue is low, <log details>

- **Message Code:** 61058

  Severity: ERROR

  Message Text: ISE has failed to update the APIC server with SGT/SGT-IP mappings

  Message Description: ISE has failed to update the APIC server with SGT/SGT-IP mappings

  Local Target Message Format: <timestamp> <seq_num>61058 ERROR TrustSec ISE has failed to update the APIC server with SGT/SGT-IP mappings, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61058 ERROR TrustSec ISE has failed to update the APIC server with SGT/SGT-IP mappings, <log details>

- **Message Code:** 61059

  Severity: INFO

  Message Text: Request from Customer Success Network

  Message Description: Deployment or Support information requested from Customer Success Network

  Local Target Message Format: <timestamp> <seq_num>61059 INFO Administrative and Operational Audit Request from Customer Success Network, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61059 INFO Administrative and Operational Audit Request from Customer Success Network, <log details>

- **Message Code:** 61060

  Severity: INFO

  Message Text: The ISE server is registered to Cisco Support Diagnostics

  Message Description: The ISE server is registered to Cisco Support Diagnostics

Local Target Message Format: <timestamp> <seq_num>61060 INFO Cisco Support Diagnostics The ISE server is registered to Cisco Support Diagnostics, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61060 INFO Cisco Support Diagnostics The ISE server is registered to Cisco Support Diagnostics, <log details>

- **Message Code:** 61061

  Severity: INFO

  Message Text: The ISE server is de-registered from Cisco Support Diagnostics

  Message Description: The ISE server is de-registered from Cisco Support Diagnostics

  Local Target Message Format: <timestamp> <seq_num>61061 INFO Cisco Support Diagnostics The ISE server is de-registered from Cisco Support Diagnostics, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61061 INFO Cisco Support Diagnostics The ISE server is de-registered from Cisco Support Diagnostics, <log details>

- **Message Code:** 61062

  Severity: INFO

  Message Text: The Cisco Support Diagnostics bi-directional connectivity is enabled

  Message Description: The Cisco Support Diagnostics bi-directional connectivity is enabled

  Local Target Message Format: <timestamp> <seq_num>61062 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is enabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61062 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is enabled, <log details>

- **Message Code:** 61063

  Severity: INFO

  Message Text: The Cisco Support Diagnostics bi-directional connectivity is disabled

  Message Description: The Cisco Support Diagnostics bi-directional connectivity is disabled

  Local Target Message Format: <timestamp> <seq_num>61063 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61063 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is disabled, <log details>

- **Message Code:** 61064

  Severity: INFO

  Message Text: The Cisco Support Diagnostics bi-directional connectivity is established

  Message Description: The Cisco Support Diagnostics bi-directional connectivity is established

Local Target Message Format: <timestamp> <seq_num>61064 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is established, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61064 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is established, <log details>

- **Message Code:** 61065

  Severity: INFO

  Message Text: The Cisco Support Diagnostics bi-directional connectivity is broken

  Message Description: The Cisco Support Diagnostics bi-directional connectivity is broken

  Local Target Message Format: <timestamp> <seq_num>61065 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is broken, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61065 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is broken, <log details>

- **Message Code:** 61066

  Severity: INFO

  Message Text: The ISE SSE services were enrolled to Cisco Support Diagnostics

  Message Description: The ISE SSE services were enrolled to Cisco Support Diagnostics

  Local Target Message Format: <timestamp> <seq_num>61066 INFO Cisco Support Diagnostics The ISE SSE services were enrolled to Cisco Support Diagnostics, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61066 INFO Cisco Support Diagnostics The ISE SSE services were enrolled to Cisco Support Diagnostics, <log details>

- **Message Code:** 61067

  Severity: INFO

  Message Text: The ISE SSE services were un-enrolled from Cisco Support Diagnostics

  Message Description: The ISE SSE services were un-enrolled from Cisco Support Diagnostics

  Local Target Message Format: <timestamp> <seq_num>61067 INFO Cisco Support Diagnostics The ISE SSE services were un-enrolled from Cisco Support Diagnostics, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61067 INFO Cisco Support Diagnostics The ISE SSE services were un-enrolled from Cisco Support Diagnostics, <log details>

- **Message Code:** 61068

  Severity: WARNING

  Message Text: ACI Integration Performance Insufficient

  Message Description: The ACI feature has encountered a performance issue: it was not possible to forward all the Endpoints IP-SGT mappings generated from the Network Access Sessions to ACI.

Local Target Message Format: <timestamp> <seq_num>61068 WARNING Alarm ACI Integration Performance Insufficient, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61068 WARNING Alarm ACI Integration Performance Insufficient, <log details>

- **Message Code:** 61069

  Severity: INFO

  Message Text: Rest request to ctsmatrix succeeded

  Message Description: Rest request to ctsmatrix succeeded

  Local Target Message Format: <timestamp> <seq_num>61069 INFO Trustsec Audit Rest request to ctsmatrix succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61069 INFO Trustsec Audit Rest request to ctsmatrix succeeded, <log details>

- **Message Code:** 61070

  Severity: INFO

  Message Text: Rest request to ctssgacls succeeded

  Message Description: Rest request to ctssgacls succeeded

  Local Target Message Format: <timestamp> <seq_num>61070 INFO Trustsec Audit Rest request to ctssgacls succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61070 INFO Trustsec Audit Rest request to ctssgacls succeeded, <log details>

- **Message Code:** 61071

  Severity: INFO

  Message Text: Rest request to ctsenvdata succeeded

  Message Description: Rest request to ctsenvdata succeeded

  Local Target Message Format: <timestamp> <seq_num>61071 INFO Trustsec Audit Rest request to ctsenvdata succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61071 INFO Trustsec Audit Rest request to ctsenvdata succeeded, <log details>

- **Message Code:** 61072

  Severity: ERROR

  Message Text: Error processing the REST request related to Trustsec Audit

  Message Description: Error processing the REST request related to Trustsec Audit

Local Target Message Format: <timestamp> <seq_num>61072 ERROR Trustsec Audit Error processing the REST request related to Trustsec Audit, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61072 ERROR Trustsec Audit Error processing the REST request related to Trustsec Audit, <log details>

- **Message Code:** 61073

  Severity: INFO

  Message Text: The Cisco Support Diagnostics bi-directional connectivity is broken

  Message Description: The Cisco Support Diagnostics bi-directional connectivity is broken

  Local Target Message Format: <timestamp> <seq_num>61073 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is broken, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61073 INFO Cisco Support Diagnostics The Cisco Support Diagnostics bi-directional connectivity is broken, <log details>

- **Message Code:** 61074

  Severity: ERROR

  Message Text: Node went out of sync due to expired system certificate

  Message Description: Node went out of sync due to expired system certificate

  Local Target Message Format: <timestamp> <seq_num>61074 ERROR Distributed-Management Node went out of sync due to expired system certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61074 ERROR Distributed-Management Node went out of sync due to expired system certificate, <log details>

- **Message Code:** 61075

  Severity: WARNING

  Message Text: ACI Integration cannot contact DNA-C

  Message Description: The ACI feature could not contact DNA-C

  Local Target Message Format: <timestamp> <seq_num>61075 WARNING Alarm ACI Integration cannot contact DNA-C, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61075 WARNING Alarm ACI Integration cannot contact DNA-C, <log details>

- **Message Code:** 51025

  Severity: NOTICE

  Message Text: Authentication for web services failed

  Message Description: Authentication for web services failed.

Local Target Message Format: <timestamp> <seq_num>51025 NOTICE User change password Authentication for web services failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>51025 NOTICE User change password Authentication for web services failed, <log details>

- **Message Code:** 61076

  Severity: INFO

  Message Text: Sponsor has been successfully logged out

  Message Description: Sponsor has been successfully logged out

  Local Target Message Format: <timestamp> <seq_num>61076 INFO Sponsor Sponsor has been successfully logged out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61076 INFO Sponsor Sponsor has been successfully logged out, <log details>

- **Message Code:** 61077

  Severity: INFO

  Message Text: MyDevices has been successfully logged out

  Message Description: MyDevices has been successfully logged out

  Local Target Message Format: <timestamp> <seq_num>61077 INFO MyDevices MyDevices has been successfully logged out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61077 INFO MyDevices MyDevices has been successfully logged out, <log details>

- **Message Code:** 61078

  Severity: INFO

  Message Text: Rest request to ctsreportconfig succeeded

  Message Description: Rest request to ctsreportconfig succeeded

  Local Target Message Format: <timestamp> <seq_num>61078 INFO Trustsec Audit Rest request to ctsreportconfig succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61078 INFO Trustsec Audit Rest request to ctsreportconfig succeeded, <log details>

- **Message Code:** 61079

  Severity: INFO

  Message Text: NAD TrustSec Propagation Status

  Message Description: NAD TrustSec Propagation Status

Local Target Message Format: <timestamp> <seq_num>61079 INFO Trustsec Audit NAD TrustSec Propagation Status, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61079 INFO Trustsec Audit NAD TrustSec Propagation Status, <log details>

- **Message Code:** 61100

  Severity: INFO

  Message Text: ISE has learned a new tenant from ACI

  Message Description: ISE has learned a new tenant from ACI

  Local Target Message Format: <timestamp> <seq_num>61100 INFO TrustSec ISE has learned a new tenant from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61100 INFO TrustSec ISE has learned a new tenant from ACI, <log details>

- **Message Code:** 61101

  Severity: INFO

  Message Text: ISE has removed ACI tenant

  Message Description: ISE has removed ACI tenant

  Local Target Message Format: <timestamp> <seq_num>61101 INFO TrustSec ISE has removed ACI tenant, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61101 INFO TrustSec ISE has removed ACI tenant, <log details>

- **Message Code:** 61102

  Severity: ERROR

  Message Text: Failed to learn new tenant from ACI in ISE

  Message Description: Failed to learn new tenant from ACI in ISE

  Local Target Message Format: <timestamp> <seq_num>61102 ERROR TrustSec Failed to learn new tenant from ACI in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61102 ERROR TrustSec Failed to learn new tenant from ACI in ISE, <log details>

- **Message Code:** 61103

  Severity: ERROR

  Message Text: Failed to remove ACI tenant in ISE

  Message Description: Failed to remove ACI tenant in ISE

Local Target Message Format: <timestamp> <seq_num>61103 ERROR TrustSec Failed to remove ACI tenant in ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61103 ERROR TrustSec Failed to remove ACI tenant in ISE, <log details>

- **Message Code:** 61104

  Severity: INFO

  Message Text: ISE has learned a new tenant from SDA

  Message Description: ISE has learned a new tenant from SDA

  Local Target Message Format: <timestamp> <seq_num>61104 INFO TrustSec ISE has learned a new tenant from SDA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61104 INFO TrustSec ISE has learned a new tenant from SDA, <log details>

- **Message Code:** 61105

  Severity: INFO

  Message Text: ISE has learned a new VN info

  Message Description: IISE has learned a new VN info

  Local Target Message Format: <timestamp> <seq_num>61105 INFO TrustSec ISE has learned a new VN info, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61105 INFO TrustSec ISE has learned a new VN info, <log details>

- **Message Code:** 61106

  Severity: ERROR

  Message Text: Failed to create VN info in ISE

  Message Description: Failed to create VN info in ISE

  Local Target Message Format: <timestamp> <seq_num>61106 ERROR TrustSec Failed to create VN info in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61106 ERROR TrustSec Failed to create VN info in ISE, <log details>

- **Message Code:** 61107

  Severity: INFO

  Message Text: VN info is updated in ISE

  Message Description: VN info is updated in ISE

Local Target Message Format: <timestamp> <seq_num>61107 INFO TrustSec VN info is updated in ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61107 INFO TrustSec VN info is updated in ISE, <log details>

- **Message Code:** 61108

  Severity: ERROR

  Message Text: Failed to update VN info in ISE

  Message Description: Failed to update VN info in ISE

  Local Target Message Format: <timestamp> <seq_num>61108 ERROR TrustSec Failed to update VN info in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61108 ERROR TrustSec Failed to update VN info in ISE, <log details>

- **Message Code:** 61109

  Severity: INFO

  Message Text: VN info is deleted in ISE

  Message Description: VN info is deleted in ISE

  Local Target Message Format: <timestamp> <seq_num>61109 INFO TrustSec VN info is deleted in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61109 INFO TrustSec VN info is deleted in ISE, <log details>

- **Message Code:** 61110

  Severity: ERROR

  Message Text: Failed to deleted VN info in ISE

  Message Description: Failed to deleted VN info in ISE

  Local Target Message Format: <timestamp> <seq_num>61110 ERROR TrustSec Failed to deleted VN info in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61110 ERROR TrustSec Failed to deleted VN info in ISE, <log details>

- **Message Code:** 61111

  Severity: ERROR

  Message Text: Domain registration process failed

  Message Description: Domain registration process failed

Local Target Message Format: <timestamp> <seq_num>61111 ERROR TrustSec Domain registration process failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61111 ERROR TrustSec Domain registration process failed, <log details>

- **Message Code:** 61112

  Severity: INFO

  Message Text: Start domain registration process in SPHUB

  Message Description: Start domain registration process in SPHUB

  Local Target Message Format: <timestamp> <seq_num>61112 INFO TrustSec Start domain registration process in SPHUB, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61112 INFO TrustSec Start domain registration process in SPHUB, <log details>

- **Message Code:** 61113

  Severity: INFO

  Message Text: Send certificate request to domain manager

  Message Description: Send certificate request to domain manager

  Local Target Message Format: <timestamp> <seq_num>61113 INFO TrustSec Send certificate request to domain manager, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61113 INFO TrustSec Send certificate request to domain manager, <log details>

- **Message Code:** 61114

  Severity: INFO

  Message Text: Domain registration completed successfully

  Message Description: Domain registration completed successfully

  Local Target Message Format: <timestamp> <seq_num>61114 INFO TrustSec Domain registration completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61114 INFO TrustSec Domain registration completed successfully, <log details>

- **Message Code:** 61115

  Severity: ERROR

  Message Text: Domain registration failed

  Message Description: DDomain registration failed

Local Target Message Format: <timestamp> <seq_num>61115 ERROR TrustSec Domain registration failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61115 ERROR TrustSec Domain registration failed, <log details>

- **Message Code:** 61116

  Severity: ERROR

  Message Text: Unable to store ACI certificate

  Message Description: Unable to store ACI certificate

  Local Target Message Format: <timestamp> <seq_num>61116 ERROR TrustSec Unable to store ACI certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61116 ERROR TrustSec Unable to store ACI certificate, <log details>

- **Message Code:** 61117

  Severity: INFO

  Message Text: ACI connector started successfully

  Message Description: ACI connector started successfully

  Local Target Message Format: <timestamp> <seq_num>61117 INFO TrustSec ACI connector started successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61117 INFO TrustSec ACI connector started successfully, <log details>

- **Message Code:** 61118

  Severity: ERROR

  Message Text: Failed to start ACI connector

  Message Description: Failed to start ACI connector

  Local Target Message Format: <timestamp> <seq_num>61118 ERROR TrustSec Failed to start ACI connector, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61118 ERROR TrustSec Failed to start ACI connector, <log details>

- **Message Code:** 61119

  Severity: INFO

  Message Text: Domain de-registration process started

  Message Description: Domain de-registration process started

Local Target Message Format: <timestamp> <seq_num>61119 INFO TrustSec Domain de-registration process started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61119 INFO TrustSec Domain de-registration process started, <log details>

- **Message Code:** 61120

  Severity: INFO

  Message Text: Successfully deleted ACI certificate from ISE

  Message Description: Successfully deleted ACI certificate from ISE

  Local Target Message Format: <timestamp> <seq_num>61120 INFO TrustSec Successfully deleted ACI certificate from ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61120 INFO TrustSec Successfully deleted ACI certificate from ISE, <log details>

- **Message Code:** 61121

  Severity: ERROR

  Message Text: Failed to delete ACI certificate from ISE

  Message Description: Failed to delete ACI certificate from ISE

  Local Target Message Format: <timestamp> <seq_num>61121 ERROR TrustSec Failed to delete ACI certificate from ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61121 ERROR TrustSec Failed to delete ACI certificate from ISE, <log details>

- **Message Code:** 61122

  Severity: ERROR

  Message Text: Failed to delete ACI keystore

  Message Description: Failed to delete ACI keystore

  Local Target Message Format: <timestamp> <seq_num>61122 ERROR TrustSec Failed to delete ACI keystore, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61122 ERROR TrustSec Failed to delete ACI keystore, <log details>

- **Message Code:** 61123

  Severity: INFO

  Message Text: ISE has learned a new ACI domain

  Message Description: ISE has learned a new ACI domain

Local Target Message Format: <timestamp> <seq_num>61123 INFO TrustSec ISE has learned a new ACI domain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61123 INFO TrustSec ISE has learned a new ACI domain, <log details>

- **Message Code:** 61124

  Severity: ERROR

  Message Text: Failed to learn a new ACI domain

  Message Description: Failed to learn a new ACI domain

  Local Target Message Format: <timestamp> <seq_num>61124 ERROR TrustSec Failed to learn a new ACI domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61124 ERROR TrustSec Failed to learn a new ACI domain, <log details>

- **Message Code:** 61125

  Severity: INFO

  Message Text: ISE has removed ACI domain

  Message Description: ISE has removed ACI domain

  Local Target Message Format: <timestamp> <seq_num>61125 INFO TrustSec ISE has removed ACI domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61125 INFO TrustSec ISE has removed ACI domain, <log details>

- **Message Code:** 61126

  Severity: ERROR

  Message Text: Failed to remove ACI domain

  Message Description: Failed to remove ACI domain

  Local Target Message Format: <timestamp> <seq_num>61126 ERROR TrustSec Failed to remove ACI domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61126 ERROR TrustSec Failed to remove ACI domain, <log details>

- **Message Code:** 61127

  Severity: INFO

  Message Text: ISE has learned a new SDA domain

  Message Description: ISE has learned a new SDA domain

Local Target Message Format: <timestamp> <seq_num>61127 INFO TrustSec ISE has learned a new SDA domain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61127 INFO TrustSec ISE has learned a new SDA domain, <log details>

- **Message Code:** 61128

  Severity: ERROR

  Message Text: Failed to learn a new SDA domain

  Message Description: Failed to learn a new SDA domain

  Local Target Message Format: <timestamp> <seq_num>61128 ERROR TrustSec Failed to learn a new SDA domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61128 ERROR TrustSec Failed to learn a new SDA domain, <log details>

- **Message Code:** 61129

  Severity: INFO

  Message Text: ISE has removed SDA domain

  Message Description: ISE has removed SDA domain

  Local Target Message Format: <timestamp> <seq_num>61129 INFO TrustSec ISE has removed SDA domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61129 INFO TrustSec ISE has removed SDA domain, <log details>

- **Message Code:** 61130

  Severity: ERROR

  Message Text: Failed to remove SDA domain

  Message Description: Failed to remove SDA domain

  Local Target Message Format: <timestamp> <seq_num>61130 ERROR TrustSec Failed to remove SDA domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61130 ERROR TrustSec Failed to remove SDA domain, <log details>

- **Message Code:** 61131

  Severity: ERROR

  Message Text: SDA peering initiation failed. Response from ISE Domain registration is unsuccessful

  Message Description: SDA peering initiation failed. Response from ISE Domain registration is unsuccessful

Local Target Message Format: <timestamp> <seq_num>61131 ERROR TrustSec SDA peering initiation failed. Response from ISE Domain registration is unsuccessful, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61131 ERROR TrustSec SDA peering initiation failed. Response from ISE Domain registration is unsuccessful, <log details>

- **Message Code:** 61132

  Severity: ERROR

  Message Text: SDA peering Initialization failed.

  Message Description: SDA peering Initialization failed.

  Local Target Message Format: <timestamp> <seq_num>61132 ERROR TrustSec SDA peering Initialization failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61132 ERROR TrustSec SDA peering Initialization failed., <log details>

- **Message Code:** 61133

  Severity: INFO

  Message Text: SDA successfully initiated peering process.

  Message Description: SDA successfully initiated peering process.

  Local Target Message Format: <timestamp> <seq_num>61133 INFO TrustSec SDA successfully initiated peering process., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61133 INFO TrustSec SDA successfully initiated peering process., <log details>

- **Message Code:** 61134

  Severity: ERROR

  Message Text: SDA Domain advertisement failed publishing to ACI

  Message Description: SDA Domain advertisement failed publishing to ACI

  Local Target Message Format: <timestamp> <seq_num>61134 ERROR TrustSec SDA Domain advertisement failed publishing to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61134 ERROR TrustSec SDA Domain advertisement failed publishing to ACI, <log details>

- **Message Code:** 61135

  Severity: ERROR

  Message Text: SDA Domain advertisement failed publishing to ISE

  Message Description: SDA Domain advertisement failed publishing to ISE

Local Target Message Format: <timestamp> <seq_num>61135 ERROR TrustSec SDA Domain advertisement failed publishing to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61135 ERROR TrustSec SDA Domain advertisement failed publishing to ISE, <log details>

- **Message Code:** 61136

  Severity: INFO

  Message Text: Successful SDA Domain advertisement to ACI

  Message Description: Successful SDA Domain advertisement to ACI

  Local Target Message Format: <timestamp> <seq_num>61136 INFO TrustSec Successful SDA Domain advertisement to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61136 INFO TrustSec Successful SDA Domain advertisement to ACI, <log details>

- **Message Code:** 61137

  Severity: INFO

  Message Text: SDA Publishing SXP information to ISE

  Message Description: SDA Publishing SXP information to ISE

  Local Target Message Format: <timestamp> <seq_num>61137 INFO TrustSec SDA Publishing SXP information to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61137 INFO TrustSec SDA Publishing SXP information to ISE, <log details>

- **Message Code:** 61138

  Severity: ERROR

  Message Text: Error processing the mdpGatewayAdv event from SDA

  Message Description: Error processing the mdpGatewayAdv event from SDA

  Local Target Message Format: <timestamp> <seq_num>61138 ERROR TrustSec Error processing the mdpGatewayAdv event from SDA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61138 ERROR TrustSec Error processing the mdpGatewayAdv event from SDA, <log details>

- **Message Code:** 61139

  Severity: INFO

  Message Text: Publishing SDA gateway advertisement information to ISE

  Message Description: Publishing SDA gateway advertisement information to ISE

Local Target Message Format: <timestamp> <seq_num>61139 INFO TrustSec Publishing SDA gateway advertisement information to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61139 INFO TrustSec Publishing SDA gateway advertisement information to ISE, <log details>

- **Message Code:** 61140

  Severity: ERROR

  Message Text: Error in Publishing SDA gateway advertisement information to ISE

  Message Description: Error in Publishing SDA gateway advertisement information to ISE

  Local Target Message Format: <timestamp> <seq_num>61140 ERROR TrustSec Error in Publishing SDA gateway advertisement information to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61140 ERROR TrustSec Error in Publishing SDA gateway advertisement information to ISE, <log details>

- **Message Code:** 61141

  Severity: INFO

  Message Text: Publishing SDA's VN information to ACI

  Message Description: Publishing SDA's VN information to ACI

  Local Target Message Format: <timestamp> <seq_num>61141 INFO TrustSec Publishing SDA's VN information to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61141 INFO TrustSec Publishing SDA's VN information to ACI, <log details>

- **Message Code:** 61142

  Severity: ERROR

  Message Text: Failed to publish SDA's VN information to ACI

  Message Description: Failed to publish SDA's VN information to ACI

  Local Target Message Format: <timestamp> <seq_num>61142 ERROR TrustSec Failed to publish SDA's VN information to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61142 ERROR TrustSec Failed to publish SDA's VN information to ACI, <log details>

- **Message Code:** 61143

  Severity: INFO

  Message Text: Publishing SDA's VN information to ISE

  Message Description: Publishing SDA's VN information to ISE

Local Target Message Format: <timestamp> <seq_num>61143 INFO TrustSec Publishing SDA's VN information to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61143 INFO TrustSec Publishing SDA's VN information to ISE, <log details>

- **Message Code:** 61144

  Severity: ERROR

  Message Text: Failed handling the SDA's VN information publish to ISE

  Message Description: Failed handling the SDA's VN information publish to ISE

  Local Target Message Format: <timestamp> <seq_num>61144 ERROR TrustSec Failed handling the SDA's VN information publish to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61144 ERROR TrustSec Failed handling the SDA's VN information publish to ISE, <log details>

- **Message Code:** 61145

  Severity: INFO

  Message Text: Publishing SDA extend VN response to ACI

  Message Description: Publishing SDA extend VN response to ACI

  Local Target Message Format: <timestamp> <seq_num>61145 INFO TrustSec Publishing SDA extend VN response to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61145 INFO TrustSec Publishing SDA extend VN response to ACI, <log details>

- **Message Code:** 61146

  Severity: ERROR

  Message Text: Failed to publish SDA extend VN response to ACI

  Message Description: Failed to publish SDA extend VN response to ACI

  Local Target Message Format: <timestamp> <seq_num>61146 ERROR TrustSec Failed to publish SDA extend VN response to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61146 ERROR TrustSec Failed to publish SDA extend VN response to ACI, <log details>

- **Message Code:** 61147

  Severity: ERROR

  Message Text: Tenant was not learned from SDA yet. Cannot publish message to ACI

  Message Description: Tenant was not learned from SDA yet. Cannot publish message to ACI

Local Target Message Format: <timestamp> <seq_num>61147 ERROR TrustSec Tenant was not learned from SDA yet. Cannot publish message to ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61147 ERROR TrustSec Tenant was not learned from SDA yet. Cannot publish message to ACI, <log details>

- **Message Code:** 61148

  Severity: ERROR

  Message Text: Failed parsing/storing SDA MdpEndpointGroupAdvEvent data

  Message Description: Failed parsing/storing SDA MdpEndpointGroupAdvEvent data

  Local Target Message Format: <timestamp> <seq_num>61148 ERROR TrustSec Failed parsing/storing SDA MdpEndpointGroupAdvEvent data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61148 ERROR TrustSec Failed parsing/storing SDA MdpEndpointGroupAdvEvent data, <log details>

- **Message Code:** 61149

  Severity: ERROR

  Message Text: Failed parsing/storing the SDA Ack message

  Message Description: Failed parsing/storing the SDA Ack message

  Local Target Message Format: <timestamp> <seq_num>61149 ERROR TrustSec Failed parsing/storing the SDA Ack message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61149 ERROR TrustSec Failed parsing/storing the SDA Ack message, <log details>

- **Message Code:** 61150

  Severity: INFO

  Message Text: Publishing ACI extend VN response to ISE

  Message Description: Publishing ACI extend VN response to ISE

  Local Target Message Format: <timestamp> <seq_num>61150 INFO TrustSec Publishing ACI extend VN response to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61150 INFO TrustSec Publishing ACI extend VN response to ISE, <log details>

- **Message Code:** 61151

  Severity: ERROR

  Message Text: Failed to publish ACI extend VN response to ISE

  Message Description: Failed to publish ACI extend VN response to ISE

Local Target Message Format: <timestamp> <seq_num>61151 ERROR TrustSec Failed to publish ACI extend VN response to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61151 ERROR TrustSec Failed to publish ACI extend VN response to ISE, <log details>

- **Message Code:** 61152

  Severity: INFO

  Message Text: ACI notified ISE it received SDA extend vn

  Message Description: ACI notified ISE it received SDA extend vn

  Local Target Message Format: <timestamp> <seq_num>61152 INFO TrustSec ACI notified ISE it received SDA extend vn, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61152 INFO TrustSec ACI notified ISE it received SDA extend vn, <log details>

- **Message Code:** 61153

  Severity: ERROR

  Message Text: SDA did not respond successfully to ACI message

  Message Description: SDA did not respond successfully to ACI message

  Local Target Message Format: <timestamp> <seq_num>61153 ERROR TrustSec SDA did not respond successfully to ACI message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61153 ERROR TrustSec SDA did not respond successfully to ACI message, <log details>

- **Message Code:** 61154

  Severity: INFO

  Message Text: ISE successfully respond to peering status retrieval

  Message Description: ISE successfully respond to peering status retrieval

  Local Target Message Format: <timestamp> <seq_num>61154 INFO TrustSec ISE successfully respond to peering status retrieval, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61154 INFO TrustSec ISE successfully respond to peering status retrieval, <log details>

- **Message Code:** 61156

  Severity: INFO

  Message Text: SDA published SXP configuration to ISE

  Message Description: SDA published SXP configuration to ISE

Local Target Message Format: <timestamp> <seq_num>61156 INFO TrustSec SDA published SXP configuration to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61156 INFO TrustSec SDA published SXP configuration to ISE, <log details>

- **Message Code:** 61157

  Severity: INFO

  Message Text: SDA SXP configuration successfully received by ISE

  Message Description: SDA SXP configuration successfully received by ISE

  Local Target Message Format: <timestamp> <seq_num>61157 INFO TrustSec SDA SXP configuration successfully received by ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61157 INFO TrustSec SDA SXP configuration successfully received by ISE, <log details>

- **Message Code:** 61158

  Severity: ERROR

  Message Text: ISE failed in receiving SDA SXP configuration

  Message Description: ISE failed in receiving SDA SXP configuration

  Local Target Message Format: <timestamp> <seq_num>61158 ERROR TrustSec ISE failed in receiving SDA SXP configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61158 ERROR TrustSec ISE failed in receiving SDA SXP configuration, <log details>

- **Message Code:** 61159

  Severity: INFO

  Message Text: ISE publishing Gateway advertisement message to ACI

  Message Description: ISE publishing Gateway advertisement message to ACI

  Local Target Message Format: <timestamp> <seq_num>61159 INFO TrustSec ISE publishing Gateway advertisement message to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61159 INFO TrustSec ISE publishing Gateway advertisement message to ACI, <log details>

- **Message Code:** 61160

  Severity: ERROR

  Message Text: ISE failed to publish Gateway advertisement message to ACI

  Message Description: ISE failed to publish Gateway advertisement message to ACI

Local Target Message Format: <timestamp> <seq_num>61160 ERROR TrustSec ISE failed to publish Gateway advertisement message to ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61160 ERROR TrustSec ISE failed to publish Gateway advertisement message to ACI, <log details>

- **Message Code:** 61161

  Severity: INFO

  Message Text: ISE learned new SXP Listener

  Message Description: ISE learned new SXP Listener

  Local Target Message Format: <timestamp> <seq_num>61161 INFO TrustSec ISE learned new SXP Listener, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61161 INFO TrustSec ISE learned new SXP Listener, <log details>

- **Message Code:** 61162

  Severity: INFO

  Message Text: ISE updates VN defined for SXP Listener

  Message Description: ISE updates VN defined for SXP Listener

  Local Target Message Format: <timestamp> <seq_num>61162 INFO TrustSec ISE updates VN defined for SXP Listener, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61162 INFO TrustSec ISE updates VN defined for SXP Listener, <log details>

- **Message Code:** 61163

  Severity: INFO

  Message Text: ISE learned new VN defined for SXP Listener

  Message Description: ISE learned new VN defined for SXP Listener

  Local Target Message Format: <timestamp> <seq_num>61163 INFO TrustSec ISE learned new VN defined for SXP Listener, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61163 INFO TrustSec ISE learned new VN defined for SXP Listener, <log details>

- **Message Code:** 61164

  Severity: INFO

  Message Text: ISE updates SXP Listener

  Message Description: ISE updates SXP Listener

Local Target Message Format: <timestamp> <seq_num>61164 INFO TrustSec ISE updates SXP Listener, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61164 INFO TrustSec ISE updates SXP Listener, <log details>

- **Message Code:** 61165

  Severity: INFO

  Message Text: ISE removed all SXP connections related to SXP Listener

  Message Description: ISE removed all SXP connections related to SXP Listener

  Local Target Message Format: <timestamp> <seq_num>61165 INFO TrustSec ISE removed all SXP connections related to SXP Listener, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61165 INFO TrustSec ISE removed all SXP connections related to SXP Listener, <log details>

- **Message Code:** 61166

  Severity: INFO

  Message Text: ACI published Gateway advertisement message to SDA

  Message Description: ACI published Gateway advertisement message to SDA

  Local Target Message Format: <timestamp> <seq_num>61166 INFO TrustSec ACI published Gateway advertisement message to SDA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61166 INFO TrustSec ACI published Gateway advertisement message to SDA, <log details>

- **Message Code:** 61167

  Severity: INFO

  Message Text: Send ACI Gateway advertisement message to ISE

  Message Description: Send ACI Gateway advertisement message to ISE

  Local Target Message Format: <timestamp> <seq_num>61167 INFO TrustSec Send ACI Gateway advertisement message to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61167 INFO TrustSec Send ACI Gateway advertisement message to ISE, <log details>

- **Message Code:** 61168

  Severity: ERROR

  Message Text: Failed to send ACI Gateway advertisement message to ISE

  Message Description: Failed to send ACI Gateway advertisement message to ISE/SDA

Local Target Message Format: <timestamp> <seq_num>61168 ERROR TrustSec Failed to send ACI Gateway advertisement message to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61168 ERROR TrustSec Failed to send ACI Gateway advertisement message to ISE, <log details>

- **Message Code:** 61169

  Severity: INFO

  Message Text: Successfully Send ACI Gateway advertisement message

  Message Description: Successfully Send ACI Gateway advertisement message

  Local Target Message Format: <timestamp> <seq_num>61169 INFO TrustSec Successfully Send ACI Gateway advertisement message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61169 INFO TrustSec Successfully Send ACI Gateway advertisement message, <log details>

- **Message Code:** 61170

  Severity: INFO

  Message Text: SDA published peer domain request to ACI

  Message Description: SDA published peer domain request to ACI

  Local Target Message Format: <timestamp> <seq_num>61170 INFO TrustSec SDA published peer domain request to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61170 INFO TrustSec SDA published peer domain request to ACI, <log details>

- **Message Code:** 61171

  Severity: ERROR

  Message Text: SDA failed to publish peer domain request to ACI

  Message Description: SDA failed to publish peer domain request to ACI

  Local Target Message Format: <timestamp> <seq_num>61171 ERROR TrustSec SDA failed to publish peer domain request to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61171 ERROR TrustSec SDA failed to publish peer domain request to ACI, <log details>

- **Message Code:** 61172

  Severity: INFO

  Message Text: SDA published peer domain response to ACI

  Message Description: SDA published peer domain response to ACI

Local Target Message Format: <timestamp> <seq_num>61172 INFO TrustSec SDA published peer domain response to ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61172 INFO TrustSec SDA published peer domain response to ACI, <log details>

- **Message Code:** 61173

  Severity: ERROR

  Message Text: SDA failed to publish peer domain response to ACI

  Message Description: SDA failed to publish peer domain response to ACI

  Local Target Message Format: <timestamp> <seq_num>61173 ERROR TrustSec SDA failed to publish peer domain response to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61173 ERROR TrustSec SDA failed to publish peer domain response to ACI, <log details>

- **Message Code:** 61174

  Severity: INFO

  Message Text: Process peer domain request

  Message Description: Process peer domain request

  Local Target Message Format: <timestamp> <seq_num>61174 INFO TrustSec Process peer domain request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61174 INFO TrustSec Process peer domain request, <log details>

- **Message Code:** 61175

  Severity: INFO

  Message Text: Process peer domain response

  Message Description: Process peer domain response

  Local Target Message Format: <timestamp> <seq_num>61175 INFO TrustSec Process peer domain response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61175 INFO TrustSec Process peer domain response, <log details>

- **Message Code:** 61176

  Severity: INFO

  Message Text: SDA initiate peering process with ACI

  Message Description: SDA initiate peering process with ACI

Local Target Message Format: <timestamp> <seq_num>61176 INFO TrustSec SDA initiate peering process with ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61176 INFO TrustSec SDA initiate peering process with ACI, <log details>

- **Message Code:** 61177

  Severity: INFO

  Message Text: ACI initiate peering process with SDA

  Message Description: ACI initiate peering process with SDA

  Local Target Message Format: <timestamp> <seq_num>61177 INFO TrustSec ACI initiate peering process with SDA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61177 INFO TrustSec ACI initiate peering process with SDA, <log details>

- **Message Code:** 61178

  Severity: ERROR

  Message Text: Peering already exist

  Message Description: Peering already exist

  Local Target Message Format: <timestamp> <seq_num>61178 ERROR TrustSec Peering already exist, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61178 ERROR TrustSec Peering already exist, <log details>

- **Message Code:** 61179

  Severity: ERROR

  Message Text: Peering process failed ACI Domain does not exist

  Message Description: Peering process failed ACI Domain does not exist

  Local Target Message Format: <timestamp> <seq_num>61179 ERROR TrustSec Peering process failed ACI Domain does not exist, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61179 ERROR TrustSec Peering process failed ACI Domain does not exist, <log details>

- **Message Code:** 61180

  Severity: ERROR

  Message Text: Peering process failed SDA Domain does not exist

  Message Description: Peering process failed SDA Domain does not exist

Local Target Message Format: <timestamp> <seq_num>61180 ERROR TrustSec Peering process failed SDA Domain does not exist, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61180 ERROR TrustSec Peering process failed SDA Domain does not exist, <log details>

- **Message Code:** 61181

  Severity: INFO

  Message Text: Peering established between SDA and ACI

  Message Description: Peering established between SDA and ACI

  Local Target Message Format: <timestamp> <seq_num>61181 INFO TrustSec Peering established between SDA and ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61181 INFO TrustSec Peering established between SDA and ACI, <log details>

- **Message Code:** 61182

  Severity: ERROR

  Message Text: SDA-ACI Peering process failed

  Message Description: SDA-ACI Peering process failed

  Local Target Message Format: <timestamp> <seq_num>61182 ERROR TrustSec SDA-ACI Peering process failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61182 ERROR TrustSec SDA-ACI Peering process failed, <log details>

- **Message Code:** 61183

  Severity: INFO

  Message Text: Received peer domain request from ACI

  Message Description: Received peer domain request from ACI

  Local Target Message Format: <timestamp> <seq_num>61183 INFO TrustSec Received peer domain request from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61183 INFO TrustSec Received peer domain request from ACI, <log details>

- **Message Code:** 61184

  Severity: ERROR

  Message Text: Failed to receive peer domain request from ACI

  Message Description: Failed to receive peer domain request from ACI

Local Target Message Format: <timestamp> <seq_num>61184 ERROR TrustSec Failed to receive peer domain request from ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61184 ERROR TrustSec Failed to receive peer domain request from ACI, <log details>

- **Message Code:** 61185

  Severity: INFO

  Message Text: Publish peer domain request to SDA from ACI

  Message Description: Publish peer domain request to SDA from ACI

  Local Target Message Format: <timestamp> <seq_num>61185 INFO TrustSec Publish peer domain request to SDA from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61185 INFO TrustSec Publish peer domain request to SDA from ACI, <log details>

- **Message Code:** 61186

  Severity: INFO

  Message Text: Failed to publish peer domain request to SDA from ACI

  Message Description: Failed to publish peer domain request to SDA from ACI

  Local Target Message Format: <timestamp> <seq_num>61186 INFO TrustSec Failed to publish peer domain request to SDA from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61186 INFO TrustSec Failed to publish peer domain request to SDA from ACI, <log details>

- **Message Code:** 61187

  Severity: INFO

  Message Text: Peering status between ACI and SDA is created

  Message Description: Peering status between ACI and SDA is created

  Local Target Message Format: <timestamp> <seq_num>61187 INFO TrustSec Peering status between ACI and SDA is created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61187 INFO TrustSec Peering status between ACI and SDA is created, <log details>

- **Message Code:** 61188

  Severity: INFO

  Message Text: Peering status between ACI and SDA is removed

  Message Description: Peering status between ACI and SDA is removed

Local Target Message Format: <timestamp> <seq_num>61188 INFO TrustSec Peering status between ACI and SDA is removed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61188 INFO TrustSec Peering status between ACI and SDA is removed, <log details>

- **Message Code:** 61189

  Severity: INFO

  Message Text: Publishing consumer to ACI

  Message Description: Publishing consumer to ACI

  Local Target Message Format: <timestamp> <seq_num>61189 INFO TrustSec Publishing consumer to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61189 INFO TrustSec Publishing consumer to ACI, <log details>

- **Message Code:** 61190

  Severity: ERROR

  Message Text: Failed to publish consumer to ACI

  Message Description: Failed to publish consumer to ACI

  Local Target Message Format: <timestamp> <seq_num>61190 ERROR TrustSec Failed to publish consumer to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61190 ERROR TrustSec Failed to publish consumer to ACI, <log details>

- **Message Code:** 61191

  Severity: INFO

  Message Text: Publishing consumer service request to ACI

  Message Description: Publishing consumer service request to ACI

  Local Target Message Format: <timestamp> <seq_num>61191 INFO TrustSec Publishing consumer service request to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61191 INFO TrustSec Publishing consumer service request to ACI, <log details>

- **Message Code:** 61192

  Severity: ERROR

  Message Text: Failed to publish consumer service request to ACI

  Message Description: Failed to publish consumer service request to ACI

Local Target Message Format: <timestamp> <seq_num>61192 ERROR TrustSec Failed to publish consumer service request to ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61192 ERROR TrustSec Failed to publish consumer service request to ACI, <log details>

- **Message Code:** 61193

  Severity: INFO

  Message Text: Deleting consumer service from ISE

  Message Description: Deleting consumer service from ISE

  Local Target Message Format: <timestamp> <seq_num>61193 INFO TrustSec Deleting consumer service from ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61193 INFO TrustSec Deleting consumer service from ISE, <log details>

- **Message Code:** 61194

  Severity: ERROR

  Message Text: Failed to delete consumer service from ISE

  Message Description: Failed to delete consumer service from ISE

  Local Target Message Format: <timestamp> <seq_num>61194 ERROR TrustSec Failed to delete consumer service from ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61194 ERROR TrustSec Failed to delete consumer service from ISE, <log details>

- **Message Code:** 61195

  Severity: INFO

  Message Text: ISE learned new SGACL from ACI

  Message Description: ISE learned new SGACL from ACI

  Local Target Message Format: <timestamp> <seq_num>61195 INFO TrustSec ISE learned new SGACL from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61195 INFO TrustSec ISE learned new SGACL from ACI, <log details>

- **Message Code:** 61196

  Severity: ERROR

  Message Text: Failed to learn new SGACL from ACI

  Message Description: Failed to learn new SGACL from ACI

Local Target Message Format: <timestamp> <seq_num>61196 ERROR TrustSec Failed to learn new SGACL from ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61196 ERROR TrustSec Failed to learn new SGACL from ACI, <log details>

- **Message Code:** 61197

  Severity: INFO

  Message Text: Successfully updated SGACL which learned from ACI

  Message Description: Successfully updated SGACL which learned from ACI

  Local Target Message Format: <timestamp> <seq_num>61197 INFO TrustSec Successfully updated SGACL which learned from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61197 INFO TrustSec Successfully updated SGACL which learned from ACI, <log details>

- **Message Code:** 61198

  Severity: ERROR

  Message Text: Failed to update SGACL which learned from ACI

  Message Description: Failed to update SGACL which learned from ACI

  Local Target Message Format: <timestamp> <seq_num>61198 ERROR TrustSec Failed to update SGACL which learned from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61198 ERROR TrustSec Failed to update SGACL which learned from ACI, <log details>

- **Message Code:** 61199

  Severity: INFO

  Message Text: ACI,Äôs SGACL was deleted from ISE

  Message Description: ACI,Äôs SGACL was deleted from ISE

  Local Target Message Format: <timestamp> <seq_num>61199 INFO TrustSec ACI,Äôs SGACL was deleted from ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61199 INFO TrustSec ACI,Äôs SGACL was deleted from ISE, <log details>

- **Message Code:** 61200

  Severity: ERROR

  Message Text: Failed to delete ACI,Äôs SGACL from ISE

  Message Description: Failed to delete ACI,Äôs SGACL from ISE

Local Target Message Format: <timestamp> <seq_num>61200 ERROR TrustSec Failed to delete ACI,Äôs SGACL from ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61200 ERROR TrustSec Failed to delete ACI,Äôs SGACL from ISE, <log details>

- **Message Code:** 61201

  Severity: INFO

  Message Text: Stored ACI Service in ISE

  Message Description: Stored ACI Service in ISE

  Local Target Message Format: <timestamp> <seq_num>61201 INFO TrustSec Stored ACI Service in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61201 INFO TrustSec Stored ACI Service in ISE, <log details>

- **Message Code:** 61202

  Severity: ERROR

  Message Text: Failed to store ACI Service in ISE

  Message Description: Failed to store ACI Service in ISE

  Local Target Message Format: <timestamp> <seq_num>61202 ERROR TrustSec Failed to store ACI Service in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61202 ERROR TrustSec Failed to store ACI Service in ISE, <log details>

- **Message Code:** 61203

  Severity: INFO

  Message Text: Updated ACI Service in ISE

  Message Description: Updated ACI Service in ISE

  Local Target Message Format: <timestamp> <seq_num>61203 INFO TrustSec Updated ACI Service in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61203 INFO TrustSec Updated ACI Service in ISE, <log details>

- **Message Code:** 61204

  Severity: ERROR

  Message Text: Failed to update ACI Service in ISE

  Message Description: Failed to update ACI Service in ISE

Local Target Message Format: <timestamp> <seq_num>61204 ERROR TrustSec Failed to update ACI Service in ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61204 ERROR TrustSec Failed to update ACI Service in ISE, <log details>

- **Message Code:** 61205

  Severity: INFO

  Message Text: Deleted ACI Service in ISE

  Message Description: Deleted ACI Service in ISE

  Local Target Message Format: <timestamp> <seq_num>61205 INFO TrustSec Deleted ACI Service in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61205 INFO TrustSec Deleted ACI Service in ISE, <log details>

- **Message Code:** 61206

  Severity: ERROR

  Message Text: Failed to delete ACI Service in ISE

  Message Description: Failed to delete ACI Service in ISE

  Local Target Message Format: <timestamp> <seq_num>61206 ERROR TrustSec Failed to delete ACI Service in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61206 ERROR TrustSec Failed to delete ACI Service in ISE, <log details>

- **Message Code:** 61207

  Severity: INFO

  Message Text: Published mdpConsumerServiceRequest to ACI

  Message Description: Published mdpConsumerServiceRequest to ACI

  Local Target Message Format: <timestamp> <seq_num>61207 INFO TrustSec Published mdpConsumerServiceRequest to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61207 INFO TrustSec Published mdpConsumerServiceRequest to ACI, <log details>

- **Message Code:** 61208

  Severity: ERROR

  Message Text: Failed to publish mdpConsumerServiceRequest to ACI

  Message Description: Failed to publish mdpConsumerServiceRequest to ACI

Local Target Message Format: <timestamp> <seq_num>61208 ERROR TrustSec Failed to publish mdpConsumerServiceRequest to ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61208 ERROR TrustSec Failed to publish mdpConsumerServiceRequest to ACI, <log details>

- **Message Code:** 61209

  Severity: INFO

  Message Text: ISE has propagated a new EEPG to ACI

  Message Description: ISE has propagated a new EEPG to ACI

  Local Target Message Format: <timestamp> <seq_num>61209 INFO TrustSec ISE has propagated a new EEPG to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61209 INFO TrustSec ISE has propagated a new EEPG to ACI, <log details>

- **Message Code:** 61210

  Severity: ERROR

  Message Text: ISE has failed to propagate a new EEPG to ACI

  Message Description: ISE has failed to propagate a new EEPG to ACI

  Local Target Message Format: <timestamp> <seq_num>61210 ERROR TrustSec ISE has failed to propagate a new EEPG to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61210 ERROR TrustSec ISE has failed to propagate a new EEPG to ACI, <log details>

- **Message Code:** 61211

  Severity: INFO

  Message Text: Received Endpoint message from ISE

  Message Description: Received Endpoint message from ISE

  Local Target Message Format: <timestamp> <seq_num>61211 INFO TrustSec Received Endpoint message from ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61211 INFO TrustSec Received Endpoint message from ISE, <log details>

- **Message Code:** 61212

  Severity: INFO

  Message Text: Published Endpoint to ACI

  Message Description: Published Endpoint to ACI

Local Target Message Format: <timestamp> <seq_num>61212 INFO TrustSec Published Endpoint to ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61212 INFO TrustSec Published Endpoint to ACI, <log details>

- **Message Code:** 61213

  Severity: ERROR

  Message Text: Failed to publish Endpoint to ACI

  Message Description: Failed to publish Endpoint to ACI

  Local Target Message Format: <timestamp> <seq_num>61213 ERROR TrustSec Failed to publish Endpoint to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61213 ERROR TrustSec Failed to publish Endpoint to ACI, <log details>

- **Message Code:** 61214

  Severity: INFO

  Message Text: Publishing endpoints addition to SDA

  Message Description: Publishing endpoints addition to SDA

  Local Target Message Format: <timestamp> <seq_num>61214 INFO TrustSec Publishing endpoints addition to SDA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61214 INFO TrustSec Publishing endpoints addition to SDA, <log details>

- **Message Code:** 61215

  Severity: INFO

  Message Text: Publishing endpoints deletion to SDA

  Message Description: Publishing endpoints deletion to SDA

  Local Target Message Format: <timestamp> <seq_num>61215 INFO TrustSec Publishing endpoints deletion to SDA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61215 INFO TrustSec Publishing endpoints deletion to SDA, <log details>

- **Message Code:** 61216

  Severity: ERROR

  Message Text: Failed to publish ACI binding to SDA

  Message Description: Failed to publish ACI binding to SDA

Local Target Message Format: <timestamp> <seq_num>61216 ERROR TrustSec Failed to publish ACI binding to SDA, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61216 ERROR TrustSec Failed to publish ACI binding to SDA, <log details>

- **Message Code:** 61217

  Severity: ERROR

  Message Text: Failed to publish message to SXP

  Message Description: Failed to publish message to SXP

  Local Target Message Format: <timestamp> <seq_num>61217 ERROR TrustSec Failed to publish message to SXP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61217 ERROR TrustSec Failed to publish message to SXP, <log details>

- **Message Code:** 61218

  Severity: INFO

  Message Text: Published ACI binding to SXP

  Message Description: Published ACI binding to SXP

  Local Target Message Format: <timestamp> <seq_num>61218 INFO TrustSec Published ACI binding to SXP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61218 INFO TrustSec Published ACI binding to SXP, <log details>

- **Message Code:** 61219

  Severity: ERROR

  Message Text: Failed to publish ACI binding to SXP

  Message Description: Failed to publish ACI binding to SXP

  Local Target Message Format: <timestamp> <seq_num>61219 ERROR TrustSec Failed to publish ACI binding to SXP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61219 ERROR TrustSec Failed to publish ACI binding to SXP, <log details>

- **Message Code:** 61220

  Severity: INFO

  Message Text: Published sxp binding from SXP to ISE

  Message Description: Published sxp binding from SXP to ISE

Local Target Message Format: <timestamp> <seq_num>61220 INFO TrustSec Published sxp binding from SXP to ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61220 INFO TrustSec Published sxp binding from SXP to ISE, <log details>

- **Message Code:** 61221

  Severity: ERROR

  Message Text: Failed to publish sxp binding from SXP to ISE

  Message Description: Failed to publish sxp binding from SXP to ISE

  Local Target Message Format: <timestamp> <seq_num>61221 ERROR TrustSec Failed to publish sxp binding from SXP to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61221 ERROR TrustSec Failed to publish sxp binding from SXP to ISE, <log details>

- **Message Code:** 61222

  Severity: INFO

  Message Text: Received EndPointGroup message from ACI

  Message Description: Received EndPointGroup message from ACI

  Local Target Message Format: <timestamp> <seq_num>61222 INFO TrustSec Received EndPointGroup message from ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61222 INFO TrustSec Received EndPointGroup message from ACI, <log details>

- **Message Code:** 61223

  Severity: ERROR

  Message Text: Failed to store new SGT in ISE

  Message Description: Failed to store new SGT in ISE

  Local Target Message Format: <timestamp> <seq_num>61223 ERROR TrustSec Failed to store new SGT in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61223 ERROR TrustSec Failed to store new SGT in ISE, <log details>

- **Message Code:** 61224

  Severity: INFO

  Message Text: Received EndPointGroup message from SDA

  Message Description: Received EndPointGroup message from SDA

Local Target Message Format: <timestamp> <seq_num>61224 INFO TrustSec Received EndPointGroup message from SDA, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61224 INFO TrustSec Received EndPointGroup message from SDA, <log details>

- **Message Code:** 61225

  Severity: INFO

  Message Text: SGT is alreaty published to ACI

  Message Description: SGT is alreaty published to ACI

  Local Target Message Format: <timestamp> <seq_num>61225 INFO TrustSec SGT is alreaty published to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61225 INFO TrustSec SGT is alreaty published to ACI, <log details>

- **Message Code:** 61226

  Severity: INFO

  Message Text: Published SGT to ACI

  Message Description: Published SGT to ACI

  Local Target Message Format: <timestamp> <seq_num>61226 INFO TrustSec Published SGT to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61226 INFO TrustSec Published SGT to ACI, <log details>

- **Message Code:** 61227

  Severity: ERROR

  Message Text: Failed publishing SGT to ACI

  Message Description: Failed publishing SGT to ACI

  Local Target Message Format: <timestamp> <seq_num>61227 ERROR TrustSec Failed publishing SGT to ACI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61227 ERROR TrustSec Failed publishing SGT to ACI, <log details>

- **Message Code:** 61228

  Severity: INFO

  Message Text: ISE has created a new SGT based on learned IEPG

  Message Description: ISE has created a new SGT based on learned IEPG

Local Target Message Format: <timestamp> <seq_num>61228 INFO TrustSec ISE has created a new SGT based on learned IEPG, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61228 INFO TrustSec ISE has created a new SGT based on learned IEPG, <log details>

- **Message Code:** 61229

  Severity: INFO

  Message Text: ISE has updated a SGT based on learned IEPG

  Message Description: ISE has updated a SGT based on learned IEPG

  Local Target Message Format: <timestamp> <seq_num>61229 INFO TrustSec ISE has updated a SGT based on learned IEPG, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61229 INFO TrustSec ISE has updated a SGT based on learned IEPG, <log details>

- **Message Code:** 61230

  Severity: INFO

  Message Text: ISE has removed a SGT based on deleted IEPG

  Message Description: ISE has removed a SGT based on deleted IEPG

  Local Target Message Format: <timestamp> <seq_num>61230 INFO TrustSec ISE has removed a SGT based on deleted IEPG, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61230 INFO TrustSec ISE has removed a SGT based on deleted IEPG, <log details>

- **Message Code:** 61231

  Severity: WARN

  Message Text: Kafka connection to ACI error while receiving message

  Message Description: Kafka connection to ACI error while receiving message

  Local Target Message Format: <timestamp> <seq_num>61231 WARN TrustSec Kafka connection to ACI error while receiving message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61231 WARN TrustSec Kafka connection to ACI error while receiving message, <log details>

- **Message Code:** 61232

  Severity: WARN

  Message Text: Kafka connection to ACI error while sending message

  Message Description: Kafka connection to ACI error while sending message

Local Target Message Format: <timestamp> <seq_num>61232 WARN TrustSec Kafka connection to ACI error while sending message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61232 WARN TrustSec Kafka connection to ACI error while sending message, <log details>

- **Message Code:** 61233

  Severity: INFO

  Message Text: Handling ACI message failure

  Message Description: Handling ACI message failure

  Local Target Message Format: <timestamp> <seq_num>61233 INFO TrustSec Handling ACI message failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61233 INFO TrustSec Handling ACI message failure, <log details>

- **Message Code:** 61234

  Severity: WARN

  Message Text: Got event with unknown properties

  Message Description: Got event with unknown properties

  Local Target Message Format: <timestamp> <seq_num>61234 WARN TrustSec Got event with unknown properties, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61234 WARN TrustSec Got event with unknown properties, <log details>

- **Message Code:** 61235

  Severity: INFO

  Message Text: SDA authenticated against ACI successfully

  Message Description: SDA authenticated against ACI successfully

  Local Target Message Format: <timestamp> <seq_num>61235 INFO TrustSec SDA authenticated against ACI successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61235 INFO TrustSec SDA authenticated against ACI successfully, <log details>

- **Message Code:** 61236

  Severity: ERROR

  Message Text: SDA failed to authenticate against ACI

  Message Description: SDA failed to authenticate against ACI

Local Target Message Format: <timestamp> <seq_num>61236 ERROR TrustSec SDA failed to authenticate against ACI, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61236 ERROR TrustSec SDA failed to authenticate against ACI, <log details>

- **Message Code:** 62000

  Severity: INFO

  Message Text: Agentless script execute completed

  Message Description: Agentless script execute completed

  Local Target Message Format: <timestamp> <seq_num>62000 INFO AgentlessPosture Agentless script execute completed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62000 INFO AgentlessPosture Agentless script execute completed, <log details>

- **Message Code:** 62001

  Severity: WARN

  Message Text: Agentless script execute failed

  Message Description: Agentless script execute failed

  Local Target Message Format: <timestamp> <seq_num>62001 WARN AgentlessPosture Agentless script execute failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62001 WARN AgentlessPosture Agentless script execute failed, <log details>

- **Message Code:** 62002

  Severity: INFO

  Message Text: Agentless script upload completed

  Message Description: Agentless script upload completed

  Local Target Message Format: <timestamp> <seq_num>62002 INFO AgentlessPosture Agentless script upload completed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62002 INFO AgentlessPosture Agentless script upload completed, <log details>

- **Message Code:** 62003

  Severity: WARN

  Message Text: Agentless script upload failed

  Message Description: Agentless script upload failed

Local Target Message Format: <timestamp> <seq_num>62003 WARN AgentlessPosture Agentless script upload failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62003 WARN AgentlessPosture Agentless script upload failed, <log details>

- **Message Code:** 60181

  Severity: INFO

  Message Text: pxGrid cloud device cleanup request completed successfully

  Message Description: pxGrid cloud device cleanup request completed successfully

  Local Target Message Format: <timestamp> <seq_num>60181 INFO System-Management pxGrid cloud device cleanup request completed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60181 INFO System-Management pxGrid cloud device cleanup request completed successfully, <log details>

- **Message Code:** 61080

  Severity: WARN

  Message Text: High Database Tablespace Usage

  Message Description: The system is experiencing high database tablespace usage

  Local Target Message Format: <timestamp> <seq_num>61080 WARN System-Management High Database Tablespace Usage, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61080 WARN System-Management High Database Tablespace Usage, <log details>

- **Message Code:** 61237

  Severity: WARN

  Message Text: ACI rejected SDA peering request

  Message Description: ACI rejected SDA peering request

  Local Target Message Format: <timestamp> <seq_num>61237 WARN TrustSec ACI rejected SDA peering request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61237 WARN TrustSec ACI rejected SDA peering request, <log details>

- **Message Code:** 61238

  Severity: WARN

  Message Text: SDA rejected ACI peering request

  Message Description: SDA rejected ACI peering request

Local Target Message Format: <timestamp> <seq_num>61238 WARN TrustSec SDA rejected ACI peering request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61238 WARN TrustSec SDA rejected ACI peering request, <log details>

- **Message Code:** 61239

  Severity: WARN

  Message Text: ACI rejected SDA delete peering request

  Message Description: ACI rejected SDA delete peering request

  Local Target Message Format: <timestamp> <seq_num>61239 WARN TrustSec ACI rejected SDA delete peering request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61239 WARN TrustSec ACI rejected SDA delete peering request, <log details>

- **Message Code:** 61240

  Severity: WARN

  Message Text: SDA rejected ACI delete peering request

  Message Description: SDA rejected ACI delete peering request

  Local Target Message Format: <timestamp> <seq_num>61240 WARN TrustSec SDA rejected ACI delete peering request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61240 WARN TrustSec SDA rejected ACI delete peering request, <log details>

- **Message Code:** 61241

  Severity: WARN

  Message Text: ACI rejected SDA extend VN request

  Message Description: ACI rejected SDA extend VN request

  Local Target Message Format: <timestamp> <seq_num>61241 WARN TrustSec ACI rejected SDA extend VN request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61241 WARN TrustSec ACI rejected SDA extend VN request, <log details>

- **Message Code:** 61242

  Severity: WARN

  Message Text: ACI rejected SDA delete extend VN request

  Message Description: ACI rejected SDA delete extend VN request

Local Target Message Format: <timestamp> <seq_num>61242 WARN TrustSec ACI rejected SDA delete extend VN request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61242 WARN TrustSec ACI rejected SDA delete extend VN request, <log details>

- **Message Code:** 61243

  Severity: WARN

  Message Text: ACI rejected SDA consume service request

  Message Description: ACI rejected SDA consume service request

  Local Target Message Format: <timestamp> <seq_num>61243 WARN TrustSec ACI rejected SDA consume service request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61243 WARN TrustSec ACI rejected SDA consume service request, <log details>

- **Message Code:** 61246

  Severity: WARN

  Message Text: ACI rejected SDA delete consume service request

  Message Description: ACI rejected SDA delete consume service request

  Local Target Message Format: <timestamp> <seq_num>61246 WARN TrustSec ACI rejected SDA delete consume service request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61246 WARN TrustSec ACI rejected SDA delete consume service request, <log details>

- **Message Code:** 61244

  Severity: WARN

  Message Text: PxGrid is not enabled and connected now, cannot publish bindings

  Message Description: PxGrid is not enabled and connected now, cannot publish bindings

  Local Target Message Format: <timestamp> <seq_num>61244 WARN TrustSec PxGrid is not enabled and connected now, cannot publish bindings, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61244 WARN TrustSec PxGrid is not enabled and connected now, cannot publish bindings, <log details>

- **Message Code:** 61245

  Severity: ERROR

  Message Text: PxGrid failed to publish bindings

  Message Description: PxGrid failed to publish bindings

Local Target Message Format: <timestamp> <seq_num>61245 ERROR TrustSec PxGrid failed to publish bindings, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61245 ERROR TrustSec PxGrid failed to publish bindings, <log details>

- **Message Code:** 62004

  Severity: INFO

  Message Text: Posture Remediation event was received

  Message Description: Posture Remediation event was received

  Local Target Message Format: <timestamp> <seq_num>62004 INFO PostureRemediation Posture Remediation event was received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62004 INFO PostureRemediation Posture Remediation event was received, <log details>

- **Message Code:** 62005

  Severity: WARN

  Message Text: Vulnerability scan failure for endpoint probe data

  Message Description: This message is generated when endpoint has received vulnerable data for XSS vulnerability scan.

  Local Target Message Format: <timestamp> <seq_num>62005 WARN Profiler Vulnerability scan failure for endpoint probe data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62005 WARN Profiler Vulnerability scan failure for endpoint probe data, <log details>

- **Message Code:** 61300

  Severity: INFO

  Message Text: Network Access policy request

  Message Description: Network Access policy request

  Local Target Message Format: <timestamp> <seq_num>61300 INFO OpenAPI Network Access policy request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61300 INFO OpenAPI Network Access policy request, <log details>

- **Message Code:** 61301

  Severity: INFO

  Message Text: Device Admin policy request

  Message Description: Device Admin policy request

Local Target Message Format: <timestamp> <seq_num>61301 INFO OpenAPI Device Admin policy request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61301 INFO OpenAPI Device Admin policy request, <log details>

- **Message Code:** 61302

  Severity: INFO

  Message Text: Policy component request

  Message Description: Policy component request

  Local Target Message Format: <timestamp> <seq_num>61302 INFO OpenAPI Policy component request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61302 INFO OpenAPI Policy component request, <log details>

- **Message Code:** 61304

  Severity: INFO

  Message Text: User has requested and seen Radius password

  Message Description: User has requested and seen Radius password

  Local Target Message Format: <timestamp> <seq_num>61304 INFO System-Management User has requested and seen Radius password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61304 INFO System-Management User has requested and seen Radius password, <log details>

- **Message Code:** 61305

  Severity: INFO

  Message Text: User has requested and seen Ipsec shared key

  Message Description: User has requested and seen Ipsec shared key

  Local Target Message Format: <timestamp> <seq_num>61305 INFO System-Management User has requested and seen Ipsec shared key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61305 INFO System-Management User has requested and seen Ipsec shared key, <log details>

- **Message Code:** 60467

  Severity: ERROR

  Message Text: OCSP Certificate renewal failed

  Message Description: OCSP Certificate renewal failed.

Local Target Message Format: <timestamp> <seq_num>60467 ERROR System-Management OCSP Certificate renewal failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60467 ERROR System-Management OCSP Certificate renewal failed, <log details>

- **Message Code:** 60468

  Severity: ERROR

  Message Text: Root CA Regeneration failed

  Message Description: Regeneration of Root CA failed.

  Local Target Message Format: <timestamp> <seq_num>60468 ERROR System-Management Root CA Regeneration failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60468 ERROR System-Management Root CA Regeneration failed, <log details>

- **Message Code:** 60466

  Severity: ERROR

  Message Text: Unable to regenerate CA certs on secondary node

  Message Description: No new CA certficates has been generated for secondary node since the communication gap between primary and secondary nodes

  Local Target Message Format: <timestamp> <seq_num>60466 ERROR System-Management Unable to regenerate CA certs on secondary node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>60466 ERROR System-Management Unable to regenerate CA certs on secondary node, <log details>

- **Message Code:** 61081

  Severity: ERROR

  Message Text: ERS packets dropped as packets rate limit was exceeded

  Message Description: ERS packets dropped as packets rate limit was exceeded

  Local Target Message Format: <timestamp> <seq_num>61081 ERROR Administrative and Operational Audit ERS packets dropped as packets rate limit was exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61081 ERROR Administrative and Operational Audit ERS packets dropped as packets rate limit was exceeded, <log details>

- **Message Code:** 61082

  Severity: ERROR

  Message Text: Synflood packets dropped as packets synflood limit was exceeded

  Message Description: Synflood packets dropped as packets synflood limit was exceeded

Local Target Message Format: <timestamp> <seq_num>61082 ERROR Administrative and Operational Audit Synflood packets dropped as packets synflood limit was exceeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61082 ERROR Administrative and Operational Audit Synflood packets dropped as packets synflood limit was exceeded, <log details>

- **Message Code:** 62007

  Severity: INFO

  Message Text: The upgrade flow was executed

  Message Description: The upgrade flow was executed

  Local Target Message Format: <timestamp> <seq_num>62007 INFO UpgradeAudit The upgrade flow was executed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62007 INFO UpgradeAudit The upgrade flow was executed, <log details>

- **Message Code:** 62008

  Severity: INFO

  Message Text: Meraki connector sync service starts

  Message Description: Meraki connector sync service starts

  Local Target Message Format: <timestamp> <seq_num>62008 INFO Meraki-Connector Meraki connector sync service starts, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62008 INFO Meraki-Connector Meraki connector sync service starts, <log details>

- **Message Code:** 62009

  Severity: INFO

  Message Text: Meraki connector sync service stops

  Message Description: Meraki connector sync service stops

  Local Target Message Format: <timestamp> <seq_num>62009 INFO Meraki-Connector Meraki connector sync service stops, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62009 INFO Meraki-Connector Meraki connector sync service stops, <log details>

- **Message Code:** 62010

  Severity: WARN

  Message Text: Meraki connector sync service failure

  Message Description: Meraki connector sync service failure

Local Target Message Format: <timestamp> <seq_num>62010 WARN Meraki-Connector Meraki connector sync service failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62010 WARN Meraki-Connector Meraki connector sync service failure, <log details>

- **Message Code:** 62011

  Severity: INFO

  Message Text: Meraki connector sync cycle starts

  Message Description: Meraki connector sync cycle starts

  Local Target Message Format: <timestamp> <seq_num>62011 INFO Meraki-Connector Meraki connector sync cycle starts, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62011 INFO Meraki-Connector Meraki connector sync cycle starts, <log details>

- **Message Code:** 62012

  Severity: INFO

  Message Text: Meraki connector sync cycle stops

  Message Description: Meraki connector sync cycle stops

  Local Target Message Format: <timestamp> <seq_num>62012 INFO Meraki-Connector Meraki connector sync cycle stops, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62012 INFO Meraki-Connector Meraki connector sync cycle stops, <log details>

- **Message Code:** 62013

  Severity: WARN

  Message Text: Meraki connector sync cycle failure

  Message Description: Meraki connector sync cycle failure

  Local Target Message Format: <timestamp> <seq_num>62013 WARN Meraki-Connector Meraki connector sync cycle failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62013 WARN Meraki-Connector Meraki connector sync cycle failure, <log details>

- **Message Code:** 62014

  Severity: INFO

  Message Text: Meraki connector sync operation success

  Message Description: Meraki connector sync operation success

Local Target Message Format: <timestamp> <seq_num>62014 INFO Meraki-Connector Meraki connector sync operation success, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62014 INFO Meraki-Connector Meraki connector sync operation success, <log details>

- **Message Code:** 62015

  Severity: WARN

  Message Text: Meraki connector sync operation failure

  Message Description: Meraki connector sync operation failure

  Local Target Message Format: <timestamp> <seq_num>62015 WARN Meraki-Connector Meraki connector sync operation failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62015 WARN Meraki-Connector Meraki connector sync operation failure, <log details>

- **Message Code:** 62016

  Severity: INFO

  Message Text: Port 2484 opened for Data Connect

  Message Description: Port 2484 opened for Data Connect

  Local Target Message Format: <timestamp> <seq_num>62016 INFO Data-Connect Port 2484 opened for Data Connect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62016 INFO Data-Connect Port 2484 opened for Data Connect, <log details>

- **Message Code:** 62017

  Severity: INFO

  Message Text: Data Connect port 2484 closed

  Message Description: Data Connect port 2484 closed

  Local Target Message Format: <timestamp> <seq_num>62017 INFO Data-Connect Data Connect port 2484 closed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62017 INFO Data-Connect Data Connect port 2484 closed, <log details>

- **Message Code:** 62018

  Severity: INFO

  Message Text: Posture OS Query Condition event was received

  Message Description: Posture OS Query Condition event was received

Local Target Message Format: <timestamp> <seq_num>62018 INFO PostureOSQueryCondition Posture OS Query Condition event was received, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62018 INFO PostureOSQueryCondition Posture OS Query Condition event was received, <log details>

- **Message Code:** 62019

  Severity: INFO

  Message Text: EndPoint SNMP Scan Event Received

  Message Description: This message is generated when an endpoint is scanned using SNMP Scanner.

  Local Target Message Format: <timestamp> <seq_num>Profiler EndPoint SNMP Scan Event Received INFO This message is generated when an endpoint is scanned using SNMP Scanner, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Profiler EndPoint SNMP Scan Event Received INFO This message is generated when an endpoint is scanned using SNMP Scanner, <log details>

- **Message Code:** 62020

  Severity: WARN

  Message Text: EndPoint SNMP Scan Failed

  Message Description: This message is generated when an endpoint Scan is failed

  Local Target Message Format: <timestamp> <seq_num>Profiler EndPoint SNMP Scan Failed WARN This message is generated when an endpoint Scan is failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Profiler EndPoint SNMP Scan Failed WARN This message is generated when an endpoint Scan is failed, <log details>

- **Message Code:** 62021

  Severity: WARN

  Message Text: EndPoint SNMP Scan Stopped By User

  Message Description: This message is generated when an endpoint Scan is Stopped By user

  Local Target Message Format: <timestamp> <seq_num>Profiler EndPoint SNMP Scan Stopped By User WARN This message is generated when an endpoint Scan is Stopped By user, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Profiler EndPoint SNMP Scan Stopped By User WARN This message is generated when an endpoint Scan is Stopped By user, <log details>

- **Message Code:** 62022

  Severity: WARN

  Message Text: EndPoint SNMP Scan System Failure

  Message Description: This message is generated when an endpoint Scan is because of System Errors

Local Target Message Format: <timestamp> <seq_num>Profiler EndPoint SNMP Scan System Failure WARN This message is generated when an endpoint Scan is because of System Errors, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Profiler EndPoint SNMP Scan System Failure WARN This message is generated when an endpoint Scan is because of System Errors, <log details>

- **Message Code:** 62006

  Severity: INFO

  Message Text: Posture Script Condition event was received

  Message Description: Posture Script Condition event was received

  Local Target Message Format: <timestamp> <seq_num>62006 INFO PostureScriptCondition Posture Script Condition event was received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>62006 INFO PostureScriptCondition Posture Script Condition event was received, <log details>

- **Message Code:** 61303

  Severity: INFO

  Message Text: OpenApi request

  Message Description: OpenApi request

  Local Target Message Format: <timestamp> <seq_num>61303 INFO OpenAPI OpenApi request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>61303 INFO OpenAPI OpenApi request, <log details>

- **Message Code:** 60469

  Severity: INFO

  Message Text: Admin certificate replaced on PPAN and all node(s) will be restarted based on configuration

  Message Description: Admin certificate replaced on PPAN and all node(s) will be restarted based on configuration

  Local Target Message Format: <timestamp> <seq_num>System-Management Admin certificate replaced on PPAN and all node(s) will be restarted based on configuration INFO Admin certificate replaced on PPAN and all node(s) will be restarted based on configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Admin certificate replaced on PPAN and all node(s) will be restarted based on configuration INFO Admin certificate replaced on PPAN and all node(s) will be restarted based on configuration, <log details>

- **Message Code:** 60470

  Severity: WARN

Message Text: Below node(s) will be restarted in 5 days, please plan accordingly

Message Description: Below node(s) will be restarted in 5 days, please plan accordingly

Local Target Message Format: <timestamp> <seq_num>System-Management Below node(s) will be restarted in 5 days, please plan accordingly WARN Below node(s) will be restarted in 5 days, please plan accordingly, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Below node(s) will be restarted in 5 days, please plan accordingly WARN Below node(s) will be restarted in 5 days, please plan accordingly, <log details>

- **Message Code:** 60472

  Severity: ERROR

  Message Text: Below node(s) restart failed, please check and restart manually if required

  Message Description: Below node(s) restart failed, please check and restart manually if required

  Local Target Message Format: <timestamp> <seq_num>System-Management Below node(s) restart failed, please check and restart manually if required ERROR Below node(s) restart failed, please check and restart manually if required, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Below node(s) restart failed, please check and restart manually if required ERROR Below node(s) restart failed, please check and restart manually if required, <log details>

- **Message Code:** 60477

  Severity: INFO

  Message Text: GC is taking time to complete.

  Message Description: GC is taking time to complete.

  Local Target Message Format: <timestamp> <seq_num>System-Management GC is taking time to complete. INFO GC is taking time to complete., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management GC is taking time to complete. INFO GC is taking time to complete., <log details>

- **Message Code:** 60479

  Severity: ERROR

  Message Text: GC is taking time to complete.

  Message Description: GC is taking time to complete.

  Local Target Message Format: <timestamp> <seq_num>System-Management GC is taking time to complete. ERROR GC is taking time to complete., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management GC is taking time to complete. ERROR GC is taking time to complete., <log details>

- **Message Code:** 60478

  Severity: WARN

  Message Text: GC is taking time to complete.

  Message Description: GC is taking time to complete.

  Local Target Message Format: <timestamp> <seq_num>System-Management GC is taking time to complete. WARN GC is taking time to complete., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management GC is taking time to complete. WARN GC is taking time to complete., <log details>

- **Message Code:** 61083

  Severity: ERROR

  Message Text: Unable to create ISE system certificate private key

  Message Description: Unable to create ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to create ISE system certificate private key ERROR Unable to create ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to create ISE system certificate private key ERROR Unable to create ISE system certificate private key, <log details>

- **Message Code:** 61084

  Severity: ERROR

  Message Text: Unable to validate and attach private key of ISE system certificate private key

  Message Description: Unable to validate and attach private key of ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to validate and attach private key of ISE system certificate private key ERROR Unable to validate and attach private key of ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to validate and attach private key of ISE system certificate private key ERROR Unable to validate and attach private key of ISE system certificate private key, <log details>

- **Message Code:** 61085

  Severity: ERROR

  Message Text: Unable to store private key of ISE system certificate private key

  Message Description: Unable to store private key of ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to store private key of ISE system certificate private key ERROR Unable to store private key of ISE system certificate private key, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to store private key of ISE system certificate private key ERROR Unable to store private key of ISE system certificate private key, <log details>

- **Message Code:** 61086

  Severity: ERROR

  Message Text: Unable to encrypt a new private key encryption password of ISE system certificate private key

  Message Description: Unable to encrypt a new private key encryption password of ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to encrypt a new private key encryption password of ISE system certificate private key ERROR Unable to encrypt a new private key encryption password of ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to encrypt a new private key encryption password of ISE system certificate private key ERROR Unable to encrypt a new private key encryption password of ISE system certificate private key, <log details>

- **Message Code:** 61087

  Severity: ERROR

  Message Text: Unable to encode ISE system certificate private key

  Message Description: Unable to encode ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to encode ISE system certificate private key ERROR Unable to encode ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to encode ISE system certificate private key ERROR Unable to encode ISE system certificate private key, <log details>

- **Message Code:** 61088

  Severity: INFO

  Message Text: Successfully imported ISE system certificate private key

  Message Description: Successfully imported ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Successfully imported ISE system certificate private key INFO Successfully imported ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Successfully imported ISE system certificate private key INFO Successfully imported ISE system certificate private key, <log details>

- **Message Code:** 61089

Severity: INFO

Message Text: Successfully deleted ISE system certificate private key

Message Description: Successfully deleted ISE system certificate private key

Local Target Message Format: <timestamp> <seq_num>System-Management Successfully deleted ISE system certificate private key INFO Successfully deleted ISE system certificate private key, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Successfully deleted ISE system certificate private key INFO Successfully deleted ISE system certificate private key, <log details>

- **Message Code:** 61090

  Severity: ERROR

  Message Text: Unable to decrypt password of ISE system certificate private key

  Message Description: Unable to decrypt password of ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to decrypt password of ISE system certificate private key ERROR Unable to decrypt password of ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to decrypt password of ISE system certificate private key ERROR Unable to decrypt password of ISE system certificate private key, <log details>

- **Message Code:** 61091

  Severity: ERROR

  Message Text: Unable to find private key of ISE system certificate

  Message Description: Unable to find private key of ISE system certificate

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to find private key of ISE system certificate ERROR Unable to find private key of ISE system certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to find private key of ISE system certificate ERROR Unable to find private key of ISE system certificate, <log details>

- **Message Code:** 61092

  Severity: ERROR

  Message Text: Unable to verify ISE system certificate private key

  Message Description: Unable to verify ISE system certificate private key

  Local Target Message Format: <timestamp> <seq_num>System-Management Unable to verify ISE system certificate private key ERROR Unable to verify ISE system certificate private key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Unable to

verify ISE system certificate private key ERROR Unable to verify ISE system certificate private key, <log details>

- **Message Code:** 63001

  Severity: NOTICE

  Message Text: Common Policy Context data was received

  Message Description: Got Common Policy Context data was received

  Local Target Message Format: <timestamp> <seq_num>CommonPolicy Common Policy Context data was received NOTICE Got Common Policy Context data was received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>CommonPolicy Common Policy Context data was received NOTICE Got Common Policy Context data was received, <log details>

- **Message Code:** 63002

  Severity: NOTICE

  Message Text: Common Policy Context data was updated

  Message Description: Got Common Policy Context data was updated

  Local Target Message Format: <timestamp> <seq_num>CommonPolicy Common Policy Context data was updated NOTICE Got Common Policy Context data was updated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>CommonPolicy Common Policy Context data was updated NOTICE Got Common Policy Context data was updated, <log details>

- **Message Code:** 63003

  Severity: NOTICE

  Message Text: Common Policy Context data was deleted

  Message Description: Got Common Policy Context data was deleted

  Local Target Message Format: <timestamp> <seq_num>CommonPolicy Common Policy Context data was deleted NOTICE Got Common Policy Context data was deleted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>CommonPolicy Common Policy Context data was deleted NOTICE Got Common Policy Context data was deleted, <log details>

- **Message Code:** 63004

  Severity: NOTICE

  Message Text: Common Policy Context data was published

  Message Description: Got Common Policy Context data was published

  Local Target Message Format: <timestamp> <seq_num>CommonPolicy Common Policy Context data was published NOTICE Got Common Policy Context data was published, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>CommonPolicy Common Policy Context data was published NOTICE Got Common Policy Context data was published, <log details>

- **Message Code:** 63005

  Severity: ERROR

  Message Text: Common Policy Context sharing encountered unexpected error

  Message Description: Got Common Policy Context sharing encountered unexpected error

  Local Target Message Format: <timestamp> <seq_num>CommonPolicy Common Policy Context sharing encountered unexpected error ERROR Got Common Policy Context sharing encountered unexpected error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>CommonPolicy Common Policy Context sharing encountered unexpected error ERROR Got Common Policy Context sharing encountered unexpected error, <log details>

- **Message Code:** 63006

  Severity: INFO

  Message Text: ACI connector service starts

  Message Description: ACI connector service starts

  Local Target Message Format: <timestamp> <seq_num>TrustSec ACI connector service starts INFO ACI connector service starts, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>TrustSec ACI connector service starts INFO ACI connector service starts, <log details>

- **Message Code:** 63007

  Severity: INFO

  Message Text: ACI connector service stops

  Message Description: ACI connector service stops

  Local Target Message Format: <timestamp> <seq_num>TrustSec ACI connector service stops INFO ACI connector service stops, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>TrustSec ACI connector service stops INFO ACI connector service stops, <log details>

- **Message Code:** 63008

  Severity: WARN

  Message Text: ACI connector service failure

  Message Description: ACI connector service failure

  Local Target Message Format: <timestamp> <seq_num>TrustSec ACI connector service failure WARN ACI connector service failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>TrustSec ACI connector service failure WARN ACI connector service failure, <log details>

- **Message Code:** 64010

  Severity: WARN

  Message Text: Syslog server handshake failed. Curve name is not present in the public key

  Message Description: Syslog server handshake failed. Curve name is not present in the public key, Secure communication not established with syslog server

  Local Target Message Format: <timestamp> <seq_num>64010 WARN System-Management Syslog server handshake failed. Curve name is not present in the public key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>64010 WARN System-Management Syslog server handshake failed. Curve name is not present in the public key, <log details>

- **Message Code:** 64011

  Severity: ERROR

  Message Text: Could not add Certificate Revocation List due to CA SKI and CRL AKI mismatch

  Message Description: Could not add the Certificate Revocation List because, although the issuer name matches, the Subject Key Identifier (SKI) does not match the Authority Key Identifier (AKI) of the CA certificate. Ensure the CA SKI and CRL AKI match

  Local Target Message Format: <timestamp> <seq_num>64011 ERROR CRL Could not add Certificate Revocation List due to CA SKI and CRL AKI mismatch, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>64011 ERROR CRL Could not add Certificate Revocation List due to CA SKI and CRL AKI mismatch, <log details>

- **Message Code:** 64013

  Severity: INFO

  Message Text: Event related to monitoring of external REST Identity Stores.

  Message Description: Event related to monitoring of external REST Identity Stores.

  Local Target Message Format: <timestamp> <seq_num>External-REST Event related to monitoring of external REST Identity Stores. INFO Event related to monitoring of external REST Identity Stores., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>External-REST Event related to monitoring of external REST Identity Stores. INFO Event related to monitoring of external REST Identity Stores., <log details>

Administrator Authentication and Authorization

- **Message Code:** 10000

Severity: DEBUG

Message Text: Received Administrator authentication request

Message Description: Handling incoming Administrator authentication request

Local Target Message Format: <timestamp> <seq_num> 10000 DEBUG AAC: Received Administrator authentication request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10000 DEBUG AAC: Received Administrator authentication request, <log details>

- **Message Code:** 10001

  Severity: ERROR

  Message Text: Internal error. Incorrect configuration version

  Message Description: An internal error occurred: Undetermined configuration version

  Local Target Message Format: <timestamp> <seq_num> 10001 ERROR AAC: Internal error. Incorrect configuration version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10001 ERROR AAC: Internal error. Incorrect configuration version, <log details>

- **Message Code:** 10002

  Severity: ERROR

  Message Text: Internal error: Failure to load appropriate service

  Message Description: Internal error: Failure to load AAC service

  Local Target Message Format: <timestamp> <seq_num> 10002 ERROR AAC: Internal error: Failure to load appropriate service, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10002 ERROR AAC: Internal error: Failure to load appropriate service, <log details>

- **Message Code:** 10003

  Severity: ERROR

  Message Text: Internal error: Administrator authentication received blank Administrator name

  Message Description: Internal error: AAC RT component received Administrator authentication request with blank Administrator name

  Local Target Message Format: <timestamp> <seq_num> 10003 ERROR AAC: Internal error: Administrator authentication received blank Administrator name, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10003 ERROR AAC: Internal error: Administrator authentication received blank Administrator name, <log details>

- **Message Code:** 10004

Severity: ERROR

Message Text: Internal error: Administrator authentication received blank Administrator password

Message Description: Internal error: AAC RT component received an Administrator authentication request with blank admin password

Local Target Message Format: <timestamp> <seq_num> 10004 ERROR AAC: Internal error: Administrator authentication received blank Administrator password, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10004 ERROR AAC: Internal error: Administrator authentication received blank Administrator password, <log details>

- **Message Code:** 10005

  Severity: INFO

  Message Text: Administrator authenticated successfully

  Message Description: Administrator authenticated successfully

  Local Target Message Format: <timestamp> <seq_num> 10005 INFO AAC: Administrator authenticated successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10005 INFO AAC: Administrator authenticated successfully, <log details>

- **Message Code:** 10006

  Severity: INFO

  Message Text: Administrator authentication failed

  Message Description: Administrator authentication failed

  Local Target Message Format: <timestamp> <seq_num> 10006 INFO AAC: Administrator authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10006 INFO AAC: Administrator authentication failed, <log details>

- **Message Code:** 10007

  Severity: ERROR

  Message Text: Administrator authentication failed - DB Error

  Message Description: Administrator authentication failed - DB Error

  Local Target Message Format: <timestamp> <seq_num> 10007 ERROR AAC: Administrator authentication failed - DB Error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10007 ERROR AAC: Administrator authentication failed - DB Error, <log details>

- **Message Code:** 10008

Severity: DEBUG

Message Text: Received valid Administrator authentication request

Message Description: Received valid Administrator authentication request

Local Target Message Format: <timestamp> <seq_num> 10008 DEBUG AAC: Received valid Administrator authentication request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10008 DEBUG AAC: Received valid Administrator authentication request, <log details>

- **Message Code:** 10009

  Severity: DEBUG

  Message Text: Received Administrator authentication request

  Message Description: Successfully performed service selection

  Local Target Message Format: <timestamp> <seq_num> 10009 DEBUG AAC: Received Administrator authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10009 DEBUG AAC: Received Administrator authentication request, <log details>

- **Message Code:** 10010

  Severity: INFO

  Message Text: Admin password change reminder

  Message Description: Reminder - Please change the admin password

  Local Target Message Format: <timestamp> <seq_num> 10010 INFO AAC: Admin password change reminder, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10010 INFO AAC: Admin password change reminder, <log details>

- **Message Code:** 10011

  Severity: INFO

  Message Text: Admin password change required due to expired password

  Message Description: Admin password has expired -Please change it.

  Local Target Message Format: <timestamp> <seq_num> 10011 INFO AAC: Admin password change required due to expired password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10011 INFO AAC: Admin password change required due to expired password, <log details>

- **Message Code:** 10012

  Severity: INFO

Message Text: Admin password change required due to account inactivity

Message Description: Due to admin account inactivity the admin password must be changed.

Local Target Message Format: <timestamp> <seq_num> 10012 INFO AAC: Admin password change required due to account inactivity, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10012 INFO AAC: Admin password change required due to account inactivity, <log details>

- **Message Code:** 10013

  Severity: INFO

  Message Text: Admin account set as 'never disabled'

  Message Description: Admin account cannot be disabled since 'never disable' option is set.

  Local Target Message Format: <timestamp> <seq_num> 10013 INFO AAC: Admin account set as 'never disabled', <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10013 INFO AAC: Admin account set as 'never disabled', <log details>

- **Message Code:** 10014

  Severity: INFO

  Message Text: Admin account set to change password on next login

  Message Description: Admin account is set to change password at the next login

  Local Target Message Format: <timestamp> <seq_num> 10014 INFO AAC: Admin account set to change password on next login, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 10014 INFO AAC: Admin account set to change password on next login, <log details>

Authentication Flow Diagnostics

- **Message Code:** 22000

  Severity: ERROR

  Message Text: Authentication resulted in internal error

  Message Description: Authentication resulted in internal error

  Local Target Message Format: <timestamp> <seq_num> 22000 ERROR Authentication: Authentication resulted in internal error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22000 ERROR Authentication: Authentication resulted in internal error, <log details>

- **Message Code:** 22001

  Severity: INFO

  Message Text: Restricted attribute(s) found

  Message Description: Restricted attribute(s) found

  Local Target Message Format: <timestamp> <seq_num> 22001 INFO Authentication: Restricted attribute(s) found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22001 INFO Authentication: Restricted attribute(s) found, <log details>

- **Message Code:** 22002

  Severity: DEBUG

  Message Text: Authentication complete

  Message Description: Authentication complete

  Local Target Message Format: <timestamp> <seq_num> 22002 DEBUG Authentication: Authentication complete, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22002 DEBUG Authentication: Authentication complete, <log details>

- **Message Code:** 22003

  Severity: INFO

  Message Text: Missing attribute for authentication

  Message Description: Missing attribute for authentication

  Local Target Message Format: <timestamp> <seq_num> 22003 INFO Authentication: Missing attribute for authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22003 INFO Authentication: Missing attribute for authentication, <log details>

- **Message Code:** 22004

  Severity: INFO

  Message Text: Wrong password

  Message Description: Wrong password

  Local Target Message Format: <timestamp> <seq_num> 22004 INFO Authentication: Wrong password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22004 INFO Authentication: Wrong password, <log details>

- **Message Code:** 22005

Severity: INFO

Message Text: Could not get shell profile object

Message Description: Could not get shell profile object

Local Target Message Format: <timestamp> <seq_num> 22005 INFO Authentication: Could not get shell profile object, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22005 INFO Authentication: Could not get shell profile object, <log details>

- **Message Code:** 22006

  Severity: INFO

  Message Text: Shell profile object is not configured

  Message Description: Shell profile object is not configured

  Local Target Message Format: <timestamp> <seq_num> 22006 INFO Authentication: Shell profile object is not configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22006 INFO Authentication: Shell profile object is not configured, <log details>

- **Message Code:** 22007

  Severity: INFO

  Message Text: Username attribute is not present in the authentication request

  Message Description: Username attribute is not present in the authentication request.

  Local Target Message Format: <timestamp> <seq_num> 22007 INFO Authentication: Username attribute is not present in the authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22007 INFO Authentication: Username attribute is not present in the authentication request, <log details>

- **Message Code:** 22008

  Severity: DEBUG

  Message Text: Changing enable password is not allowed

  Message Description: Changing enable password is not allowed because user was authenticated against regular password

  Local Target Message Format: <timestamp> <seq_num> 22008 DEBUG Authentication : Changing enable password is not allowed , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22008 DEBUG Authentication : Changing enable password is not allowed , <log details>

- **Message Code:** 22015

Severity: DEBUG

Message Text: Identity sequence continues to the next IDStore

Message Description: Identity sequence continues to the next IDStore

Local Target Message Format: <timestamp> <seq_num> 22015 DEBUG Workflow: Identity sequence continues to the next IDStore, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22015 DEBUG Workflow: Identity sequence continues to the next IDStore, <log details>

- **Message Code:** 22016

  Severity: DEBUG

  Message Text: Identity sequence completed iterating the IDStores

  Message Description: Identity sequence completed iterating the IDStores

  Local Target Message Format: <timestamp> <seq_num> 22016 DEBUG Workflow: Identity sequence completed iterating the IDStores, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22016 DEBUG Workflow: Identity sequence completed iterating the IDStores, <log details>

- **Message Code:** 22017

  Severity: INFO

  Message Text: Selected Identity Source is DenyAccess

  Message Description: Selected Identity Source is DenyAccess

  Local Target Message Format: <timestamp> <seq_num> 22017 INFO Workflow: Selected Identity Source is DenyAccess, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22017 INFO Workflow: Selected Identity Source is DenyAccess, <log details>

- **Message Code:** 22019

  Severity: DEBUG

  Message Text: Identity Policy was evaluated before; Identity Sequence continuing

  Message Description: Identity Policy was evaluated before. Identity Sequence continuing

  Local Target Message Format: <timestamp> <seq_num> 22019 DEBUG Workflow: Identity Policy was evaluated before; Identity Sequence continuing, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22019 DEBUG Workflow: Identity Policy was evaluated before; Identity Sequence continuing, <log details>

- **Message Code:** 22020

  Severity: ERROR

Message Text: Configuration error: identity source blank

Message Description: Configuration error: identity source blank

Local Target Message Format: <timestamp> <seq_num> 22020 ERROR Workflow: Configuration error: identity source blank, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22020 ERROR Workflow: Configuration error: identity source blank, <log details>

- **Message Code:** 22021

  Severity: ERROR

  Message Text: Configuration error: authentication IDStores list blank

  Message Description: Configuration error, authentication IDStores list blank

  Local Target Message Format: <timestamp> <seq_num> 22021 ERROR Workflow: Configuration error: authentication IDStores list blank, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22021 ERROR Workflow: Configuration error: authentication IDStores list blank, <log details>

- **Message Code:** 22022

  Severity: ERROR

  Message Text: Error in setting fail open options

  Message Description: Error in setting fail open options

  Local Target Message Format: <timestamp> <seq_num> 22022 ERROR Workflow: Error in setting fail open options, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22022 ERROR Workflow: Error in setting fail open options, <log details>

- **Message Code:** 22023

  Severity: INFO

  Message Text: Proceed to attribute retrieval

  Message Description: Authentication completed successfully. Proceed to attribute retrieval

  Local Target Message Format: <timestamp> <seq_num> 22023 INFO Workflow: Proceed to attribute retrieval, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22023 INFO Workflow: Proceed to attribute retrieval, <log details>

- **Message Code:** 22028

  Severity: INFO

  Message Text: Authentication failed and the advanced options are ignored

Message Description: Authentication of the user failed and the advanced option settings specified in the identity portion of the relevant authentication policy were ignored. For PEAP, LEAP, EAP-FAST or RADIUS MSCHAP authentications, when authentication fails, ISE stops processing the request.

Local Target Message Format: <timestamp> <seq_num> 22028 INFO Workflow: Authentication failed and the advanced options are ignored, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22028 INFO Workflow: Authentication failed and the advanced options are ignored, <log details>

- **Message Code:** 22034

  Severity: INFO

  Message Text: Attribute retrieval failed

  Message Description: Attribute retrieval failed

  Local Target Message Format: <timestamp> <seq_num> 22034 INFO Workflow: Attribute retrieval failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22034 INFO Workflow: Attribute retrieval failed, <log details>

- **Message Code:** 22036

  Severity: INFO

  Message Text: Retrieved Attributes successfully from current IDStore

  Message Description: Retrieved Attributes successfully from the current IDStore

  Local Target Message Format: <timestamp> <seq_num> 22036 INFO Workflow: Retrieved Attributes successfully from current IDStore, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22036 INFO Workflow: Retrieved Attributes successfully from current IDStore, <log details>

- **Message Code:** 22037

  Severity: DEBUG

  Message Text: Authentication Passed

  Message Description: Authentication Passed, Skipping Attribute Retrieval

  Local Target Message Format: <timestamp> <seq_num> 22037 DEBUG Workflow: Authentication Passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22037 DEBUG Workflow: Authentication Passed, <log details>

- **Message Code:** 22038

  Severity: INFO

Message Text: Skipping the next IDStore for attribute retrieval because it is the one we authenticated against

Message Description: Skipping the next IDStore for attribute retrieval because it is the one we authenticated against

Local Target Message Format: <timestamp> <seq_num> 22038 INFO Workflow: Skipping the next IDStore for attribute retrieval because it is the one we authenticated against, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22038 INFO Workflow: Skipping the next IDStore for attribute retrieval because it is the one we authenticated against, <log details>

- **Message Code:** 22039

  Severity: ERROR

  Message Text: Invalid workflow sequence type

  Message Description: Invalid workflow sequence type

  Local Target Message Format: <timestamp> <seq_num> 22039 ERROR Workflow: Invalid workflow sequence type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22039 ERROR Workflow: Invalid workflow sequence type, <log details>

- **Message Code:** 22040

  Severity: INFO

  Message Text: Wrong password or invalid shared secret

  Message Description: Wrong password or invalid shared secret

  Local Target Message Format: <timestamp> <seq_num> 22040 INFO Authentication: Wrong password or invalid shared secret, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22040 INFO Authentication: Wrong password or invalid shared secret, <log details>

- **Message Code:** 22043

  Severity: INFO

  Message Text: Current Identity Store does not support the authentication method; Skipping it

  Message Description: Current Identity Store does not support the authentication method. Skipping it.

  Local Target Message Format: <timestamp> <seq_num> 22043 INFO Authentication: Current Identity Store does not support the authentication method; Skipping it, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22043 INFO Authentication: Current Identity Store does not support the authentication method; Skipping it, <log details>

- **Message Code:** 22044

  Severity: INFO

Message Text: Identity policy result is configured for certificate based authentication methods but received password based

Message Description: Identity policy result is configured for certificate based authentication methods but received password based

Local Target Message Format: <timestamp> <seq_num> 22044 INFO Workflow: Identity policy result is configured for certificate based authentication methods but received password based, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22044 INFO Workflow: Identity policy result is configured for certificate based authentication methods but received password based, <log details>

- **Message Code:** 22045

  Severity: INFO

  Message Text: Identity policy result is configured for password based authentication methods but received certificate based authentication request

  Message Description: Identity policy result is configured for password based authentication methods but received certificate based authentication request

  Local Target Message Format: <timestamp> <seq_num> 22045 INFO Workflow: Identity policy result is configured for password based authentication methods but received certificate based authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22045 INFO Workflow: Identity policy result is configured for password based authentication methods but received certificate based authentication request, <log details>

- **Message Code:** 22046

  Severity: DEBUG

  Message Text: Identity sequence received a certificate authentication request

  Message Description: Identity sequence received a certificate authentication request

  Local Target Message Format: <timestamp> <seq_num> 22046 DEBUG Workflow: Identity sequence received a certificate authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22046 DEBUG Workflow: Identity sequence received a certificate authentication request, <log details>

- **Message Code:** 22047

  Severity: DEBUG

  Message Text: User name attribute is missing in client certificate

  Message Description: User name attribute is missing in client certificate

  Local Target Message Format: <timestamp> <seq_num> 22047 DEBUG Authentication: User name attribute is missing in client certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22047 DEBUG Authentication: User name attribute is missing in client certificate, <log details>

- **Message Code:** 22048

  Severity: DEBUG

  Message Text: Client certificate binary is missing

  Message Description: Client certificate binary is missing

  Local Target Message Format: <timestamp> <seq_num> 22048 DEBUG Authentication: Client certificate binary is missing, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22048 DEBUG Authentication: Client certificate binary is missing, <log details>

- **Message Code:** 22049

  Severity: DEBUG

  Message Text: Binary comparison of certificates failed

  Message Description: Binary comparison of certificates failed

  Local Target Message Format: <timestamp> <seq_num> 22049 DEBUG Authentication: Binary comparison of certificates failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22049 DEBUG Authentication: Binary comparison of certificates failed, <log details>

- **Message Code:** 22050

  Severity: INFO

  Message Text: User or host disabled in current IDStore in attribute retrieval mode

  Message Description: The user or host is disabled in the current IDStore in attribute retrieval mode

  Local Target Message Format: <timestamp> <seq_num> 22050 INFO Workflow: User or host disabled in current IDStore in attribute retrieval mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22050 INFO Workflow: User or host disabled in current IDStore in attribute retrieval mode, <log details>

- **Message Code:** 22051

  Severity: INFO

  Message Text: User or host disabled in Internal IDStore, proceed according to Advanced Option

  Message Description: The user or host is disabled in the Internal IDStore, proceed according to Advanced Option

  Local Target Message Format: <timestamp> <seq_num> 22051 INFO Workflow: User or host disabled in Internal IDStore, proceed according to Advanced Option, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22051 INFO Workflow: User or host disabled in Internal IDStore, proceed according to Advanced Option, <log details>

- **Message Code:** 22052

  Severity: ERROR

  Message Text: Authentication IDStore empty after completing authentication

  Message Description: Authentication IDStore empty after completing authentication

  Local Target Message Format: <timestamp> <seq_num> 22052 ERROR Workflow: Authentication IDStore empty after completing authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22052 ERROR Workflow: Authentication IDStore empty after completing authentication, <log details>

- **Message Code:** 22054

  Severity: DEBUG

  Message Text: Binary comparison of certificates succeeded

  Message Description: Binary comparison of certificates succeeded.

  Local Target Message Format: <timestamp> <seq_num> 22054 DEBUG Authentication: Binary comparison of certificates succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22054 DEBUG Authentication: Binary comparison of certificates succeeded, <log details>

- **Message Code:** 22055

  Severity: INFO

  Message Text: Failed to find expected Principal Username X509 Attribute in user's certificate

  Message Description: The user's certificate does not contain the specific Principal Username X509 Attribute that has been configured in the selected Certificate Authentication Profile.

  Local Target Message Format: <timestamp> <seq_num> 22055 INFO Authentication: Failed to find expected Principal Username X509 Attribute in user's certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22055 INFO Authentication: Failed to find expected Principal Username X509 Attribute in user's certificate, <log details>

- **Message Code:** 22056

  Severity: DEBUG

  Message Text: Subject not found in the applicable identity store(s)

  Message Description: Subject not found in the applicable identity store(s).

  Local Target Message Format: <timestamp> <seq_num> 22056 DEBUG Workflow: Subject not found in the applicable identity store(s), <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22056 DEBUG Workflow: Subject not found in the applicable identity store(s), <log details>

- **Message Code:** 22057

  Severity: INFO

  Message Text: The advanced option that is configured for a failed authentication request is used

  Message Description: The advanced option that is configured for a failed authentication request is used.

  Local Target Message Format: <timestamp> <seq_num> 22057 INFO Workflow: The advanced option that is configured for a failed authentication request is used, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22057 INFO Workflow: The advanced option that is configured for a failed authentication request is used, <log details>

- **Message Code:** 22058

  Severity: INFO

  Message Text: The advanced option that is configured for an unknown user is used

  Message Description: The advanced option that is configured for an unknown user is used.

  Local Target Message Format: <timestamp> <seq_num> 22058 INFO Workflow: The advanced option that is configured for an unknown user is used, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22058 INFO Workflow: The advanced option that is configured for an unknown user is used, <log details>

- **Message Code:** 22059

  Severity: INFO

  Message Text: The advanced option that is configured for process failure is used

  Message Description: The advanced option that is configured for process failure is used.

  Local Target Message Format: <timestamp> <seq_num> 22059 INFO Workflow: The advanced option that is configured for process failure is used, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22059 INFO Workflow: The advanced option that is configured for process failure is used, <log details>

- **Message Code:** 22060

  Severity: INFO

  Message Text: The 'Continue' advanced option is configured in case of a failed authentication request

  Message Description: In case of a failed authentication request, the Continue advanced option is configured.

  Local Target Message Format: <timestamp> <seq_num> 22060 INFO Workflow: The 'Continue' advanced option is configured in case of a failed authentication request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22060 INFO Workflow: The 'Continue' advanced option is configured in case of a failed authentication request, <log details>

- **Message Code:** 22061

  Severity: INFO

  Message Text: The 'Reject' advanced option is configured in case of a failed authentication request

  Message Description: In case of a failed authentication request, the Reject advanced option is configured.

  Local Target Message Format: <timestamp> <seq_num> 22061 INFO Workflow: The 'Reject' advanced option is configured in case of a failed authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22061 INFO Workflow: The 'Reject' advanced option is configured in case of a failed authentication request, <log details>

- **Message Code:** 22062

  Severity: INFO

  Message Text: The 'Drop' advanced option is configured in case of a failed authentication request

  Message Description: In case of a failed authentication request, the Drop advanced option is configured.

  Local Target Message Format: <timestamp> <seq_num> 22062 INFO Workflow: The 'Drop' advanced option is configured in case of a failed authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22062 INFO Workflow: The 'Drop' advanced option is configured in case of a failed authentication request, <log details>

- **Message Code:** 22063

  Severity: INFO

  Message Text: Wrong password

  Message Description: Wrong password

  Local Target Message Format: <timestamp> <seq_num> 22063 INFO Authentication: Wrong password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22063 INFO Authentication: Wrong password, <log details>

- **Message Code:** 22064

  Severity: DEBUG

  Message Text: Authentication method is not supported by any applicable identity store(s)

  Message Description: Authentication method is not supported by any applicable identity store(s)

  Local Target Message Format: <timestamp> <seq_num> 22064 DEBUG Workflow: Authentication method is not supported by any applicable identity store(s), <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22064 DEBUG Workflow: Authentication method is not supported by any applicable identity store(s), <log details>

- **Message Code:** 22065

  Severity: WARN

  Message Text: Guest session limit could not be enforced as MnT node not reachable

  Message Description: Guest session limit could not be enforced as MnT node not reachable

  Local Target Message Format: <timestamp> <seq_num> 22065 WARN Authentication: Guest session limit could not be enforced as MnT node not reachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22065 WARN Authentication: Guest session limit could not be enforced as MnT node not reachable, <log details>

- **Message Code:** 22066

  Severity: INFO

  Message Text: Guest session limit is active; removing older guest sessions

  Message Description: Guest session limit is active; removing older guest sessions

  Local Target Message Format: <timestamp> <seq_num> 22066 INFO Authentication: Guest session limit is active; removing older guest sessions, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22066 INFO Authentication: Guest session limit is active; removing older guest sessions, <log details>

- **Message Code:** 22067

  Severity: WARN

  Message Text: Guest session limit response is missing relevant information in order to remove old guest sessions

  Message Description: Guest session limit response is missing relevant information in order to remove old guest sessions

  Local Target Message Format: <timestamp> <seq_num> 22067 WARN Authentication: Guest session limit response is missing relevant information in order to remove old guest sessions, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22067 WARN Authentication: Guest session limit response is missing relevant information in order to remove old guest sessions, <log details>

- **Message Code:** 22068

  Severity: DEBUG

  Message Text: Binary comparison of certificates skipped on EAP session resume.

  Message Description: Binary comparison of certificates skipped on EAP session resume.

Local Target Message Format: <timestamp> <seq_num> 22068 DEBUG Authentication: Binary comparison of certificates skipped on EAP session resume., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22068 DEBUG Authentication: Binary comparison of certificates skipped on EAP session resume., <log details>

- **Message Code:** 22069

  Severity: DEBUG

  Message Text: AD account search attribute is missing in client certificate

  Message Description: Attribute selected in Certificate Authentication Profile for AD account search is missing in client certificate

  Local Target Message Format: <timestamp> <seq_num> 22069 DEBUG Authentication: AD account search attribute is missing in client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22069 DEBUG Authentication: AD account search attribute is missing in client certificate, <log details>

- **Message Code:** 22070

  Severity: DEBUG

  Message Text: Identity name is taken from certificate attribute

  Message Description: Identity name is taken from certificate attribute according to Certificate Authentication Profile settings

  Local Target Message Format: <timestamp> <seq_num> 22070 DEBUG Authentication: Identity name is taken from certificate attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22070 DEBUG Authentication: Identity name is taken from certificate attribute, <log details>

- **Message Code:** 22071

  Severity: DEBUG

  Message Text: Identity name is taken from AD account Implicit UPN

  Message Description: Identity name is taken from AD account Implicit UPN according to Certificate Authentication Profile settings

  Local Target Message Format: <timestamp> <seq_num> 22071 DEBUG Authentication: Identity name is taken from AD account Implicit UPN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22071 DEBUG Authentication: Identity name is taken from AD account Implicit UPN, <log details>

- **Message Code:** 22072

  Severity: INFO

  Message Text: Selected identity source sequence

Message Description: Selected identity source sequence

Local Target Message Format: <timestamp> <seq_num> 22072 INFO Authentication: Selected identity source sequence, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22072 INFO Authentication: Selected identity source sequence, <log details>

- **Message Code:** 22073

  Severity: INFO

  Message Text: Guest session limit is active; removing newest guest session

  Message Description: Guest session limit is active; removing newest guest session

  Local Target Message Format: <timestamp> <seq_num> 22073 INFO Authentication: Guest session limit is active; removing newest guest session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22073 INFO Authentication: Guest session limit is active; removing newest guest session, <log details>

- **Message Code:** 22074

  Severity: ERROR

  Message Text: This Protocol is disabled in FIPS mode.

  Message Description: Protocol is disabled in FIPS mode.

  Local Target Message Format: <timestamp> <seq_num> 22074 ERROR Authentication: This Protocol is disabled in FIPS mode., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22074 ERROR Authentication: This Protocol is disabled in FIPS mode., <log details>

- **Message Code:** 22075

  Severity: ERROR

  Message Text: Multi-factor Authentication Successful

  Message Description: Multi-factor Authentication Successful

  Local Target Message Format: <timestamp> <seq_num>Authentication Multi-factor Authentication Successful ERROR Multi-factor Authentication Successful, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Authentication Multi-factor Authentication Successful ERROR Multi-factor Authentication Successful, <log details>

- **Message Code:** 22076

  Severity: DEBUG

  Message Text: Multi-factor Authentication Failed

  Message Description: Multi-factor Authentication Failed

Local Target Message Format: <timestamp> <seq_num>Authentication Multi-factor Authentication Failed DEBUG Multi-factor Authentication Failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Authentication Multi-factor Authentication Failed DEBUG Multi-factor Authentication Failed, <log details>

- **Message Code:** 22077

  Severity: WARN

  Message Text: User password is corrupted

  Message Description: Failed to decipher password. User password is corrupted

  Local Target Message Format: <timestamp> <seq_num>Authentication User password is corrupted WARN Failed to decipher password. User password is corrupted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Authentication User password is corrupted WARN Failed to decipher password. User password is corrupted, <log details>

- **Message Code:** 22078

  Severity: WARN

  Message Text: In FIPS mode PAP is allowed only over DTLS

  Message Description: In FIPS mode PAP is allowed only over DTLS

  Local Target Message Format: <timestamp> <seq_num>22078 WARN Authentication In FIPS mode PAP is allowed only over DTLS, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>22078 WARN Authentication In FIPS mode PAP is allowed only over DTLS, <log details>

- **Message Code:** 22080

  Severity: INFO

  Message Text: New accounting session created in Session cache

  Message Description: New accounting session created in Session cache.

  Local Target Message Format: <timestamp> <seq_num> 22080 INFO Authentication: New accounting session created in Session cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22080 INFO Authentication: New accounting session created in Session cache, <log details>

- **Message Code:** 22081

  Severity: INFO

  Message Text: Max sessions policy passed

  Message Description: Max sessions policy passed.

Local Target Message Format: <timestamp> <seq_num> 22081 INFO Authentication: Max sessions policy passed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22081 INFO Authentication: Max sessions policy passed, <log details>

- **Message Code:** 22082

  Severity: INFO

  Message Text: Max sessions policy disabled

  Message Description: Max sessions policy disabled.

  Local Target Message Format: <timestamp> <seq_num> 22082 INFO Authentication: Max sessions policy disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22082 INFO Authentication: Max sessions policy disabled, <log details>

- **Message Code:** 22083

  Severity: INFO

  Message Text: User/group session counters incremented on accounting start

  Message Description: User/group session counters incremented on accounting start

  Local Target Message Format: <timestamp> <seq_num> 22083 INFO Authentication: User/group session counters incremented on accounting start, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22083 INFO Authentication: User/group session counters incremented on accounting start, <log details>

- **Message Code:** 22084

  Severity: INFO

  Message Text: User/group session counters decremented on accounting stop

  Message Description: User/group session counters decremented on accounting stop. The session was removed.

  Local Target Message Format: <timestamp> <seq_num> 22084 INFO Authentication: User/group session counters decremented on accounting stop, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22084 INFO Authentication: User/group session counters decremented on accounting stop, <log details>

- **Message Code:** 22085

  Severity: INFO

  Message Text: The accounting session was updated in Session cache

  Message Description: The accounting session was updated in Session cache

Local Target Message Format: <timestamp> <seq_num> 22085 INFO Authentication: The accounting session was updated in Session cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22085 INFO Authentication: The accounting session was updated in Session cache, <log details>

- **Message Code:** 22086

  Severity: INFO

  Message Text: The active sessions were purged for device

  Message Description: The active sessions were purged for device

  Local Target Message Format: <timestamp> <seq_num> 22086 INFO Authentication: The active sessions were purged for device, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22086 INFO Authentication: The active sessions were purged for device, <log details>

- **Message Code:** 22087

  Severity: INFO

  Message Text: The accounting session was timed out

  Message Description: The accounting session was timed out

  Local Target Message Format: <timestamp> <seq_num> 22087 INFO Authentication: The accounting session was timed out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22087 INFO Authentication: The accounting session was timed out, <log details>

- **Message Code:** 22088

  Severity: INFO

  Message Text: The accounting session was purged

  Message Description: The accounting session was purged

  Local Target Message Format: <timestamp> <seq_num> 22088 INFO Authentication: The accounting session was purged, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22088 INFO Authentication: The accounting session was purged, <log details>

- **Message Code:** 22089

  Severity: INFO

  Message Text: New user session not permitted. Max sessions user limit has been reached

  Message Description: New user session not permitted. Max sessions user limit exceeded.

Local Target Message Format: <timestamp> <seq_num> 22089 INFO Authentication: New user session not permitted. Max sessions user limit has been reached, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22089 INFO Authentication: New user session not permitted. Max sessions user limit has been reached, <log details>

- **Message Code:** 22090

  Severity: WARN

  Message Text: One or more attributes are missing for the accounting Session Key

  Message Description: One or more attributes are missing for the accounting Session Key. Please ACS and network device configuration.

  Local Target Message Format: <timestamp> <seq_num> 22090 WARN Authentication: One or more attributes are missing for the accounting Session Key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22090 WARN Authentication: One or more attributes are missing for the accounting Session Key, <log details>

- **Message Code:** 22091

  Severity: INFO

  Message Text: Authentication failed. User account is disabled due to excessive failed authentication attempts at global level

  Message Description: Authentication failed. User account is disabled due to excessive failed authentication attempts at global level.

  Local Target Message Format: <timestamp> <seq_num> 22091 INFO Authentication: Authentication failed. User account is disabled due to excessive failed authentication attempts at global level, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22091 INFO Authentication: Authentication failed. User account is disabled due to excessive failed authentication attempts at global level, <log details>

- **Message Code:** 22092

  Severity: INFO

  Message Text: No accounting start was received for the session

  Message Description: No accounting start was received for the session. The request will be ignored.

  Local Target Message Format: <timestamp> <seq_num> 22092 INFO Authentication: No accounting start was received for the session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22092 INFO Authentication: No accounting start was received for the session, <log details>

- **Message Code:** 22093

  Severity: INFO

Message Text: Duplicate session was found with a different user name

Message Description: Duplicate session was found with a different user name. The request will be ignored. Check the session key configuration.

Local Target Message Format: <timestamp> <seq_num> 22093 INFO Authentication: Duplicate session was found with a different user name, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22093 INFO Authentication: Duplicate session was found with a different user name, <log details>

- **Message Code:** 22094

  Severity: INFO

  Message Text: Audit session was not found

  Message Description: Audit session was not found. The session is expired or purged.

  Local Target Message Format: <timestamp> <seq_num> 22094 INFO Authentication: Audit session was not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22094 INFO Authentication: Audit session was not found, <log details>

- **Message Code:** 22095

  Severity: INFO

  Message Text: Accounting start was received for non-existing session

  Message Description: Accounting start was received for the session that was not found in the cache. Either the session was not created or it was purged.

  Local Target Message Format: <timestamp> <seq_num> 22095 INFO Authentication: Accounting start was received for non-existing session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22095 INFO Authentication: Accounting start was received for non-existing session, <log details>

- **Message Code:** 22096

  Severity: INFO

  Message Text: Max session policy is not available for Proxy

  Message Description: Max session policy is not available for Proxy.

  Local Target Message Format: <timestamp> <seq_num> 22096 INFO Authentication: Max session policy is not available for Proxy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22096 INFO Authentication: Max session policy is not available for Proxy, <log details>

- **Message Code:** 22097

  Severity: INFO

Message Text: New user session not permitted. Max sessions group limit has been reached

Message Description: New user session not permitted. Max sessions group limit has been reached.

Local Target Message Format: <timestamp> <seq_num> 22097 INFO Authentication: New user session not permitted. Max sessions group limit has been reached, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22097 INFO Authentication: New user session not permitted. Max sessions group limit has been reached, <log details>

- **Message Code:** 22098

  Severity: INFO

  Message Text: New user session not permitted. Max sessions user in group limit has been reached

  Message Description: New user session not permitted. Max sessions user in group limit has been reached.

  Local Target Message Format: <timestamp> <seq_num> 22098 INFO Authentication: New user session not permitted. Max sessions user in group limit has been reached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 22098 INFO Authentication: New user session not permitted. Max sessions user in group limit has been reached, <log details>

Distributed Management

- **Message Code:** 41000

  Severity: WARN

  Message Text: Memory statistics not found

  Message Description: The system call made to generate the local system's memory usage failed.

  Local Target Message Format: <timestamp> <seq_num> 41000 WARN Distributed-Management: Memory statistics not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41000 WARN Distributed-Management: Memory statistics not found, <log details>

- **Message Code:** 41001

  Severity: WARN

  Message Text: Total memory not found

  Message Description: The system call made to generate the total system memory failed.

  Local Target Message Format: <timestamp> <seq_num> 41001 WARN Distributed-Management: Total memory not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41001 WARN Distributed-Management: Total memory not found, <log details>

- **Message Code:** 41002

  Severity: WARN

  Message Text: Total swap not found

  Message Description: The system call made to generate the Total Swap size failed.

  Local Target Message Format: <timestamp> <seq_num> 41002 WARN Distributed-Management: Total swap not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41002 WARN Distributed-Management: Total swap not found, <log details>

- **Message Code:** 41003

  Severity: WARN

  Message Text: Disk size not found

  Message Description: The system call made to generate the Disk Size failed.

  Local Target Message Format: <timestamp> <seq_num> 41003 WARN Distributed-Management: Disk size not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41003 WARN Distributed-Management: Disk size not found, <log details>

- **Message Code:** 41004

  Severity: WARN

  Message Text: Disk device not found

  Message Description: The system call made to generate the list of Disk Devices failed.

  Local Target Message Format: <timestamp> <seq_num> 41004 WARN Distributed-Management: Disk device not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41004 WARN Distributed-Management: Disk device not found, <log details>

- **Message Code:** 41005

  Severity: WARN

  Message Text: ISE version not found

  Message Description: The system call made to obtain the ISE Software version failed.

  Local Target Message Format: <timestamp> <seq_num> 41005 WARN Distributed-Management: ISE version not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41005 WARN Distributed-Management: ISE version not found, <log details>

- **Message Code:** 41007

Severity: INFO

Message Text: ISE Node record found

Message Description: The underlying ISE Node record could not be found in the database.

Local Target Message Format: <timestamp> <seq_num> 41007 INFO Distributed-Management: ISE Node record found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41007 INFO Distributed-Management: ISE Node record found, <log details>

- **Message Code:** 41008

  Severity: INFO

  Message Text: Primary ISE Node record found taking over primary role

  Message Description: Since the appropriate ISE Node record for the local device could not be found, the Primary ISE Node record was found. Therefore, the local node is taking over the Primary role.

  Local Target Message Format: <timestamp> <seq_num> 41008 INFO Distributed-Management: Primary ISE Node record found taking over primary role, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41008 INFO Distributed-Management: Primary ISE Node record found taking over primary role, <log details>

- **Message Code:** 41009

  Severity: INFO

  Message Text: Default ISE Deployment created

  Message Description: During system initialization the default ISE Deployment record was created in the database. This is the normal behavior for the system.

  Local Target Message Format: <timestamp> <seq_num> 41009 INFO Distributed-Management: Default ISE Deployment created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41009 INFO Distributed-Management: Default ISE Deployment created, <log details>

- **Message Code:** 41010

  Severity: INFO

  Message Text: Default ISE Node created

  Message Description: During system initialization the Default ISE Node record was created in the database. This is the normal behavior for the system.

  Local Target Message Format: <timestamp> <seq_num> 41010 INFO Distributed-Management: Default ISE Node created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41010 INFO Distributed-Management: Default ISE Node created, <log details>

- **Message Code:** 41011

  Severity: INFO

  Message Text: Node Status initialized

  Message Description: During system initialization Node Status initialized.

  Local Target Message Format: <timestamp> <seq_num> 41011 INFO Distributed-Management: Node Status initialized, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41011 INFO Distributed-Management: Node Status initialized, <log details>

- **Message Code:** 41012

  Severity: INFO

  Message Text: Secondary registered

  Message Description: A new ISE instance has joined the deployment.

  Local Target Message Format: <timestamp> <seq_num> 41012 INFO Distributed-Management: Secondary registered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41012 INFO Distributed-Management: Secondary registered, <log details>

- **Message Code:** 41013

  Severity: INFO

  Message Text: ISE Node has been deregistered and is now running as a Primary node

  Message Description: The ISE Node has been deregistered and is now running as a Primary node

  Local Target Message Format: <timestamp> <seq_num> 41013 INFO Distributed-Management: ISE Node has been deregistered and is now running as a Primary node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41013 INFO Distributed-Management: ISE Node has been deregistered and is now running as a Primary node, <log details>

- **Message Code:** 41014

  Severity: ERROR

  Message Text: Software version not found

  Message Description: The system call that obtains the ISE Software version failed.

  Local Target Message Format: <timestamp> <seq_num> 41014 ERROR Distributed-Management: Software version not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41014 ERROR Distributed-Management: Software version not found, <log details>

- **Message Code:** 41015

  Severity: ERROR

  Message Text: Could not run

  Message Description: The system call that was activated, did not run correctly.

  Local Target Message Format: <timestamp> <seq_num> 41015 ERROR Distributed-Management: Could not run, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41015 ERROR Distributed-Management: Could not run, <log details>

- **Message Code:** 41016

  Severity: ERROR

  Message Text: could not read stdout

  Message Description: While running a system call, the stdout of the system call could not be read.

  Local Target Message Format: <timestamp> <seq_num> 41016 ERROR Distributed-Management: could not read stdout, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41016 ERROR Distributed-Management: could not read stdout, <log details>

- **Message Code:** 41017

  Severity: WARN

  Message Text: Hostname not found

  Message Description: The system call that obtains the local system's hostname failed.

  Local Target Message Format: <timestamp> <seq_num> 41017 WARN Distributed-Management: Hostname not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41017 WARN Distributed-Management: Hostname not found, <log details>

- **Message Code:** 41018

  Severity: ERROR

  Message Text: Service Selection Policy update failed

  Message Description: During system initialization the Default Service Selection Policy update failed.

  Local Target Message Format: <timestamp> <seq_num> 41018 ERROR Distributed-Management: Service Selection Policy update failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41018 ERROR Distributed-Management: Service Selection Policy update failed, <log details>

- **Message Code:** 41019

Severity: ERROR

Message Text: Could not add relation to Service Selection Policy

Message Description: During system initialization the Default Service Selection Policy update failed.

Local Target Message Format: <timestamp> <seq_num> 41019 ERROR Distributed-Management: Could not add relation to Service Selection Policy, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41019 ERROR Distributed-Management: Could not add relation to Service Selection Policy, <log details>

- **Message Code:** 41020

  Severity: ERROR

  Message Text: Could not initialize Service Selection Policy

  Message Description: During system initialization the Default Service Selection Policy update failed.

  Local Target Message Format: <timestamp> <seq_num> 41020 ERROR Distributed-Management: Could not initialize Service Selection Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41020 ERROR Distributed-Management: Could not initialize Service Selection Policy, <log details>

- **Message Code:** 41021

  Severity: ERROR

  Message Text: Could not update ISE Node Object

  Message Description: Failed to update ISE Node with the local node information when the system started.

  Local Target Message Format: <timestamp> <seq_num> 41021 ERROR Distributed-Management: Could not update ISE Node Object, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41021 ERROR Distributed-Management: Could not update ISE Node Object, <log details>

- **Message Code:** 41022

  Severity: ERROR

  Message Text: An error occurred while collecting NodeInfo

  Message Description: Collection of the local node information failed.

  Local Target Message Format: <timestamp> <seq_num> 41022 ERROR Distributed-Management: An error occurred while collecting NodeInfo, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41022 ERROR Distributed-Management: An error occurred while collecting NodeInfo, <log details>

- **Message Code:** 41023

Severity: ERROR

Message Text: An error occurred while collecting replication status

Message Description: Collection of the replication status failed.

Local Target Message Format: <timestamp> <seq_num> 41023 ERROR Distributed-Management: An error occurred while collecting replication status, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41023 ERROR Distributed-Management: An error occurred while collecting replication status, <log details>

- **Message Code:** 41024

  Severity: ERROR

  Message Text: Error loading NodeInfo

  Message Description: The NodeInfo file did not load correctly.

  Local Target Message Format: <timestamp> <seq_num> 41024 ERROR Distributed-Management: Error loading NodeInfo, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41024 ERROR Distributed-Management: Error loading NodeInfo, <log details>

- **Message Code:** 41025

  Severity: ERROR

  Message Text: NodeInfo file contains incomplete information

  Message Description: NodeInfo file contains incomplete information and has loaded incorrectly.

  Local Target Message Format: <timestamp> <seq_num> 41025 ERROR Distributed-Management: NodeInfo file contains incomplete information, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41025 ERROR Distributed-Management: NodeInfo file contains incomplete information, <log details>

- **Message Code:** 41026

  Severity: ERROR

  Message Text: Management config directory could not be created

  Message Description: The Management config directory could not be created.

  Local Target Message Format: <timestamp> <seq_num> 41026 ERROR Distributed-Management: Management config directory could not be created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41026 ERROR Distributed-Management: Management config directory could not be created, <log details>

- **Message Code:** 41027

  Severity: ERROR

Message Text: NodeInfo file could not be created

Message Description: NodeInfo file could not be created in the config directory.

Local Target Message Format: <timestamp> <seq_num> 41027 ERROR Distributed-Management: NodeInfo file could not be created, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41027 ERROR Distributed-Management: NodeInfo file could not be created, <log details>

- **Message Code:** 41028

  Severity: ERROR

  Message Text: MAC Address not found during initialization

  Message Description: Machine Network Address could not be found in the system network interface output during initialization.

  Local Target Message Format: <timestamp> <seq_num> 41028 ERROR Distributed-Management: MAC Address not found during initialization, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41028 ERROR Distributed-Management: MAC Address not found during initialization, <log details>

- **Message Code:** 41029

  Severity: ERROR

  Message Text: ISE Node record not found in existing nodes. ISE cannot start

  Message Description: During system initialization the ISE Node record representing the local instance was not found in the existing nodes. ISE Management could not to start.

  Local Target Message Format: <timestamp> <seq_num> 41029 ERROR Distributed-Management: ISE Node record not found in existing nodes. ISE cannot start, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41029 ERROR Distributed-Management: ISE Node record not found in existing nodes. ISE cannot start, <log details>

- **Message Code:** 41030

  Severity: ERROR

  Message Text: MAC Id not found in ACSNodeInfo

  Message Description: The Machine address field was not found in the ACSNodeInfo record in the database.

  Local Target Message Format: <timestamp> <seq_num> 41030 ERROR Distributed-Management: MAC Id not found in ACSNodeInfo, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41030 ERROR Distributed-Management: MAC Id not found in ACSNodeInfo, <log details>

- **Message Code:** 41031

Severity: ERROR

Message Text: Registering Secondary Hostname already exists in Primary database

Message Description: An attempt is being made to register the Secondary hostname. However, it already exists in the Primary database.

Local Target Message Format: <timestamp> <seq_num> 41031 ERROR Distributed-Management: Registering Secondary Hostname already exists in Primary database, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41031 ERROR Distributed-Management: Registering Secondary Hostname already exists in Primary database, <log details>

- **Message Code:** 41032

  Severity: ERROR

  Message Text: Register failed since Secondary MAC address already exists in the Primary database

  Message Description: An attempt is being made to register the machine address of the Secondary hostname. However, it already exists in the Primary database.

  Local Target Message Format: <timestamp> <seq_num> 41032 ERROR Distributed-Management: Register failed since Secondary MAC address already exists in the Primary database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41032 ERROR Distributed-Management: Register failed since Secondary MAC address already exists in the Primary database, <log details>

- **Message Code:** 41033

  Severity: ERROR

  Message Text: Deregistration failed since Secondary ISE Node not found in the Primary database

  Message Description: ISE instance de-registration failed since the Secondary's ISE Node record was not found in Primary database.

  Local Target Message Format: <timestamp> <seq_num> 41033 ERROR Distributed-Management: Deregistration failed since Secondary ISE Node not found in the Primary database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41033 ERROR Distributed-Management: Deregistration failed since Secondary ISE Node not found in the Primary database, <log details>

- **Message Code:** 41034

  Severity: ERROR

  Message Text: Activation failed since Secondary ISE Node is not found

  Message Description: Activation of the Secondary node from the Primary database failed because the Secondary ACSNode record was not found in the database.

  Local Target Message Format: <timestamp> <seq_num> 41034 ERROR Distributed-Management: Activation failed since Secondary ISE Node is not found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41034 ERROR Distributed-Management: Activation failed since Secondary ISE Node is not found, <log details>

- **Message Code:** 41035

  Severity: ERROR

  Message Text: Remote host is not a Primary AcsNode

  Message Description: During a Distributed Management Remote operation connection to the Primary was not possible because the host is not a Primary instance.

  Local Target Message Format: <timestamp> <seq_num> 41035 ERROR Distributed-Management: Remote host is not a Primary AcsNode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41035 ERROR Distributed-Management: Remote host is not a Primary AcsNode, <log details>

- **Message Code:** 41036

  Severity: ERROR

  Message Text: Cannot deregister a Primary ISE Node

  Message Description: The Primary instance of a deployment cannot be de-registered.

  Local Target Message Format: <timestamp> <seq_num> 41036 ERROR Distributed-Management: Cannot deregister a Primary ISE Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41036 ERROR Distributed-Management: Cannot deregister a Primary ISE Node, <log details>

- **Message Code:** 41037

  Severity: ERROR

  Message Text: ISE Deployment record cannot be found, therefore Primary initialization is incorrect

  Message Description: During system initialization the ISE Deployment record could not be found and the system could not start correctly.

  Local Target Message Format: <timestamp> <seq_num> 41037 ERROR Distributed-Management: ISE Deployment record cannot be found, therefore Primary initialization is incorrect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41037 ERROR Distributed-Management: ISE Deployment record cannot be found, therefore Primary initialization is incorrect, <log details>

- **Message Code:** 41038

  Severity: ERROR

  Message Text: Interface configuration cannot be found

  Message Description: During the System call to obtain the Network Interface configuration, a failure occurred.

Local Target Message Format: <timestamp> <seq_num> 41038 ERROR Distributed-Management: Interface configuration cannot be found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41038 ERROR Distributed-Management: Interface configuration cannot be found, <log details>

- **Message Code:** 41039

  Severity: ERROR

  Message Text: Network interface eth0 cannot be found

  Message Description: During the system call to obtain the Network Interface eth0 configuration, a failure occurred and the interface was not found.

  Local Target Message Format: <timestamp> <seq_num> 41039 ERROR Distributed-Management: Network interface eth0 cannot be found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41039 ERROR Distributed-Management: Network interface eth0 cannot be found, <log details>

- **Message Code:** 41040

  Severity: ERROR

  Message Text: Network interface eth0 hardware address cannot be found

  Message Description: During the system call to obtain the Network Interface eth0 configuration hardware address, a failure occurred and the hardware address was not found.

  Local Target Message Format: <timestamp> <seq_num> 41040 ERROR Distributed-Management: Network interface eth0 hardware address cannot be found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41040 ERROR Distributed-Management: Network interface eth0 hardware address cannot be found, <log details>

- **Message Code:** 41041

  Severity: ERROR

  Message Text: Network interface eth0 inet address cannot be found

  Message Description: During the System call to obtain the Network Interface eth0 configuration IP address, a failure occurred and the IP address was not found.

  Local Target Message Format: <timestamp> <seq_num> 41041 ERROR Distributed-Management: Network interface eth0 inet address cannot be found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41041 ERROR Distributed-Management: Network interface eth0 inet address cannot be found, <log details>

- **Message Code:** 41042

  Severity: ERROR

  Message Text: Network interface eth0 mask cannot be found

Message Description: During the system call to obtain the Network Interface eth0 configuration subnet mask a failure occurred and the subnet mask was not found.

Local Target Message Format: <timestamp> <seq_num> 41042 ERROR Distributed-Management: Network interface eth0 mask cannot be found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41042 ERROR Distributed-Management: Network interface eth0 mask cannot be found, <log details>

- **Message Code:** 41043

  Severity: ERROR

  Message Text: Could not create ACSNodeInfo

  Message Description: The system failed to create AcsNodeInfo record and attach it to the AcsNode record for the instance.

  Local Target Message Format: <timestamp> <seq_num> 41043 ERROR Distributed-Management: Could not create ACSNodeInfo, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41043 ERROR Distributed-Management: Could not create ACSNodeInfo, <log details>

- **Message Code:** 41044

  Severity: ERROR

  Message Text: Failure to find the reconnection Acs Instance in the primary, please check that the Acs Instance exists in the Primary Acs Instance Listing page

  Message Description: During a Hardware Replacement or LocalMode reconnection the AcsNode record with the specified Replacement Keyword could not be found. This keyword is the hostname of the system by default.

  Local Target Message Format: <timestamp> <seq_num> 41044 ERROR Distributed-Management: Failure to find the reconnection Acs Instance in the primary, please check that the Acs Instance exists in the Primary Acs Instance Listing page, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41044 ERROR Distributed-Management: Failure to find the reconnection Acs Instance in the primary, please check that the Acs Instance exists in the Primary Acs Instance Listing page, <log details>

- **Message Code:** 41045

  Severity: ERROR

  Message Text: Failure. Specified replacement keyword is associated with a registered instance

  Message Description: During hardware replacement the specified replacement keyword is associated with an ISE instance that has already been registered.

  Local Target Message Format: <timestamp> <seq_num> 41045 ERROR Distributed-Management: Failure. Specified replacement keyword is associated with a registered instance, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41045 ERROR

Distributed-Management: Failure. Specified replacement keyword is associated with a registered instance, <log details>

- **Message Code:** 41046

  Severity: INFO

  Message Text: Registering to Primary

  Message Description: An ISE instance is in the process of registering to the Primary node.

  Local Target Message Format: <timestamp> <seq_num> 41046 INFO Distributed-Management: Registering to Primary, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41046 INFO Distributed-Management: Registering to Primary, <log details>

- **Message Code:** 41047

  Severity: INFO

  Message Text: Initiate Full Sync of Data from Primary

  Message Description: A full synchronization of data from the Primary node has been initiated for the specified ISE instance.

  Local Target Message Format: <timestamp> <seq_num> 41047 INFO Distributed-Management: Initiate Full Sync of Data from Primary, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41047 INFO Distributed-Management: Initiate Full Sync of Data from Primary, <log details>

- **Message Code:** 41048

  Severity: INFO

  Message Text: ACSNode has been replaced

  Message Description: The specified ISE instance has been hardware-replaced correctly.

  Local Target Message Format: <timestamp> <seq_num> 41048 INFO Distributed-Management: ACSNode has been replaced, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41048 INFO Distributed-Management: ACSNode has been replaced, <log details>

- **Message Code:** 41049

  Severity: INFO

  Message Text: New ACSNode Registering to Primary

  Message Description: A new ISE instance has been registered to the Primary node.

  Local Target Message Format: <timestamp> <seq_num> 41049 INFO Distributed-Management: New ACSNode Registering to Primary, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41049 INFO Distributed-Management: New ACSNode Registering to Primary, <log details>

- **Message Code:** 41050

  Severity: INFO

  Message Text: Activating ACSNode

  Message Description: The specified ISE instance is being activated on the Primary.

  Local Target Message Format: <timestamp> <seq_num> 41050 INFO Distributed-Management: Activating ACSNode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41050 INFO Distributed-Management: Activating ACSNode, <log details>

- **Message Code:** 41051

  Severity: INFO

  Message Text: Deactivating ACSNode

  Message Description: The specified ISE instance is being deactivated on the Primary.

  Local Target Message Format: <timestamp> <seq_num> 41051 INFO Distributed-Management: Deactivating ACSNode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41051 INFO Distributed-Management: Deactivating ACSNode, <log details>

- **Message Code:** 41053

  Severity: INFO

  Message Text: Promote node to Primary

  Message Description: The specified ISE instance is being promoted to the Primary node of the deployment.

  Local Target Message Format: <timestamp> <seq_num> 41053 INFO Distributed-Management: Promote node to Primary, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41053 INFO Distributed-Management: Promote node to Primary, <log details>

- **Message Code:** 41054

  Severity: INFO

  Message Text: Switching Secondary to Local Mode Operation

  Message Description: The specified ISE instance is switching to Local Mode Operation.

  Local Target Message Format: <timestamp> <seq_num> 41054 INFO Distributed-Management: Switching Secondary to Local Mode Operation, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41054 INFO Distributed-Management: Switching Secondary to Local Mode Operation, <log details>

- **Message Code:** 41055

  Severity: INFO

  Message Text: Upgrading node to new software version

  Message Description: The specified ISE instance is being upgraded/patched to a new software version.

  Local Target Message Format: <timestamp> <seq_num> 41055 INFO Distributed-Management: Upgrading node to new software version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41055 INFO Distributed-Management: Upgrading node to new software version, <log details>

- **Message Code:** 41056

  Severity: INFO

  Message Text: Apply upgrade

  Message Description: A software upgrade is being applied to the local ISE instance.

  Local Target Message Format: <timestamp> <seq_num> 41056 INFO Distributed-Management: Apply upgrade, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41056 INFO Distributed-Management: Apply upgrade, <log details>

- **Message Code:** 41057

  Severity: INFO

  Message Text: Automatic backup being created

  Message Description: The system is being backed up as part of applying an upgrade or patch.

  Local Target Message Format: <timestamp> <seq_num> 41057 INFO Distributed-Management: Automatic backup being created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41057 INFO Distributed-Management: Automatic backup being created, <log details>

- **Message Code:** 41058

  Severity: INFO

  Message Text: Downloading bundle for Primary hosting

  Message Description: The Primary node is downloading the software upgrade/patch bundle from the remote host so it can be hosted on the primary node.

  Local Target Message Format: <timestamp> <seq_num> 41058 INFO Distributed-Management: Downloading bundle for Primary hosting, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41058 INFO Distributed-Management: Downloading bundle for Primary hosting, <log details>

- **Message Code:** 41059

  Severity: INFO

  Message Text: Node upgrade completed

  Message Description: The upgrade or patch process has completed on the local node.

  Local Target Message Format: <timestamp> <seq_num> 41059 INFO Distributed-Management: Node upgrade completed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41059 INFO Distributed-Management: Node upgrade completed, <log details>

- **Message Code:** 41060

  Severity: INFO

  Message Text: Enabling Log Collector Target

  Message Description: Enabling Log Collector Target for the ISE deployment. After it is enabled, remote logging from each instance in the deployment will be sent to the collector.

  Local Target Message Format: <timestamp> <seq_num> 41060 INFO Distributed-Management: Enabling Log Collector Target, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41060 INFO Distributed-Management: Enabling Log Collector Target, <log details>

- **Message Code:** 41061

  Severity: INFO

  Message Text: Disabling Log Collector Target

  Message Description: Disabling Log Collector Target for the ISE Deployment. Remote logging to the Log collector will cease until re-enabled.

  Local Target Message Format: <timestamp> <seq_num> 41061 INFO Distributed-Management: Disabling Log Collector Target, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41061 INFO Distributed-Management: Disabling Log Collector Target, <log details>

- **Message Code:** 41062

  Severity: INFO

  Message Text: Select the Log Collector Node

  Message Description: The Log Collector ISE instance has been selected for the deployment. After Log Collector is enabled, remote logging will appear on the collector.

Local Target Message Format: <timestamp> <seq_num> 41062 INFO Distributed-Management: Select the Log Collector Node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41062 INFO Distributed-Management: Select the Log Collector Node, <log details>

- **Message Code:** 41063

  Severity: INFO

  Message Text: Remote Syslog Target for Log Collector has been created

  Message Description: Remote Syslog Target for the Log Collector has been created and remote logging to the Log Collector will begin.

  Local Target Message Format: <timestamp> <seq_num> 41063 INFO Distributed-Management: Remote Syslog Target for Log Collector has been created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41063 INFO Distributed-Management: Remote Syslog Target for Log Collector has been created, <log details>

- **Message Code:** 41064

  Severity: ERROR

  Message Text: The deployment Log Collector cannot be deregistered

  Message Description: The deployment cannot be left without a Log Collector configured. De-registering this node will remove the selected Log Collector.

  Local Target Message Format: <timestamp> <seq_num> 41064 ERROR Distributed-Management: The deployment Log Collector cannot be deregistered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41064 ERROR Distributed-Management: The deployment Log Collector cannot be deregistered, <log details>

- **Message Code:** 41065

  Severity: INFO

  Message Text: Apply upgrade diagnostic messages

  Message Description: Apply upgrade diagnostic messages

  Local Target Message Format: <timestamp> <seq_num> 41065 INFO Distributed-Management: Apply upgrade diagnostic messages, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 41065 INFO Distributed-Management: Apply upgrade diagnostic messages, <log details>

External MDM

- **Message Code:** 89000

Severity: INFO

Message Text: Mabile device manager unregistered

Message Description: Device is not registered with Mobile device manager

Local Target Message Format: <timestamp> <seq_num> 89000 INFO MDM: Mabile device manager unregistered, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89000 INFO MDM: Mabile device manager unregistered, <log details>

- **Message Code:** 89001

  Severity: INFO

  Message Text: Mobile device management compliant

  Message Description: Device is compliant with Mobile device management

  Local Target Message Format: <timestamp> <seq_num> 89001 INFO MDM: Mobile device management compliant, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89001 INFO MDM: Mobile device management compliant, <log details>

- **Message Code:** 89002

  Severity: INFO

  Message Text: Mobile device management non-compliant

  Message Description: Device is non-compliant with Mobile device management

  Local Target Message Format: <timestamp> <seq_num> 89002 INFO MDM: Mobile device management non-compliant, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89002 INFO MDM: Mobile device management non-compliant, <log details>

- **Message Code:** 89003

  Severity: WARN

  Message Text: Failed to connect to MDM server

  Message Description: Failed to connect to MDM server

  Local Target Message Format: <timestamp> <seq_num> 89003 WARN MDM: Failed to connect to MDM server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89003 WARN MDM: Failed to connect to MDM server, <log details>

- **Message Code:** 89004

  Severity: ERROR

Message Text: MDM server API version mismatch

Message Description: MDM server API version doesn't match that configured in ISE

Local Target Message Format: <timestamp> <seq_num> 89004 ERROR MDM: MDM server API version mismatch, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89004 ERROR MDM: MDM server API version mismatch, <log details>

- **Message Code:** 89005

  Severity: WARN

  Message Text: MDM server response error

  Message Description: MDM server response error

  Local Target Message Format: <timestamp> <seq_num> 89005 WARN MDM: MDM server response error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89005 WARN MDM: MDM server response error, <log details>

Failed Attempts

- **Message Code:** 5400

  Severity: NOTICE

  Message Text: Authentication failed

  Message Description: User authentication failed. See FailureReason for more information

  Local Target Message Format: <timestamp> <seq_num> 5400 NOTICE Failed-Attempt: Authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5400 NOTICE Failed-Attempt: Authentication failed, <log details>

- **Message Code:** 5401

  Severity: NOTICE

  Message Text: Authentication failed

  Message Description: User authentication failed. See FailureReason for more information

  Local Target Message Format: <timestamp> <seq_num> 5401 NOTICE Failed-Attempt: Authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5401 NOTICE Failed-Attempt: Authentication failed, <log details>

- **Message Code:** 5402

  Severity: NOTICE

  Message Text: Command Authorization failed

  Message Description: Command Authorization failed

  Local Target Message Format: <timestamp> <seq_num> 5402 NOTICE Failed-Attempt: Command Authorization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5402 NOTICE Failed-Attempt: Command Authorization failed, <log details>

- **Message Code:** 5403

  Severity: NOTICE

  Message Text: Session Authorization failed

  Message Description: Session Authorization failed

  Local Target Message Format: <timestamp> <seq_num> 5403 NOTICE Device-Administration: Session Authorization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5403 NOTICE Device-Administration: Session Authorization failed, <log details>

- **Message Code:** 5404

  Severity: NOTICE

  Message Text: Authorization failed

  Message Description: Authorization failed

  Local Target Message Format: <timestamp> <seq_num> 5404 NOTICE Device-Administration: Authorization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5404 NOTICE Device-Administration: Authorization failed, <log details>

- **Message Code:** 5405

  Severity: NOTICE

  Message Text: RADIUS Request dropped

  Message Description: RADIUS request dropped

  Local Target Message Format: <timestamp> <seq_num> 5405 NOTICE Failed-Attempt: RADIUS Request dropped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5405 NOTICE Failed-Attempt: RADIUS Request dropped, <log details>

- **Message Code:** 5406

Severity: NOTICE

Message Text: TACACS+ Request dropped

Message Description: TACACS+ request dropped

Local Target Message Format: <timestamp> <seq_num> 5406 NOTICE Failed-Attempt: TACACS+ Request dropped, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5406 NOTICE Failed-Attempt: TACACS+ Request dropped, <log details>

- **Message Code:** 5407

  Severity: NOTICE

  Message Text: TACACS+ Authorization failed

  Message Description: TACACS+ Authorization failed

  Local Target Message Format: <timestamp> <seq_num> 5407 NOTICE Failed-Attempt: TACACS+ Authorization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5407 NOTICE Failed-Attempt: TACACS+ Authorization failed, <log details>

- **Message Code:** 5408

  Severity: NOTICE

  Message Text: Command Authorization encountered an error

  Message Description: Command Authorization encountered error. See FailureReason for more information

  Local Target Message Format: <timestamp> <seq_num> 5408 NOTICE Failed-Attempt: Command Authorization encountered an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5408 NOTICE Failed-Attempt: Command Authorization encountered an error, <log details>

- **Message Code:** 5409

  Severity: NOTICE

  Message Text: Session Authorization encountered an error

  Message Description: Session Authorization encountered an error. See FailureReason for more information

  Local Target Message Format: <timestamp> <seq_num> 5409 NOTICE Failed-Attempt: Session Authorization encountered an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5409 NOTICE Failed-Attempt: Session Authorization encountered an error, <log details>

- **Message Code:** 5410

Severity: NOTICE

Message Text: TACACS+ Authorization encountered an error

Message Description: TACACS+ Authorization encountered an error

Local Target Message Format: <timestamp> <seq_num> 5410 NOTICE Failed-Attempt: TACACS+ Authorization encountered an error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5410 NOTICE Failed-Attempt: TACACS+ Authorization encountered an error, <log details>

- **Message Code:** 5411

  Severity: NOTICE

  Message Text: Supplicant stopped responding to ISE

  Message Description: Supplicant did not respond to the last message that ISE sent to it

  Local Target Message Format: <timestamp> <seq_num> 5411 NOTICE Failed-Attempt: Supplicant stopped responding to ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5411 NOTICE Failed-Attempt: Supplicant stopped responding to ISE, <log details>

- **Message Code:** 5412

  Severity: NOTICE

  Message Text: TACACS+ authentication request ended with error

  Message Description: TACACS+ authentication request ended with an error

  Local Target Message Format: <timestamp> <seq_num> 5412 NOTICE Failed-Attempt: TACACS+ authentication request ended with error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5412 NOTICE Failed-Attempt: TACACS+ authentication request ended with error, <log details>

- **Message Code:** 5413

  Severity: NOTICE

  Message Text: RADIUS Accounting-Request dropped

  Message Description: The RADIUS Accounting-Request was dropped.

  Local Target Message Format: <timestamp> <seq_num> 5413 NOTICE Failed-Attempt: RADIUS Accounting-Request dropped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5413 NOTICE Failed-Attempt: RADIUS Accounting-Request dropped, <log details>

- **Message Code:** 5414

  Severity: NOTICE

Message Text: TACACS+ accounting has failed

Message Description: TACACS+ accounting has failed. For more information, see the failure reason records.

Local Target Message Format: <timestamp> <seq_num> 5414 NOTICE Failed-Attempt: TACACS+ accounting has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5414 NOTICE Failed-Attempt: TACACS+ accounting has failed, <log details>

- **Message Code:** 5415

  Severity: NOTICE

  Message Text: Change password failed

  Message Description: User change password failed. See FailureReason for more information.

  Local Target Message Format: <timestamp> <seq_num> 5415 NOTICE Failed-Attempt: Change password failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5415 NOTICE Failed-Attempt: Change password failed, <log details>

- **Message Code:** 5416

  Severity: NOTICE

  Message Text: RADIUS PAP session cleaned up

  Message Description: The RADIUS PAP session has been cleaned up

  Local Target Message Format: <timestamp> <seq_num> 5416 NOTICE Failed-Attempt: RADIUS PAP session cleaned up, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5416 NOTICE Failed-Attempt: RADIUS PAP session cleaned up, <log details>

- **Message Code:** 5417

  Severity: NOTICE

  Message Text: Dynamic Authorization failed

  Message Description: Dynamic Authorization failed

  Local Target Message Format: <timestamp> <seq_num> 5417 NOTICE Dynamic-Authorization: Dynamic Authorization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5417 NOTICE Dynamic-Authorization: Dynamic Authorization failed, <log details>

- **Message Code:** 5418

  Severity: NOTICE

Message Text: Guest Authentication Failed

Message Description: Guest Authentication failed; please see Failure code for more details

Local Target Message Format: <timestamp> <seq_num> 5418 NOTICE Guest: Guest Authentication Failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5418 NOTICE Guest: Guest Authentication Failed, <log details>

- **Message Code:** 5419

  Severity: NOTICE

  Message Text: DACL Download Failed

  Message Description: DACL Download Failed

  Local Target Message Format: <timestamp> <seq_num> 5419 NOTICE Failed-Attempt: DACL Download Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5419 NOTICE Failed-Attempt: DACL Download Failed, <log details>

- **Message Code:** 5420

  Severity: NOTICE

  Message Text: TrustSec Data Download Failed

  Message Description: TrustSec Data Download Failed

  Local Target Message Format: <timestamp> <seq_num> 5420 NOTICE Failed-Attempt: TrustSec Data Download Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5420 NOTICE Failed-Attempt: TrustSec Data Download Failed, <log details>

- **Message Code:** 5421

  Severity: NOTICE

  Message Text: TrustSec Peer Policy Download Failed

  Message Description: TrustSec Peer Policy Download Failed

  Local Target Message Format: <timestamp> <seq_num> 5421 NOTICE Failed-Attempt: TrustSec Peer Policy Download Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5421 NOTICE Failed-Attempt: TrustSec Peer Policy Download Failed, <log details>

- **Message Code:** 5422

  Severity: NOTICE

  Message Text: Authorize-Only failed

Message Description: Authorize-Only failed. See FailureReason for more information

Local Target Message Format: <timestamp> <seq_num> 5422 NOTICE Failed-Attempt: Authorize-Only failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5422 NOTICE Failed-Attempt: Authorize-Only failed, <log details>

- **Message Code:** 5423

  Severity: NOTICE

  Message Text: Device Registration Web Authentication Failed

  Message Description: Device Registration Web Authentication Failed

  Local Target Message Format: <timestamp> <seq_num> 5423 NOTICE Guest: Device Registration Web Authentication Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5423 NOTICE Guest: Device Registration Web Authentication Failed, <log details>

- **Message Code:** 5434

  Severity: WARN

  Message Text: Endpoint conducted several failed authentications of the same scenario

  Message Description: Endpoint conducted several failed authentications of the same scenario

  Local Target Message Format: <timestamp> <seq_num> 5434 WARN RADIUS: Endpoint conducted several failed authentications of the same scenario, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5434 WARN RADIUS: Endpoint conducted several failed authentications of the same scenario, <log details>

- **Message Code:** 5435

  Severity: WARN

  Message Text: NAS conducted several failed authentications of the same scenario

  Message Description: NAS conducted several failed authentications of the same scenario

  Local Target Message Format: <timestamp> <seq_num> 5435 WARN RADIUS: NAS conducted several failed authentications of the same scenario, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5435 WARN RADIUS: NAS conducted several failed authentications of the same scenario, <log details>

- **Message Code:** 5436

  Severity: WARN

  Message Text: RADIUS packet already in the process

Message Description: Ignoring this request because it is a duplicate of another packet that is currently being processed

Local Target Message Format: <timestamp> <seq_num> 5436 WARN RADIUS: RADIUS packet already in the process, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5436 WARN RADIUS: RADIUS packet already in the process, <log details>

- **Message Code:** 5437

  Severity: WARN

  Message Text: Duplicate RADIUS packet for existing session but with different RADIUS parameters

  Message Description: A duplicate RADIUS request was detected for the packet that was already processed or for the packet that was already accepted but this time with at least one different parameter in Source IP, Source Port, RADIUS ID. Dropping. Possible unexpected NAD behavior.

  Local Target Message Format: <timestamp> <seq_num> 5437 WARN RADIUS: Duplicate RADIUS packet for existing session but with different RADIUS parameters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5437 WARN RADIUS: Duplicate RADIUS packet for existing session but with different RADIUS parameters, <log details>

- **Message Code:** 5438

  Severity: WARN

  Message Text: RADIUS packet contains session on this PSN that does not exist

  Message Description: Session was not found on this ISE. Possible unexpected NAD behavior. Session belongs to this ISE according to hostname but may has already been reaped by timeout. This packet arrived too late.

  Local Target Message Format: <timestamp> <seq_num> 5438 WARN RADIUS: RADIUS packet contains session on this PSN that does not exist, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5438 WARN RADIUS: RADIUS packet contains session on this PSN that does not exist, <log details>

- **Message Code:** 5439

  Severity: WARN

  Message Text: RADIUS packet contains session not started on this PSN

  Message Description: Session does not belong to this ISE according to hostname. Possible unexpected NAD behavior. Maybe NAD sent a packet from the middle of the conversation with another ISE.

  Local Target Message Format: <timestamp> <seq_num> 5439 WARN RADIUS: RADIUS packet contains session not started on this PSN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5439 WARN RADIUS: RADIUS packet contains session not started on this PSN, <log details>

- **Message Code:** 5440

  Severity: WARN

  Message Text: Endpoint abandoned EAP session and started new

  Message Description: Endpoint started new authentication while previous is still in progress. Most probable that supplicant on that endpoint stopped conducting the previous authentication and started the new one. Closing the previous authentication.

  Local Target Message Format: <timestamp> <seq_num> 5440 WARN RADIUS: Endpoint abandoned EAP session and started new, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5440 WARN RADIUS: Endpoint abandoned EAP session and started new, <log details>

- **Message Code:** 5441

  Severity: WARN

  Message Text: Endpoint started new session while the packet of previous session is being processed. Dropping new session.

  Message Description: Endpoint started new session while the packet of previous session is being processed

  Local Target Message Format: <timestamp> <seq_num> 5441 WARN RADIUS: Endpoint started new session while the packet of previous session is being processed. Dropping new session., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5441 WARN RADIUS: Endpoint started new session while the packet of previous session is being processed. Dropping new session., <log details>

- **Message Code:** 5442

  Severity: WARN

  Message Text: RADIUS request dropped due to system overload

  Message Description: A RADIUS request was dropped due to system overload. This condition can be caused by too many parallel authentication requests.

  Local Target Message Format: <timestamp> <seq_num> 5442 WARN RADIUS: RADIUS request dropped due to system overload, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5442 WARN RADIUS: RADIUS request dropped due to system overload, <log details>

- **Message Code:** 5443

  Severity: WARN

  Message Text: RADIUS request dropped due to reaching EAP sessions limit

  Message Description: A RADIUS request was dropped due to reaching EAP sessions limit. This condition can be caused by too many parallel EAP authentication requests.

Local Target Message Format: <timestamp> <seq_num> 5443 WARN RADIUS: RADIUS request dropped due to reaching EAP sessions limit, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5443 WARN RADIUS: RADIUS request dropped due to reaching EAP sessions limit, <log details>

- **Message Code:** 5447

  Severity: NOTICE

  Message Text: MDM Authentication Passed

  Message Description: MDM Authentication passed

  Local Target Message Format: <timestamp> <seq_num> 5447 NOTICE MDM: MDM Authentication Passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5447 NOTICE MDM: MDM Authentication Passed, <log details>

- **Message Code:** 5448

  Severity: NOTICE

  Message Text: MDM Authentication Failed

  Message Description: MDM Authentication failed; please see Failure code for more details

  Local Target Message Format: <timestamp> <seq_num> 5448 NOTICE MDM: MDM Authentication Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5448 NOTICE MDM: MDM Authentication Failed, <log details>

- **Message Code:** 5449

  Severity: WARN

  Message Text: Endpoint failed authentication of the same scenario several times and was rejected

  Message Description: Endpoint failed authentication of the same scenario several times and all further requests will be rejected for the duration of the Request Rejection Interval

  Local Target Message Format: <timestamp> <seq_num> 5449 WARN RADIUS: Endpoint failed authentication of the same scenario several times and was rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5449 WARN RADIUS: Endpoint failed authentication of the same scenario several times and was rejected, <log details>

- **Message Code:** 5450

  Severity: NOTICE

  Message Text: RADIUS DTLS handshake failed

  Message Description: RADIUS DTLS handshake failed

Local Target Message Format: <timestamp> <seq_num> 5450 NOTICE Failed-Attempt: RADIUS DTLS handshake failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5450 NOTICE Failed-Attempt: RADIUS DTLS handshake failed, <log details>

- **Message Code:** 5451

  Severity: INFO

  Message Text: Social Login: User did not grant permission for ISE application to read user's information from Facebook

  Message Description: Indicates that User did not grant permission for ISE application to read user's information from Facebook

  Local Target Message Format: <timestamp> <seq_num> 5451 INFO GUEST: Social Login: User did not grant permission for ISE application to read user's information from Facebook, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5451 INFO GUEST: Social Login: User did not grant permission for ISE application to read user's information from Facebook, <log details>

- **Message Code:** 5452

  Severity: WARN

  Message Text: Social Login: Error while getting Social User info

  Message Description: Indicates that there is an error while getting Social User info

  Local Target Message Format: <timestamp> <seq_num> 5452 WARN GUEST: Social Login: Error while getting Social User info, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5452 WARN GUEST: Social Login: Error while getting Social User info, <log details>

- **Message Code:** 5453

  Severity: WARN

  Message Text: Failed to resolve the authorization profile, sending disconnect.

  Message Description: Failed to resolve the authorization profile, sending disconnect.

  Local Target Message Format: <timestamp> <seq_num>5453 WARN Dynamic-Authorization Failed to resolve the authorization profile, sending disconnect., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>5453 WARN Dynamic-Authorization Failed to resolve the authorization profile, sending disconnect., <log details>

Guest

- **Message Code:** 86001

Severity: INFO

Message Text: Guest user has entered the guest portal login page

Message Description: Guest user has entered the guest portal login page

Local Target Message Format: <timestamp> <seq_num> 86001 INFO Guest: Guest user has entered the guest portal login page, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86001 INFO Guest: Guest user has entered the guest portal login page, <log details>

- **Message Code:** 86002

  Severity: INFO

  Message Text: Sponsor has suspended a guest user account

  Message Description: Sponsor has suspended a guest user account

  Local Target Message Format: <timestamp> <seq_num> 86002 INFO Guest: Sponsor has suspended a guest user account, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86002 INFO Guest: Sponsor has suspended a guest user account, <log details>

- **Message Code:** 86003

  Severity: INFO

  Message Text: Sponsor has enabled a guest user account

  Message Description: Sponsor has enabled a guest user account

  Local Target Message Format: <timestamp> <seq_num> 86003 INFO Guest: Sponsor has enabled a guest user account, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86003 INFO Guest: Sponsor has enabled a guest user account, <log details>

- **Message Code:** 86004

  Severity: INFO

  Message Text: Guest user has changed the password

  Message Description: Guest user has changed the password

  Local Target Message Format: <timestamp> <seq_num> 86004 INFO Guest: Guest user has changed the password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86004 INFO Guest: Guest user has changed the password, <log details>

- **Message Code:** 86005

  Severity: INFO

Message Text: Guest user has accepted the Use Policy

Message Description: Guest user has accepted the use policy

Local Target Message Format: <timestamp> <seq_num> 86005 INFO Guest: Guest user has accepted the Use Policy, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86005 INFO Guest: Guest user has accepted the Use Policy, <log details>

- **Message Code:** 86006

  Severity: INFO

  Message Text: Guest user account is created

  Message Description: Guest user account is created

  Local Target Message Format: <timestamp> <seq_num> 86006 INFO Guest: Guest user account is created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86006 INFO Guest: Guest user account is created, <log details>

- **Message Code:** 86007

  Severity: INFO

  Message Text: Guest user account is updated

  Message Description: Guest user account is updated

  Local Target Message Format: <timestamp> <seq_num> 86007 INFO Guest: Guest user account is updated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86007 INFO Guest: Guest user account is updated, <log details>

- **Message Code:** 86008

  Severity: INFO

  Message Text: Guest user account is deleted

  Message Description: Guest user account is deleted

  Local Target Message Format: <timestamp> <seq_num> 86008 INFO Guest: Guest user account is deleted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86008 INFO Guest: Guest user account is deleted, <log details>

- **Message Code:** 86009

  Severity: INFO

  Message Text: Guest user is not found

Message Description: Guest user record is not found in the database

Local Target Message Format: <timestamp> <seq_num> 86009 INFO Guest: Guest user is not found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86009 INFO Guest: Guest user is not found, <log details>

- **Message Code:** 86010

  Severity: INFO

  Message Text: Guest user authentication failed

  Message Description: Guest user authentication failed. Please check your password and account permission

  Local Target Message Format: <timestamp> <seq_num> 86010 INFO Guest: Guest user authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86010 INFO Guest: Guest user authentication failed, <log details>

- **Message Code:** 86011

  Severity: INFO

  Message Text: Guest user is not enabled

  Message Description: Guest user authentication failed. User is not enabled. Please contact your system administrator

  Local Target Message Format: <timestamp> <seq_num> 86011 INFO Guest: Guest user is not enabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86011 INFO Guest: Guest user is not enabled, <log details>

- **Message Code:** 86012

  Severity: INFO

  Message Text: User declined Access-Use Policy

  Message Description: Guest User must accept Access-Use policy before network access is granted

  Local Target Message Format: <timestamp> <seq_num> 86012 INFO Guest: User declined Access-Use Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86012 INFO Guest: User declined Access-Use Policy, <log details>

- **Message Code:** 86013

  Severity: INFO

  Message Text: Portal not found

Message Description: Portal is not found in the database. Please contact your system administrator

Local Target Message Format: <timestamp> <seq_num> 86013 INFO Guest: Portal not found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86013 INFO Guest: Portal not found, <log details>

- **Message Code:** 86014

  Severity: INFO

  Message Text: User is suspended

  Message Description: User authentication failed. User account is suspended

  Local Target Message Format: <timestamp> <seq_num> 86014 INFO Guest: User is suspended, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86014 INFO Guest: User is suspended, <log details>

- **Message Code:** 86015

  Severity: INFO

  Message Text: Invalid Password Change

  Message Description: Invalid password change. Use correct password based on the password policy

  Local Target Message Format: <timestamp> <seq_num> 86015 INFO Guest: Invalid Password Change, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86015 INFO Guest: Invalid Password Change, <log details>

- **Message Code:** 86016

  Severity: INFO

  Message Text: Guest Timeout Exceeded

  Message Description: Timeout from server has exceeded the threshold. Please contact your system administrator

  Local Target Message Format: <timestamp> <seq_num> 86016 INFO Guest: Guest Timeout Exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86016 INFO Guest: Guest Timeout Exceeded, <log details>

- **Message Code:** 86017

  Severity: INFO

  Message Text: Session Missing

Message Description: SessionID is missing. Please contact your System Administrator

Local Target Message Format: <timestamp> <seq_num> 86017 INFO Guest: Session Missing, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86017 INFO Guest: Session Missing, <log details>

- **Message Code:** 86018

  Severity: INFO

  Message Text: Guest Change of Authorization Failed

  Message Description: Guest Change of Authorization has failed. Please contact your System Administrator

  Local Target Message Format: <timestamp> <seq_num> 86018 INFO Guest: Guest Change of Authorization Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86018 INFO Guest: Guest Change of Authorization Failed, <log details>

- **Message Code:** 86019

  Severity: INFO

  Message Text: Guest User restricted

  Message Description: User access is restricted based on time profile. Please contact your system administrator

  Local Target Message Format: <timestamp> <seq_num> 86019 INFO Guest: Guest User restricted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86019 INFO Guest: Guest User restricted, <log details>

- **Message Code:** 86020

  Severity: INFO

  Message Text: Guest Unknown Error

  Message Description: User authentication failed. Please contact your System Administrator

  Local Target Message Format: <timestamp> <seq_num> 86020 INFO Guest: Guest Unknown Error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86020 INFO Guest: Guest Unknown Error, <log details>

- **Message Code:** 86021

  Severity: INFO

  Message Text: Entering Device Registration Web Authentication Portal

Message Description: Entering Device Registration Web Authentication Portal

Local Target Message Format: <timestamp> <seq_num> 86021 INFO Guest: Entering Device Registration Web Authentication Portal, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86021 INFO Guest: Entering Device Registration Web Authentication Portal, <log details>

- **Message Code:** 86022

  Severity: INFO

  Message Text: Device Registration Web Authentication AUP Accepted

  Message Description: Device Registration Web Authentication AUP (Acceptable Use Policy) accepted

  Local Target Message Format: <timestamp> <seq_num> 86022 INFO Guest: Device Registration Web Authentication AUP Accepted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86022 INFO Guest: Device Registration Web Authentication AUP Accepted, <log details>

- **Message Code:** 86023

  Severity: INFO

  Message Text: Device Registration Web Authentication AUP Declined

  Message Description: Device Registration Web Authentication AUP (Acceptable Use Policy) declined

  Local Target Message Format: <timestamp> <seq_num> 86023 INFO Guest: Device Registration Web Authentication AUP Declined, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86023 INFO Guest: Device Registration Web Authentication AUP Declined, <log details>

- **Message Code:** 86024

  Severity: INFO

  Message Text: Device Registration Web Authentication Portal Endpoint Creation Passed

  Message Description: Device Registration Web Authentication Portal successfully created an endpoint

  Local Target Message Format: <timestamp> <seq_num> 86024 INFO Guest: Device Registration Web Authentication Portal Endpoint Creation Passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86024 INFO Guest: Device Registration Web Authentication Portal Endpoint Creation Passed, <log details>

- **Message Code:** 86025

  Severity: ERROR

  Message Text: Device Registration Web Authentication Portal Endpoint Creation Failed

  Message Description: Device Registration Web Authentication Portal failed to created an endpoint

Local Target Message Format: <timestamp> <seq_num> 86025 ERROR Guest: Device Registration Web Authentication Portal Endpoint Creation Failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86025 ERROR Guest: Device Registration Web Authentication Portal Endpoint Creation Failed, <log details>

- **Message Code:** 86026

  Severity: ERROR

  Message Text: Device Registration Web Authentication Portal CoA Termination Failed

  Message Description: Device Registration Web Authentication Portal failed to perform a CoA termination

  Local Target Message Format: <timestamp> <seq_num> 86026 ERROR Guest: Device Registration Web Authentication Portal CoA Termination Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86026 ERROR Guest: Device Registration Web Authentication Portal CoA Termination Failed, <log details>

- **Message Code:** 86027

  Severity: INFO

  Message Text: Device Registration Web Authentication sending CoA Termination message

  Message Description: Device Registration Web Authentication sending CoA Termination message

  Local Target Message Format: <timestamp> <seq_num> 86027 INFO Guest: Device Registration Web Authentication sending CoA Termination message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86027 INFO Guest: Device Registration Web Authentication sending CoA Termination message, <log details>

- **Message Code:** 86028

  Severity: INFO

  Message Text: Successfully performed CoA termination(s) for a deleted guest or a suspended guest

  Message Description: Successfully performed CoA termination(s) for a deleted guest or a suspended guest

  Local Target Message Format: <timestamp> <seq_num> 86028 INFO Guest: Successfully performed CoA termination(s) for a deleted guest or a suspended guest, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86028 INFO Guest: Successfully performed CoA termination(s) for a deleted guest or a suspended guest, <log details>

- **Message Code:** 86029

  Severity: WARN

  Message Text: Failed to perform a CoA termination

  Message Description: Failed to perform a CoA termination

Local Target Message Format: <timestamp> <seq_num> 86029 WARN Guest: Failed to perform a CoA termination, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86029 WARN Guest: Failed to perform a CoA termination, <log details>

- **Message Code:** 86030

  Severity: INFO

  Message Text: Sponsor user accepted the user policy

  Message Description: Indicates that a sponsor user accepted user policy

  Local Target Message Format: <timestamp> <seq_num> 86030 INFO GUEST: Sponsor user accepted the user policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86030 INFO GUEST: Sponsor user accepted the user policy, <log details>

- **Message Code:** 86031

  Severity: INFO

  Message Text: Sponsor user declined the user policy

  Message Description: Indicates that a sponsor user declined user policy

  Local Target Message Format: <timestamp> <seq_num> 86031 INFO GUEST: Sponsor user declined the user policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 86031 INFO GUEST: Sponsor user declined the user policy, <log details>

Identity Stores Diagnostics

- **Message Code:** 24000

  Severity: INFO

  Message Text: Connection established with LDAP server

  Message Description: Connection established with LDAP server

  Local Target Message Format: <timestamp> <seq_num> 24000 INFO External-LDAP: Connection established with LDAP server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24000 INFO External-LDAP: Connection established with LDAP server, <log details>

- **Message Code:** 24001

  Severity: ERROR

Message Text: Cannot establish connection with LDAP server

Message Description: Cannot establish connection with LDAP server

Local Target Message Format: <timestamp> <seq_num> 24001 ERROR External-LDAP: Cannot establish connection with LDAP server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24001 ERROR External-LDAP: Cannot establish connection with LDAP server, <log details>

- **Message Code:** 24002

  Severity: ERROR

  Message Text: Cannot bind connection with administrator credentials

  Message Description: Cannot bind connection with administrator credentials

  Local Target Message Format: <timestamp> <seq_num> 24002 ERROR External-LDAP: Cannot bind connection with administrator credentials, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24002 ERROR External-LDAP: Cannot bind connection with administrator credentials, <log details>

- **Message Code:** 24003

  Severity: ERROR

  Message Text: Cannot bind connection with anonymous credentials

  Message Description: Cannot bind connection with anonymous credentials

  Local Target Message Format: <timestamp> <seq_num> 24003 ERROR External-LDAP: Cannot bind connection with anonymous credentials, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24003 ERROR External-LDAP: Cannot bind connection with anonymous credentials, <log details>

- **Message Code:** 24004

  Severity: DEBUG

  Message Text: User search finished successfully

  Message Description: User search finished successfully in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24004 DEBUG External-LDAP: User search finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24004 DEBUG External-LDAP: User search finished successfully, <log details>

- **Message Code:** 24005

  Severity: DEBUG

  Message Text: Host search finished successfully

Message Description: Host search finished successfully in LDAP Server

Local Target Message Format: <timestamp> <seq_num> 24005 DEBUG External-LDAP: Host search finished successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24005 DEBUG External-LDAP: Host search finished successfully, <log details>

- **Message Code:** 24006

  Severity: ERROR

  Message Text: User search ended with an error

  Message Description: User search ended with an error

  Local Target Message Format: <timestamp> <seq_num> 24006 ERROR External-LDAP: User search ended with an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24006 ERROR External-LDAP: User search ended with an error, <log details>

- **Message Code:** 24007

  Severity: ERROR

  Message Text: Host search ended with an error

  Message Description: Host search ended with an error

  Local Target Message Format: <timestamp> <seq_num> 24007 ERROR External-LDAP: Host search ended with an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24007 ERROR External-LDAP: Host search ended with an error, <log details>

- **Message Code:** 24008

  Severity: DEBUG

  Message Text: User not found in LDAP Server

  Message Description: User is not found in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24008 DEBUG External-LDAP: User not found in LDAP Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24008 DEBUG External-LDAP: User not found in LDAP Server, <log details>

- **Message Code:** 24009

  Severity: DEBUG

  Message Text: Host not found in LDAP Server

  Message Description: Host is not found in LDAP Server

Local Target Message Format: <timestamp> <seq_num> 24009 DEBUG External-LDAP: Host not found in LDAP Server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24009 DEBUG External-LDAP: Host not found in LDAP Server, <log details>

- **Message Code:** 24010

  Severity: DEBUG

  Message Text: Ambiguous user

  Message Description: Multiple users matching the username are found in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24010 DEBUG External-LDAP: Ambiguous user, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24010 DEBUG External-LDAP: Ambiguous user, <log details>

- **Message Code:** 24011

  Severity: DEBUG

  Message Text: Ambiguous host

  Message Description: Multiple users matching the hostname are found in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24011 DEBUG External-LDAP: Ambiguous host, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24011 DEBUG External-LDAP: Ambiguous host, <log details>

- **Message Code:** 24014

  Severity: DEBUG

  Message Text: Noncompliant attributes detected in LDAP

  Message Description: Noncompliant attributes detected in LDAP

  Local Target Message Format: <timestamp> <seq_num> 24014 DEBUG External-LDAP: Noncompliant attributes detected in LDAP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24014 DEBUG External-LDAP: Noncompliant attributes detected in LDAP, <log details>

- **Message Code:** 24015

  Severity: DEBUG

  Message Text: Authenticating user against LDAP Server

  Message Description: Authenticating user against LDAP Server

Local Target Message Format: <timestamp> <seq_num> 24015 DEBUG External-LDAP: Authenticating user against LDAP Server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24015 DEBUG External-LDAP: Authenticating user against LDAP Server, <log details>

- **Message Code:** 24016

  Severity: DEBUG

  Message Text: Looking up user in LDAP Server

  Message Description: Looking up user in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24016 DEBUG External-LDAP: Looking up user in LDAP Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24016 DEBUG External-LDAP: Looking up user in LDAP Server, <log details>

- **Message Code:** 24017

  Severity: DEBUG

  Message Text: Looking up host in LDAP Server

  Message Description: Looking up host in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24017 DEBUG External-LDAP: Looking up host in LDAP Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24017 DEBUG External-LDAP: Looking up host in LDAP Server, <log details>

- **Message Code:** 24018

  Severity: DEBUG

  Message Text: Cannot retrieve user's certificate

  Message Description: Certificate is not found on user's record in LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24018 DEBUG External-LDAP: Cannot retrieve user's certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24018 DEBUG External-LDAP: Cannot retrieve user's certificate, <log details>

- **Message Code:** 24019

  Severity: ERROR

  Message Text: LDAP connection error was encountered

  Message Description: ISE cannot connect to LDAP external ID store

Local Target Message Format: <timestamp> <seq_num> 24019 ERROR External-LDAP: LDAP connection error was encountered, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24019 ERROR External-LDAP: LDAP connection error was encountered, <log details>

- **Message Code:** 24020

  Severity: DEBUG

  Message Text: User authentication against the LDAP Server failed

  Message Description: User authentication against the LDAP Server failed. The user entered the wrong password or the user record in the LDAP Server is disabled or expired

  Local Target Message Format: <timestamp> <seq_num> 24020 DEBUG External-LDAP: User authentication against the LDAP Server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24020 DEBUG External-LDAP: User authentication against the LDAP Server failed, <log details>

- **Message Code:** 24021

  Severity: ERROR

  Message Text: User authentication ended with an error

  Message Description: User authentication against LDAP Server ended with an error

  Local Target Message Format: <timestamp> <seq_num> 24021 ERROR External-LDAP: User authentication ended with an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24021 ERROR External-LDAP: User authentication ended with an error, <log details>

- **Message Code:** 24022

  Severity: DEBUG

  Message Text: User authentication succeeded

  Message Description: User authentication against LDAP Server succeeded

  Local Target Message Format: <timestamp> <seq_num> 24022 DEBUG External-LDAP: User authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24022 DEBUG External-LDAP: User authentication succeeded, <log details>

- **Message Code:** 24023

  Severity: DEBUG

  Message Text: User's groups are retrieved

  Message Description: User's groups are retrieved from LDAP Server

Local Target Message Format: <timestamp> <seq_num> 24023 DEBUG External-LDAP: User's groups are retrieved, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24023 DEBUG External-LDAP: User's groups are retrieved, <log details>

- **Message Code:** 24024

  Severity: DEBUG

  Message Text: Host's groups are retrieved

  Message Description: Host's groups are retrieved from LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24024 DEBUG External-LDAP: Host's groups are retrieved, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24024 DEBUG External-LDAP: Host's groups are retrieved, <log details>

- **Message Code:** 24025

  Severity: DEBUG

  Message Text: No user's groups are found

  Message Description: No user's groups are found on LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24025 DEBUG External-LDAP: No user's groups are found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24025 DEBUG External-LDAP: No user's groups are found, <log details>

- **Message Code:** 24026

  Severity: DEBUG

  Message Text: No host's groups are found

  Message Description: No host's groups are found on LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24026 DEBUG External-LDAP: No host's groups are found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24026 DEBUG External-LDAP: No host's groups are found, <log details>

- **Message Code:** 24027

  Severity: ERROR

  Message Text: Groups search ended with an error

  Message Description: Groups search ended with an error

Local Target Message Format: <timestamp> <seq_num> 24027 ERROR External-LDAP: Groups search ended with an error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24027 ERROR External-LDAP: Groups search ended with an error, <log details>

- **Message Code:** 24028

  Severity: DEBUG

  Message Text: User's attributes are retrieved

  Message Description: User's attributes are retrieved from LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24028 DEBUG External-LDAP: User's attributes are retrieved, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24028 DEBUG External-LDAP: User's attributes are retrieved, <log details>

- **Message Code:** 24029

  Severity: DEBUG

  Message Text: Host's attributes are retrieved

  Message Description: Host's attributes are retrieved from LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24029 DEBUG External-LDAP: Host's attributes are retrieved, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24029 DEBUG External-LDAP: Host's attributes are retrieved, <log details>

- **Message Code:** 24030

  Severity: ERROR

  Message Text: SSL connection error was encountered

  Message Description: SSL connection error was encountered

  Local Target Message Format: <timestamp> <seq_num> 24030 ERROR External-LDAP: SSL connection error was encountered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24030 ERROR External-LDAP: SSL connection error was encountered, <log details>

- **Message Code:** 24031

  Severity: INFO

  Message Text: Sending request to primary LDAP server

  Message Description: Sending request to primary LDAP server

Local Target Message Format: <timestamp> <seq_num> 24031 INFO External-LDAP: Sending request to primary LDAP server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24031 INFO External-LDAP: Sending request to primary LDAP server, <log details>

- **Message Code:** 24032

  Severity: INFO

  Message Text: Sending request to secondary LDAP server

  Message Description: Sending request to secondary LDAP server

  Local Target Message Format: <timestamp> <seq_num> 24032 INFO External-LDAP: Sending request to secondary LDAP server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24032 INFO External-LDAP: Sending request to secondary LDAP server, <log details>

- **Message Code:** 24033

  Severity: INFO

  Message Text: Primary server failover. Switching to secondary server

  Message Description: Unable to connect to the primary server

  Local Target Message Format: <timestamp> <seq_num> 24033 INFO External-LDAP: Primary server failover. Switching to secondary server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24033 INFO External-LDAP: Primary server failover. Switching to secondary server, <log details>

- **Message Code:** 24034

  Severity: INFO

  Message Text: Secondary server failover. Switching to primary server

  Message Description: Unable to connect to the secondary server

  Local Target Message Format: <timestamp> <seq_num> 24034 INFO External-LDAP: Secondary server failover. Switching to primary server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24034 INFO External-LDAP: Secondary server failover. Switching to primary server, <log details>

- **Message Code:** 24035

  Severity: INFO

  Message Text: Perform domain prefix stripping

  Message Description: Perform domain prefix stripping

Local Target Message Format: <timestamp> <seq_num> 24035 INFO External-LDAP: Perform domain prefix stripping, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24035 INFO External-LDAP: Perform domain prefix stripping, <log details>

- **Message Code:** 24036

  Severity: INFO

  Message Text: Perform domain suffix stripping

  Message Description: Perform domain suffix stripping

  Local Target Message Format: <timestamp> <seq_num> 24036 INFO External-LDAP: Perform domain suffix stripping, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24036 INFO External-LDAP: Perform domain suffix stripping, <log details>

- **Message Code:** 24037

  Severity: DEBUG

  Message Text: Sent a subject search request

  Message Description: Sent a subject search request.

  Local Target Message Format: <timestamp> <seq_num> 24037 DEBUG External-LDAP: Sent a subject search request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24037 DEBUG External-LDAP: Sent a subject search request, <log details>

- **Message Code:** 24038

  Severity: DEBUG

  Message Text: Received a subject search response

  Message Description: Received a subject search response.

  Local Target Message Format: <timestamp> <seq_num> 24038 DEBUG External-LDAP: Received a subject search response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24038 DEBUG External-LDAP: Received a subject search response, <log details>

- **Message Code:** 24039

  Severity: DEBUG

  Message Text: Sent a subject's group search request

  Message Description: Sent a subject's group search request.

Local Target Message Format: <timestamp> <seq_num> 24039 DEBUG External-LDAP: Sent a subject's group search request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24039 DEBUG External-LDAP: Sent a subject's group search request, <log details>

- **Message Code:** 24040

  Severity: DEBUG

  Message Text: Received a subject's group search response

  Message Description: Received a subject's group search response.

  Local Target Message Format: <timestamp> <seq_num> 24040 DEBUG External-LDAP: Received a subject's group search response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24040 DEBUG External-LDAP: Received a subject's group search response, <log details>

- **Message Code:** 24041

  Severity: DEBUG

  Message Text: Sent subject bind request

  Message Description: Sent subject bind request

  Local Target Message Format: <timestamp> <seq_num> 24041 DEBUG External-LDAP: Sent subject bind request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24041 DEBUG External-LDAP: Sent subject bind request, <log details>

- **Message Code:** 24042

  Severity: DEBUG

  Message Text: Received subject bind response

  Message Description: Received subject bind response

  Local Target Message Format: <timestamp> <seq_num> 24042 DEBUG External-LDAP: Received subject bind response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24042 DEBUG External-LDAP: Received subject bind response, <log details>

- **Message Code:** 24043

  Severity: DEBUG

  Message Text: Sent an administrator bind request

  Message Description: Sent an administrator bind request.

Local Target Message Format: <timestamp> <seq_num> 24043 DEBUG External-LDAP: Sent an administrator bind request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24043 DEBUG External-LDAP: Sent an administrator bind request, <log details>

- **Message Code:** 24044

  Severity: DEBUG

  Message Text: Received an administrator bind response

  Message Description: Received an administrator bind response.

  Local Target Message Format: <timestamp> <seq_num> 24044 DEBUG External-LDAP: Received an administrator bind response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24044 DEBUG External-LDAP: Received an administrator bind response, <log details>

- **Message Code:** 24050

  Severity: WARN

  Message Text: Cannot authenticate with LDAP Identity Store because password was not present or was empty

  Message Description: ISE did not receive user password or received empty password. Plain password authentication cannot be performed with no password or empty password

  Local Target Message Format: <timestamp> <seq_num> 24050 WARN External-LDAP: Cannot authenticate with LDAP Identity Store because password was not present or was empty, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24050 WARN External-LDAP: Cannot authenticate with LDAP Identity Store because password was not present or was empty, <log details>

- **Message Code:** 24051

  Severity: ERROR

  Message Text: Secure LDAP failed SSL handshake because of an unknown CA in the certificates chain

  Message Description: Secure LDAP failed SSL handshake because of an unknown CA in the certificates chain

  Local Target Message Format: <timestamp> <seq_num> 24051 ERROR External-LDAP: Secure LDAP failed SSL handshake because of an unknown CA in the certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24051 ERROR External-LDAP: Secure LDAP failed SSL handshake because of an unknown CA in the certificates chain, <log details>

- **Message Code:** 24052

  Severity: ERROR

Message Text: Secure LDAP connection reconnect due to OCSP found revoked certificate

Message Description: OCSP check result is that the certificate used for LDAP connection is revoked

Local Target Message Format: <timestamp> <seq_num> 24052 ERROR External-LDAP: Secure LDAP connection reconnect due to OCSP found revoked certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24052 ERROR External-LDAP: Secure LDAP connection reconnect due to OCSP found revoked certificate, <log details>

- **Message Code:** 24053

  Severity: ERROR

  Message Text: Secure LDAP connection reconnect due to CRL found revoked certificate

  Message Description: CRL check result is that the certificate used for LDAP connection is revoked

  Local Target Message Format: <timestamp> <seq_num> 24053 ERROR External-LDAP: Secure LDAP connection reconnect due to CRL found revoked certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24053 ERROR External-LDAP: Secure LDAP connection reconnect due to CRL found revoked certificate, <log details>

- **Message Code:** 24054

  Severity: DEBUG

  Message Text: User authentication against LDAP server detected that user password has expired

  Message Description: The password has expired but there are remaining grace authentications. The user needs to change it

  Local Target Message Format: <timestamp> <seq_num> 24054 DEBUG External-LDAP: User authentication against LDAP server detected that user password has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24054 DEBUG External-LDAP: User authentication against LDAP server detected that user password has expired, <log details>

- **Message Code:** 24055

  Severity: DEBUG

  Message Text: User authentication against LDAP server detected that the user is authenticating for the first time after the password administrator set the password

  Message Description: The user needs to change his password immediately

  Local Target Message Format: <timestamp> <seq_num> 24055 DEBUG External-LDAP: User authentication against LDAP server detected that the user is authenticating for the first time after the password administrator set the password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24055 DEBUG External-LDAP: User authentication against LDAP server detected that the user is authenticating for the first time after the password administrator set the password, <log details>

- **Message Code:** 24056

  Severity: WARN

  Message Text: User authentication against LDAP server detected that user password has expired and there are no more grace authentications

  Message Description: The user needs to contact the password administrator in order to have its password reset

  Local Target Message Format: <timestamp> <seq_num> 24056 WARN External-LDAP: User authentication against LDAP server detected that user password has expired and there are no more grace authentications, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24056 WARN External-LDAP: User authentication against LDAP server detected that user password has expired and there are no more grace authentications, <log details>

- **Message Code:** 24057

  Severity: WARN

  Message Text: User authentication against LDAP server detected that the password failure limit has been reached and the account is locked

  Message Description: The user needs to retry later or contact the password administrator to reset the password

  Local Target Message Format: <timestamp> <seq_num> 24057 WARN External-LDAP: User authentication against LDAP server detected that the password failure limit has been reached and the account is locked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24057 WARN External-LDAP: User authentication against LDAP server detected that the password failure limit has been reached and the account is locked, <log details>

- **Message Code:** 24058

  Severity: ERROR

  Message Text: LDAP server does not support password modify extended operation (RFC 3062)

  Message Description: ACS Administrator should disable password change on LDAP Identity Store configuration

  Local Target Message Format: <timestamp> <seq_num> 24058 ERROR External-LDAP: LDAP server does not support password modify extended operation (RFC 3062), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24058 ERROR External-LDAP: LDAP server does not support password modify extended operation (RFC 3062), <log details>

- **Message Code:** 24059

  Severity: ERROR

  Message Text: User password change ended with an error

Message Description: LDAP server logs should be examined for getting more details

Local Target Message Format: <timestamp> <seq_num> 24059 ERROR External-LDAP: User password change ended with an error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24059 ERROR External-LDAP: User password change ended with an error, <log details>

- **Message Code:** 24060

  Severity: INFO

  Message Text: Changing user's password on LDAP Server

  Message Description: Changing user's password on LDAP Server

  Local Target Message Format: <timestamp> <seq_num> 24060 INFO External-LDAP: Changing user's password on LDAP Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24060 INFO External-LDAP: Changing user's password on LDAP Server, <log details>

- **Message Code:** 24061

  Severity: DEBUG

  Message Text: Sent password modify request

  Message Description: Sent password modify request

  Local Target Message Format: <timestamp> <seq_num> 24061 DEBUG External-LDAP: Sent password modify request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24061 DEBUG External-LDAP: Sent password modify request, <log details>

- **Message Code:** 24062

  Severity: DEBUG

  Message Text: Received password modify response

  Message Description: Received password modify response

  Local Target Message Format: <timestamp> <seq_num> 24062 DEBUG External-LDAP: Received password modify response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24062 DEBUG External-LDAP: Received password modify response, <log details>

- **Message Code:** 24063

  Severity: WARN

  Message Text: The user's password will expire soon

  Message Description: The user's password will expire soon

Local Target Message Format: <timestamp> <seq_num> 24063 WARN External-LDAP: The user's password will expire soon, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24063 WARN External-LDAP: The user's password will expire soon, <log details>

- **Message Code:** 24064

  Severity: WARN

  Message Text: The user doesn't have sufficient rights to change password

  Message Description: The user doesn't have sufficient rights to change password

  Local Target Message Format: <timestamp> <seq_num> 24064 WARN External-LDAP: The user doesn't have sufficient rights to change password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24064 WARN External-LDAP: The user doesn't have sufficient rights to change password, <log details>

- **Message Code:** 24065

  Severity: WARN

  Message Text: The new password does not conform to LDAP password policy

  Message Description: The new password does not conform to LDAP password policy

  Local Target Message Format: <timestamp> <seq_num> 24065 WARN External-LDAP: The new password does not conform to LDAP password policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24065 WARN External-LDAP: The new password does not conform to LDAP password policy, <log details>

- **Message Code:** 24066

  Severity: INFO

  Message Text: User password change succeeded

  Message Description: User password change on LDAP Server succeeded

  Local Target Message Format: <timestamp> <seq_num> 24066 INFO External-LDAP: User password change succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24066 INFO External-LDAP: User password change succeeded, <log details>

- **Message Code:** 24067

  Severity: WARN

  Message Text: The password change is not enabled on LDAP Identity Store configuration page

  Message Description: The password change is not enabled on LDAP Identity Store configuration page

Local Target Message Format: <timestamp> <seq_num> 24067 WARN External-LDAP: The password change is not enabled on LDAP Identity Store configuration page, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24067 WARN External-LDAP: The password change is not enabled on LDAP Identity Store configuration page, <log details>

- **Message Code:** 24100

  Severity: DEBUG

  Message Text: Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes

  Message Description: Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.

  Local Target Message Format: <timestamp> <seq_num> 24100 DEBUG Generic-ID-Store: Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24100 DEBUG Generic-ID-Store: Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes, <log details>

- **Message Code:** 24101

  Severity: WARN

  Message Text: Some of the retrieved attributes contain multiple values. These values are discarded. The default values, if configured, will be used for these attributes

  Message Description: Some of the retrieved attributes contain multiple values. These values are discarded. The default values, if configured, will be used for these attributes.

  Local Target Message Format: <timestamp> <seq_num> 24101 WARN Generic-ID-Store: Some of the retrieved attributes contain multiple values. These values are discarded. The default values, if configured, will be used for these attributes, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24101 WARN Generic-ID-Store: Some of the retrieved attributes contain multiple values. These values are discarded. The default values, if configured, will be used for these attributes, <log details>

- **Message Code:** 24102

  Severity: WARN

  Message Text: Some of the retrieved attributes contain values that are of an incompatible type. These values are discarded. The default values, if configured, will be used for these attributes

  Message Description: Some of the retrieved attributes contain values that are of an incompatible type. These values are discarded. The default values, if configured, will be used for these attributes.

  Local Target Message Format: <timestamp> <seq_num> 24102 WARN Generic-ID-Store: Some of the retrieved attributes contain values that are of an incompatible type. These values are discarded. The default values, if configured, will be used for these attributes, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24102 WARN Generic-ID-Store: Some of the retrieved attributes contain values that are of an incompatible type. These values are discarded. The default values, if configured, will be used for these attributes, <log details>

- **Message Code:** 24201

  Severity: INFO

  Message Text: Internal ID Store successfully connected to database

  Message Description: Internal ID Store successfully connected to database

  Local Target Message Format: <timestamp> <seq_num> 24201 INFO Local-user-DB: Internal ID Store successfully connected to database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24201 INFO Local-user-DB: Internal ID Store successfully connected to database, <log details>

- **Message Code:** 24202

  Severity: ERROR

  Message Text: Internal ID Store could not connect to the database

  Message Description: Internal ID Store could not connect to the database

  Local Target Message Format: <timestamp> <seq_num> 24202 ERROR Local-user-DB: Internal ID Store could not connect to the database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24202 ERROR Local-user-DB: Internal ID Store could not connect to the database, <log details>

- **Message Code:** 24203

  Severity: INFO

  Message Text: User need to change password

  Message Description: User was marked to change password in Internal database

  Local Target Message Format: <timestamp> <seq_num> 24203 INFO Local-user-DB: User need to change password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24203 INFO Local-user-DB: User need to change password, <log details>

- **Message Code:** 24204

  Severity: INFO

  Message Text: Password changed successfully

  Message Description: Password of user was changed successfully in Internal database

  Local Target Message Format: <timestamp> <seq_num> 24204 INFO Local-user-DB: Password changed successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24204 INFO Local-user-DB: Password changed successfully, <log details>

- **Message Code:** 24205

  Severity: ERROR

  Message Text: Could not change password to new password

  Message Description: Could not change password to new password in Internal database

  Local Target Message Format: <timestamp> <seq_num> 24205 ERROR Local-user-DB: Could not change password to new password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24205 ERROR Local-user-DB: Could not change password to new password, <log details>

- **Message Code:** 24206

  Severity: INFO

  Message Text: User disabled

  Message Description: User marked disabled in Internal database.

  Local Target Message Format: <timestamp> <seq_num> 24206 INFO Local-user-DB: User disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24206 INFO Local-user-DB: User disabled, <log details>

- **Message Code:** 24207

  Severity: INFO

  Message Text: Host disabled

  Message Description: Host marked disabled in Internal database.

  Local Target Message Format: <timestamp> <seq_num> 24207 INFO Local-user-DB: Host disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24207 INFO Local-user-DB: Host disabled, <log details>

- **Message Code:** 24208

  Severity: DEBUG

  Message Text: Looking up Admin in Internal Admins IDStore

  Message Description: Looking up Admin in Internal Admins IDStore

  Local Target Message Format: <timestamp> <seq_num> 24208 DEBUG Local-user-DB: Looking up Admin in Internal Admins IDStore, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24208 DEBUG Local-user-DB: Looking up Admin in Internal Admins IDStore, <log details>

- **Message Code:** 24209

  Severity: DEBUG

  Message Text: Looking up Endpoint in Internal Endpoints IDStore

  Message Description: Looking up Endpoint in Internal Endpoints IDStore

  Local Target Message Format: <timestamp> <seq_num> 24209 DEBUG Local-user-DB: Looking up Endpoint in Internal Endpoints IDStore, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24209 DEBUG Local-user-DB: Looking up Endpoint in Internal Endpoints IDStore, <log details>

- **Message Code:** 24210

  Severity: DEBUG

  Message Text: Looking up User in Internal Users IDStore

  Message Description: Looking up User in Internal Users IDStore

  Local Target Message Format: <timestamp> <seq_num> 24210 DEBUG Local-user-DB: Looking up User in Internal Users IDStore, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24210 DEBUG Local-user-DB: Looking up User in Internal Users IDStore, <log details>

- **Message Code:** 24211

  Severity: DEBUG

  Message Text: Found Endpoint in Internal Endpoints IDStore

  Message Description: Found Endpoint in Internal Endpoints IDStore

  Local Target Message Format: <timestamp> <seq_num> 24211 DEBUG Local-user-DB: Found Endpoint in Internal Endpoints IDStore, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24211 DEBUG Local-user-DB: Found Endpoint in Internal Endpoints IDStore, <log details>

- **Message Code:** 24212

  Severity: DEBUG

  Message Text: Found User in Internal Users IDStore

  Message Description: Found User in Internal Users IDStore

  Local Target Message Format: <timestamp> <seq_num> 24212 DEBUG Local-user-DB: Found User in Internal Users IDStore, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24212 DEBUG Local-user-DB: Found User in Internal Users IDStore, <log details>

- **Message Code:** 24213

  Severity: DEBUG

  Message Text: Found TrustSec Device in Network Devices and AAA Clients

  Message Description: Found TrustSec Device in Network Devices and AAA Clients

  Local Target Message Format: <timestamp> <seq_num> 24213 DEBUG Local-user-DB: Found TrustSec Device in Network Devices and AAA Clients, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24213 DEBUG Local-user-DB: Found TrustSec Device in Network Devices and AAA Clients, <log details>

- **Message Code:** 24214

  Severity: INFO

  Message Text: MSCHAP is used for the change password request in the internal users identity store

  Message Description: MSCHAP is used for the change password request in the internal users identity store.

  Local Target Message Format: <timestamp> <seq_num> 24214 INFO Local-user-DB: MSCHAP is used for the change password request in the internal users identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24214 INFO Local-user-DB: MSCHAP is used for the change password request in the internal users identity store, <log details>

- **Message Code:** 24215

  Severity: INFO

  Message Text: PAP is used for the change password request in the internal identity store

  Message Description: PAP is used for the change password request in the internal identity store.

  Local Target Message Format: <timestamp> <seq_num> 24215 INFO Local-user-DB: PAP is used for the change password request in the internal identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24215 INFO Local-user-DB: PAP is used for the change password request in the internal identity store, <log details>

- **Message Code:** 24216

  Severity: DEBUG

  Message Text: The user is not found in the internal users identity store

  Message Description: The specified user is not found in the internal users identity store.

  Local Target Message Format: <timestamp> <seq_num> 24216 DEBUG Local-user-DB: The user is not found in the internal users identity store, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24216 DEBUG Local-user-DB: The user is not found in the internal users identity store, <log details>

- **Message Code:** 24217

  Severity: DEBUG

  Message Text: The host is not found in the internal endpoints identity store

  Message Description: The specified host is not found in the internal endpoints identity store.

  Local Target Message Format: <timestamp> <seq_num> 24217 DEBUG Local-user-DB: The host is not found in the internal endpoints identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24217 DEBUG Local-user-DB: The host is not found in the internal endpoints identity store, <log details>

- **Message Code:** 24218

  Severity: DEBUG

  Message Text: The TrustSec device is not defined under Network Devices and AAA Clients in ISE

  Message Description: The specified TrustSec device is not defined under Network Devices and AAA Clients in ISE.

  Local Target Message Format: <timestamp> <seq_num> 24218 DEBUG Local-user-DB: The TrustSec device is not defined under Network Devices and AAA Clients in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24218 DEBUG Local-user-DB: The TrustSec device is not defined under Network Devices and AAA Clients in ISE, <log details>

- **Message Code:** 24219

  Severity: INFO

  Message Text: User account suspended

  Message Description: User account is suspended due to multiple failed authentication attempts

  Local Target Message Format: <timestamp> <seq_num> 24219 INFO Local-user-DB: User account suspended, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24219 INFO Local-user-DB: User account suspended, <log details>

- **Message Code:** 24300

  Severity: ERROR

  Message Text: No domain controller available

  Message Description: No domain controller available

  Local Target Message Format: <timestamp> <seq_num> 24300 ERROR External-Active-Directory: No domain controller available, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24300 ERROR External-Active-Directory: No domain controller available, <log details>

- **Message Code:** 24301

  Severity: ERROR

  Message Text: No writable domain controller available

  Message Description: No writable domain controller available

  Local Target Message Format: <timestamp> <seq_num> 24301 ERROR External-Active-Directory: No writable domain controller available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24301 ERROR External-Active-Directory: No writable domain controller available, <log details>

- **Message Code:** 24302

  Severity: ERROR

  Message Text: No global catalog available

  Message Description: No global catalog available

  Local Target Message Format: <timestamp> <seq_num> 24302 ERROR External-Active-Directory: No global catalog available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24302 ERROR External-Active-Directory: No global catalog available, <log details>

- **Message Code:** 24303

  Severity: WARN

  Message Text: Communication with domain controller failed

  Message Description: Communication with domain controller failed

  Local Target Message Format: <timestamp> <seq_num> 24303 WARN External-Active-Directory: Communication with domain controller failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24303 WARN External-Active-Directory: Communication with domain controller failed, <log details>

- **Message Code:** 24304

  Severity: WARN

  Message Text: Communication with global catalog failed

  Message Description: Communication with global catalog failed

  Local Target Message Format: <timestamp> <seq_num> 24304 WARN External-Active-Directory: Communication with global catalog failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24304 WARN External-Active-Directory: Communication with global catalog failed, <log details>

- **Message Code:** 24305

  Severity: ERROR

  Message Text: Failover threshold has been exceeded

  Message Description: Failover threshold has been exceeded

  Local Target Message Format: <timestamp> <seq_num> 24305 ERROR External-Active-Directory: Failover threshold has been exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24305 ERROR External-Active-Directory: Failover threshold has been exceeded, <log details>

- **Message Code:** 24306

  Severity: ERROR

  Message Text: No DNS server available

  Message Description: No DNS server available

  Local Target Message Format: <timestamp> <seq_num> 24306 ERROR External-Active-Directory: No DNS server available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24306 ERROR External-Active-Directory: No DNS server available, <log details>

- **Message Code:** 24307

  Severity: ERROR

  Message Text: DNS server returned error

  Message Description: DNS server returned error

  Local Target Message Format: <timestamp> <seq_num> 24307 ERROR External-Active-Directory: DNS server returned error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24307 ERROR External-Active-Directory: DNS server returned error, <log details>

- **Message Code:** 24308

  Severity: ERROR

  Message Text: None of required domains is joined

  Message Description: None of required domains is joined

  Local Target Message Format: <timestamp> <seq_num> 24308 ERROR External-Active-Directory: None of required domains is joined, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24308 ERROR External-Active-Directory: None of required domains is joined, <log details>

- **Message Code:** 24309

  Severity: DEBUG

  Message Text: Identity name with no domain markup has been rejected by join points

  Message Description: Identity name with no domain markup has been rejected according to AD Identity Store Advanced Settings

  Local Target Message Format: <timestamp> <seq_num> 24309 DEBUG External-Active-Directory: Identity name with no domain markup has been rejected by join points, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24309 DEBUG External-Active-Directory: Identity name with no domain markup has been rejected by join points, <log details>

- **Message Code:** 24310

  Severity: DEBUG

  Message Text: User Principal Name (UPN) format recognized

  Message Description: User Principal Name (UPN) format recognized

  Local Target Message Format: <timestamp> <seq_num> 24310 DEBUG External-Active-Directory: User Principal Name (UPN) format recognized, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24310 DEBUG External-Active-Directory: User Principal Name (UPN) format recognized, <log details>

- **Message Code:** 24311

  Severity: DEBUG

  Message Text: Down-Level Logon (NetBIOS) Name format recognized

  Message Description: Down-Level Logon (NetBIOS) Name format recognized

  Local Target Message Format: <timestamp> <seq_num> 24311 DEBUG External-Active-Directory: Down-Level Logon (NetBIOS) Name format recognized, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24311 DEBUG External-Active-Directory: Down-Level Logon (NetBIOS) Name format recognized, <log details>

- **Message Code:** 24312

  Severity: DEBUG

  Message Text: SAM Account Name format recognized

  Message Description: SAM Account Name format recognized

  Local Target Message Format: <timestamp> <seq_num> 24312 DEBUG External-Active-Directory: SAM Account Name format recognized, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24312 DEBUG External-Active-Directory: SAM Account Name format recognized, <log details>

- **Message Code:** 24313

  Severity: DEBUG

  Message Text: Search for matching accounts at join point

  Message Description: Search for matching accounts at join point

  Local Target Message Format: <timestamp> <seq_num> 24313 DEBUG External-Active-Directory: Search for matching accounts at join point, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24313 DEBUG External-Active-Directory: Search for matching accounts at join point, <log details>

- **Message Code:** 24314

  Severity: DEBUG

  Message Text: No matching account found in domain

  Message Description: No matching account found in domain

  Local Target Message Format: <timestamp> <seq_num> 24314 DEBUG External-Active-Directory: No matching account found in domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24314 DEBUG External-Active-Directory: No matching account found in domain, <log details>

- **Message Code:** 24315

  Severity: DEBUG

  Message Text: Single matching account found in domain

  Message Description: Single matching account found in domain

  Local Target Message Format: <timestamp> <seq_num> 24315 DEBUG External-Active-Directory: Single matching account found in domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24315 DEBUG External-Active-Directory: Single matching account found in domain, <log details>

- **Message Code:** 24316

  Severity: DEBUG

  Message Text: Multiple matching accounts found in domain

  Message Description: Multiple matching accounts found in domain

  Local Target Message Format: <timestamp> <seq_num> 24316 DEBUG External-Active-Directory: Multiple matching accounts found in domain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24316 DEBUG External-Active-Directory: Multiple matching accounts found in domain, <log details>

- **Message Code:** 24317

  Severity: ERROR

  Message Text: LDAP search in domain failed

  Message Description: LDAP search in domain failed

  Local Target Message Format: <timestamp> <seq_num> 24317 ERROR External-Active-Directory: LDAP search in domain failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24317 ERROR External-Active-Directory: LDAP search in domain failed, <log details>

- **Message Code:** 24318

  Severity: DEBUG

  Message Text: No matching account found in forest

  Message Description: No matching account found in forest

  Local Target Message Format: <timestamp> <seq_num> 24318 DEBUG External-Active-Directory: No matching account found in forest, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24318 DEBUG External-Active-Directory: No matching account found in forest, <log details>

- **Message Code:** 24319

  Severity: DEBUG

  Message Text: Single matching account found in forest

  Message Description: Single matching account found in forest

  Local Target Message Format: <timestamp> <seq_num> 24319 DEBUG External-Active-Directory: Single matching account found in forest, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24319 DEBUG External-Active-Directory: Single matching account found in forest, <log details>

- **Message Code:** 24320

  Severity: DEBUG

  Message Text: Multiple matching accounts in forest

  Message Description: Multiple matching accounts in forest

  Local Target Message Format: <timestamp> <seq_num> 24320 DEBUG External-Active-Directory: Multiple matching accounts in forest, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24320 DEBUG External-Active-Directory: Multiple matching accounts in forest, <log details>

- **Message Code:** 24321

  Severity: ERROR

  Message Text: LDAP search in forest failed

  Message Description: LDAP search in forest failed

  Local Target Message Format: <timestamp> <seq_num> 24321 ERROR External-Active-Directory: LDAP search in forest failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24321 ERROR External-Active-Directory: LDAP search in forest failed, <log details>

- **Message Code:** 24322

  Severity: DEBUG

  Message Text: Identity resolution detected no matching account

  Message Description: Identity resolution detected no matching account

  Local Target Message Format: <timestamp> <seq_num> 24322 DEBUG External-Active-Directory: Identity resolution detected no matching account, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24322 DEBUG External-Active-Directory: Identity resolution detected no matching account, <log details>

- **Message Code:** 24323

  Severity: DEBUG

  Message Text: Identity resolution detected single matching account

  Message Description: Identity resolution detected single matching account

  Local Target Message Format: <timestamp> <seq_num> 24323 DEBUG External-Active-Directory: Identity resolution detected single matching account, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24323 DEBUG External-Active-Directory: Identity resolution detected single matching account, <log details>

- **Message Code:** 24324

  Severity: DEBUG

  Message Text: Identity resolution detected multiple matching accounts

  Message Description: Identity resolution detected multiple matching accounts

  Local Target Message Format: <timestamp> <seq_num> 24324 DEBUG External-Active-Directory: Identity resolution detected multiple matching accounts, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24324 DEBUG External-Active-Directory: Identity resolution detected multiple matching accounts, <log details>

- **Message Code:** 24325

  Severity: DEBUG

  Message Text: Resolving identity

  Message Description: Resolving identity

  Local Target Message Format: <timestamp> <seq_num> 24325 DEBUG External-Active-Directory: Resolving identity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24325 DEBUG External-Active-Directory: Resolving identity, <log details>

- **Message Code:** 24326

  Severity: DEBUG

  Message Text: Searching subject object by UPN

  Message Description: Searching subject object by UPN

  Local Target Message Format: <timestamp> <seq_num> 24326 DEBUG External-Active-Directory: Searching subject object by UPN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24326 DEBUG External-Active-Directory: Searching subject object by UPN, <log details>

- **Message Code:** 24327

  Severity: DEBUG

  Message Text: Subject object found in a cache

  Message Description: Subject object found in a cache

  Local Target Message Format: <timestamp> <seq_num> 24327 DEBUG External-Active-Directory: Subject object found in a cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24327 DEBUG External-Active-Directory: Subject object found in a cache, <log details>

- **Message Code:** 24328

  Severity: DEBUG

  Message Text: Subject object not found in a cache

  Message Description: Subject object not found in a cache

  Local Target Message Format: <timestamp> <seq_num> 24328 DEBUG External-Active-Directory: Subject object not found in a cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24328 DEBUG External-Active-Directory: Subject object not found in a cache, <log details>

- **Message Code:** 24329

  Severity: DEBUG

  Message Text: Subject cache entry expired

  Message Description: Subject cache entry expired

  Local Target Message Format: <timestamp> <seq_num> 24329 DEBUG External-Active-Directory: Subject cache entry expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24329 DEBUG External-Active-Directory: Subject cache entry expired, <log details>

- **Message Code:** 24330

  Severity: DEBUG

  Message Text: Lookup SID By Name request succeeded

  Message Description: Lookup SID By Name request succeeded

  Local Target Message Format: <timestamp> <seq_num> 24330 DEBUG External-Active-Directory: Lookup SID By Name request succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24330 DEBUG External-Active-Directory: Lookup SID By Name request succeeded, <log details>

- **Message Code:** 24331

  Severity: DEBUG

  Message Text: Lookup SID By Name request failed

  Message Description: Lookup SID By Name request failed

  Local Target Message Format: <timestamp> <seq_num> 24331 DEBUG External-Active-Directory: Lookup SID By Name request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24331 DEBUG External-Active-Directory: Lookup SID By Name request failed, <log details>

- **Message Code:** 24332

  Severity: DEBUG

  Message Text: Lookup Object By SID request succeeded

  Message Description: Lookup Object By SID request succeeded

  Local Target Message Format: <timestamp> <seq_num> 24332 DEBUG External-Active-Directory: Lookup Object By SID request succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24332 DEBUG External-Active-Directory: Lookup Object By SID request succeeded, <log details>

- **Message Code:** 24333

  Severity: DEBUG

  Message Text: Lookup Object By SID request failed

  Message Description: Lookup Object By SID request failed

  Local Target Message Format: <timestamp> <seq_num> 24333 DEBUG External-Active-Directory: Lookup Object By SID request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24333 DEBUG External-Active-Directory: Lookup Object By SID request failed, <log details>

- **Message Code:** 24336

  Severity: DEBUG

  Message Text: Subject object cached

  Message Description: Subject object cached

  Local Target Message Format: <timestamp> <seq_num> 24336 DEBUG External-Active-Directory: Subject object cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24336 DEBUG External-Active-Directory: Subject object cached, <log details>

- **Message Code:** 24337

  Severity: DEBUG

  Message Text: Authentication Ticket (TGT) request succeeded

  Message Description: Authentication Ticket (TGT) request succeeded

  Local Target Message Format: <timestamp> <seq_num> 24337 DEBUG External-Active-Directory: Authentication Ticket (TGT) request succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24337 DEBUG External-Active-Directory: Authentication Ticket (TGT) request succeeded, <log details>

- **Message Code:** 24338

  Severity: DEBUG

  Message Text: Authentication Ticket (TGT) request failed

  Message Description: Authentication Ticket (TGT) request failed

  Local Target Message Format: <timestamp> <seq_num> 24338 DEBUG External-Active-Directory: Authentication Ticket (TGT) request failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24338 DEBUG External-Active-Directory: Authentication Ticket (TGT) request failed, <log details>

- **Message Code:** 24339

  Severity: DEBUG

  Message Text: Service Ticket request succeeded

  Message Description: Service Ticket request succeeded

  Local Target Message Format: <timestamp> <seq_num> 24339 DEBUG External-Active-Directory: Service Ticket request succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24339 DEBUG External-Active-Directory: Service Ticket request succeeded, <log details>

- **Message Code:** 24340

  Severity: DEBUG

  Message Text: Service Ticket request failed

  Message Description: Service Ticket request failed

  Local Target Message Format: <timestamp> <seq_num> 24340 DEBUG External-Active-Directory: Service Ticket request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24340 DEBUG External-Active-Directory: Service Ticket request failed, <log details>

- **Message Code:** 24341

  Severity: DEBUG

  Message Text: Service Ticket validation succeeded

  Message Description: Service Ticket validation succeeded

  Local Target Message Format: <timestamp> <seq_num> 24341 DEBUG External-Active-Directory: Service Ticket validation succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24341 DEBUG External-Active-Directory: Service Ticket validation succeeded, <log details>

- **Message Code:** 24342

  Severity: DEBUG

  Message Text: Service Ticket validation failed

  Message Description: Service Ticket validation failed

  Local Target Message Format: <timestamp> <seq_num> 24342 DEBUG External-Active-Directory: Service Ticket validation failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24342 DEBUG External-Active-Directory: Service Ticket validation failed, <log details>

- **Message Code:** 24343

  Severity: DEBUG

  Message Text: RPC Logon request succeeded

  Message Description: RPC Logon request succeeded

  Local Target Message Format: <timestamp> <seq_num> 24343 DEBUG External-Active-Directory: RPC Logon request succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24343 DEBUG External-Active-Directory: RPC Logon request succeeded, <log details>

- **Message Code:** 24344

  Severity: DEBUG

  Message Text: RPC Logon request failed

  Message Description: RPC Logon request failed

  Local Target Message Format: <timestamp> <seq_num> 24344 DEBUG External-Active-Directory: RPC Logon request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24344 DEBUG External-Active-Directory: RPC Logon request failed, <log details>

- **Message Code:** 24345

  Severity: DEBUG

  Message Text: RPC Change Password request succeeded

  Message Description: RPC Change Password request succeeded

  Local Target Message Format: <timestamp> <seq_num> 24345 DEBUG External-Active-Directory: RPC Change Password request succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24345 DEBUG External-Active-Directory: RPC Change Password request succeeded, <log details>

- **Message Code:** 24346

  Severity: DEBUG

  Message Text: RPC Change Password request failed

  Message Description: RPC Change Password request failed

  Local Target Message Format: <timestamp> <seq_num> 24346 DEBUG External-Active-Directory: RPC Change Password request failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24346 DEBUG External-Active-Directory: RPC Change Password request failed, <log details>

- **Message Code:** 24347

  Severity: ERROR

  Message Text: Account disabled

  Message Description: Account disabled

  Local Target Message Format: <timestamp> <seq_num> 24347 ERROR External-Active-Directory: Account disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24347 ERROR External-Active-Directory: Account disabled, <log details>

- **Message Code:** 24348

  Severity: ERROR

  Message Text: Account locked

  Message Description: Account locked

  Local Target Message Format: <timestamp> <seq_num> 24348 ERROR External-Active-Directory: Account locked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24348 ERROR External-Active-Directory: Account locked, <log details>

- **Message Code:** 24349

  Severity: ERROR

  Message Text: Account expired

  Message Description: Account expired

  Local Target Message Format: <timestamp> <seq_num> 24349 ERROR External-Active-Directory: Account expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24349 ERROR External-Active-Directory: Account expired, <log details>

- **Message Code:** 24350

  Severity: ERROR

  Message Text: Password expired

  Message Description: Password expired

  Local Target Message Format: <timestamp> <seq_num> 24350 ERROR External-Active-Directory: Password expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24350 ERROR External-Active-Directory: Password expired, <log details>

- **Message Code:** 24351

  Severity: DEBUG

  Message Text: Account validation succeeded

  Message Description: Account validation succeeded

  Local Target Message Format: <timestamp> <seq_num> 24351 DEBUG External-Active-Directory: Account validation succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24351 DEBUG External-Active-Directory: Account validation succeeded, <log details>

- **Message Code:** 24352

  Severity: DEBUG

  Message Text: Identity resolution failed

  Message Description: Identity resolution failed

  Local Target Message Format: <timestamp> <seq_num> 24352 DEBUG External-Active-Directory: Identity resolution failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24352 DEBUG External-Active-Directory: Identity resolution failed, <log details>

- **Message Code:** 24353

  Severity: DEBUG

  Message Text: Resolving identity

  Message Description: Resolving identity

  Local Target Message Format: <timestamp> <seq_num> 24353 DEBUG External-Active-Directory: Resolving identity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24353 DEBUG External-Active-Directory: Resolving identity, <log details>

- **Message Code:** 24354

  Severity: DEBUG

  Message Text: LDAP fetch found no matching account in domain

  Message Description: LDAP fetch found no matching account in domain

  Local Target Message Format: <timestamp> <seq_num> 24354 DEBUG External-Active-Directory: LDAP fetch found no matching account in domain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24354 DEBUG External-Active-Directory: LDAP fetch found no matching account in domain, <log details>

- **Message Code:** 24355

  Severity: DEBUG

  Message Text: LDAP fetch succeeded

  Message Description: LDAP fetch succeeded

  Local Target Message Format: <timestamp> <seq_num> 24355 DEBUG External-Active-Directory: LDAP fetch succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24355 DEBUG External-Active-Directory: LDAP fetch succeeded, <log details>

- **Message Code:** 24356

  Severity: ERROR

  Message Text: LDAP fetch failed

  Message Description: LDAP fetch failed

  Local Target Message Format: <timestamp> <seq_num> 24356 ERROR External-Active-Directory: LDAP fetch failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24356 ERROR External-Active-Directory: LDAP fetch failed, <log details>

- **Message Code:** 24357

  Severity: DEBUG

  Message Text: Incoming identity was rewritten

  Message Description: Incoming identity was rewritten

  Local Target Message Format: <timestamp> <seq_num> 24357 DEBUG External-Active-Directory: Incoming identity was rewritten, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24357 DEBUG External-Active-Directory: Incoming identity was rewritten, <log details>

- **Message Code:** 24358

  Severity: DEBUG

  Message Text: Match was not found for any existing identity rewrite rule

  Message Description: Match was not found for any existing identity rewrite rule

  Local Target Message Format: <timestamp> <seq_num> 24358 DEBUG External-Active-Directory: Match was not found for any existing identity rewrite rule, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24358 DEBUG External-Active-Directory: Match was not found for any existing identity rewrite rule, <log details>

- **Message Code:** 24359

  Severity: DEBUG

  Message Text: Incoming identity was not rewritten

  Message Description: Incoming identity was not rewritten

  Local Target Message Format: <timestamp> <seq_num> 24359 DEBUG External-Active-Directory: Incoming identity was not rewritten, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24359 DEBUG External-Active-Directory: Incoming identity was not rewritten, <log details>

- **Message Code:** 24360

  Severity: DEBUG

  Message Text: [Diagnostic step] : Identity was found, but filtered since it is not in authentication domsins

  Message Description: [Diagnostic step] : Identity was found, but filtered since it is not in authentication domains

  Local Target Message Format: <timestamp> <seq_num> 24360 DEBUG External-Active-Directory: [Diagnostic step] : Identity was found, but filtered since it is not in authentication domsins, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24360 DEBUG External-Active-Directory: [Diagnostic step] : Identity was found, but filtered since it is not in authentication domsins, <log details>

- **Message Code:** 24361

  Severity: INFO

  Message Text: Machine authentication is disabled for some of the configured join points

  Message Description: Machine authentication is disabled for some of the configured join points

  Local Target Message Format: <timestamp> <seq_num> 24361 INFO External-Active-Directory: Machine authentication is disabled for some of the configured join points, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24361 INFO External-Active-Directory: Machine authentication is disabled for some of the configured join points, <log details>

- **Message Code:** 24362

  Severity: DEBUG

  Message Text: Client certificate matches AD account certificate

  Message Description: Client certificate matches AD account certificate

Local Target Message Format: <timestamp> <seq_num> 24362 DEBUG Authentication: Client certificate matches AD account certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24362 DEBUG Authentication: Client certificate matches AD account certificate, <log details>

- **Message Code:** 24363

  Severity: DEBUG

  Message Text: Client certificate does not match AD account certificate

  Message Description: Client certificate does not match AD account certificate

  Local Target Message Format: <timestamp> <seq_num> 24363 DEBUG Authentication: Client certificate does not match AD account certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24363 DEBUG Authentication: Client certificate does not match AD account certificate, <log details>

- **Message Code:** 24364

  Severity: DEBUG

  Message Text: Resolve certificate identity ambiguity using certificates match

  Message Description: Resolve certificate identity ambiguity using certificates match

  Local Target Message Format: <timestamp> <seq_num> 24364 DEBUG Authentication: Resolve certificate identity ambiguity using certificates match, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24364 DEBUG Authentication: Resolve certificate identity ambiguity using certificates match, <log details>

- **Message Code:** 24365

  Severity: DEBUG

  Message Text: Resolve identity ambiguity using password verification

  Message Description: Resolve identity ambiguity using password verification

  Local Target Message Format: <timestamp> <seq_num> 24365 DEBUG Authentication: Resolve identity ambiguity using password verification, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24365 DEBUG Authentication: Resolve identity ambiguity using password verification, <log details>

- **Message Code:** 24366

  Severity: DEBUG

  Message Text: Skipping unjoined domain

  Message Description: Identity search in join point was skipped because ISE is not joined to the domain

Local Target Message Format: <timestamp> <seq_num> 24366 DEBUG External-Active-Directory: Skipping unjoined domain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24366 DEBUG External-Active-Directory: Skipping unjoined domain, <log details>

- **Message Code:** 24367

  Severity: INFO

  Message Text: Skipping unusable domain

  Message Description: Identity search in join point was skipped because the domain is unusable

  Local Target Message Format: <timestamp> <seq_num> 24367 INFO External-Active-Directory: Skipping unusable domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24367 INFO External-Active-Directory: Skipping unusable domain, <log details>

- **Message Code:** 24368

  Severity: INFO

  Message Text: Skipping unavailable domain

  Message Description: Identity search in join point was skipped because the domain is unavailable

  Local Target Message Format: <timestamp> <seq_num> 24368 INFO External-Active-Directory: Skipping unavailable domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24368 INFO External-Active-Directory: Skipping unavailable domain, <log details>

- **Message Code:** 24369

  Severity: INFO

  Message Text: Skipping unavailable forest

  Message Description: Identity search in join point was skipped because the forest is unavailable

  Local Target Message Format: <timestamp> <seq_num> 24369 INFO External-Active-Directory: Skipping unavailable forest, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24369 INFO External-Active-Directory: Skipping unavailable forest, <log details>

- **Message Code:** 24370

  Severity: ERROR

  Message Text: User credentials have been revoked.

  Message Description: User credentials have been revoked.

Local Target Message Format: <timestamp> <seq_num> 24370 ERROR External-Active-Directory: User credentials have been revoked., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24370 ERROR External-Active-Directory: User credentials have been revoked., <log details>

- **Message Code:** 24371

  Severity: ERROR

  Message Text: The ISE machine account does not have the required privileges to fetch groups.

  Message Description: The ISE machine account does not have the required privileges to fetch groups.

  Local Target Message Format: <timestamp> <seq_num> 24371 ERROR External-Active-Directory: The ISE machine account does not have the required privileges to fetch groups., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24371 ERROR External-Active-Directory: The ISE machine account does not have the required privileges to fetch groups., <log details>

- **Message Code:** 24400

  Severity: INFO

  Message Text: Connection to ISE Active Directory agent established successfully

  Message Description: Connection to ISE Active Directory agent established successfully

  Local Target Message Format: <timestamp> <seq_num> 24400 INFO External-Active-Directory: Connection to ISE Active Directory agent established successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24400 INFO External-Active-Directory: Connection to ISE Active Directory agent established successfully, <log details>

- **Message Code:** 24401

  Severity: ERROR

  Message Text: Could not establish connection with ISE Active Directory agent

  Message Description: Could not establish connection with ISE Active Directory agent

  Local Target Message Format: <timestamp> <seq_num> 24401 ERROR External-Active-Directory: Could not establish connection with ISE Active Directory agent, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24401 ERROR External-Active-Directory: Could not establish connection with ISE Active Directory agent, <log details>

- **Message Code:** 24402

  Severity: INFO

  Message Text: User authentication against Active Directory succeeded

  Message Description: User authentication against Active Directory succeeded

Local Target Message Format: <timestamp> <seq_num> 24402 INFO External-Active-Directory: User authentication against Active Directory succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24402 INFO External-Active-Directory: User authentication against Active Directory succeeded, <log details>

- **Message Code:** 24403

  Severity: ERROR

  Message Text: User authentication against Active Directory failed

  Message Description: User authentication against Active Directory failed

  Local Target Message Format: <timestamp> <seq_num> 24403 ERROR External-Active-Directory: User authentication against Active Directory failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24403 ERROR External-Active-Directory: User authentication against Active Directory failed, <log details>

- **Message Code:** 24404

  Severity: DEBUG

  Message Text: Active Directory operation failed because of an invalid input parameter

  Message Description: Active Directory operation failed because of an invalid input parameter

  Local Target Message Format: <timestamp> <seq_num> 24404 DEBUG External-Active-Directory: Active Directory operation failed because of an invalid input parameter, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24404 DEBUG External-Active-Directory: Active Directory operation failed because of an invalid input parameter, <log details>

- **Message Code:** 24405

  Severity: ERROR

  Message Text: Active Directory operation failed because of a timeout error

  Message Description: Active Directory operation failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24405 ERROR External-Active-Directory: Active Directory operation failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24405 ERROR External-Active-Directory: Active Directory operation failed because of a timeout error, <log details>

- **Message Code:** 24406

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since user has invalid credentials

  Message Description: User authentication against Active Directory failed since user has invalid credentials

Local Target Message Format: <timestamp> <seq_num> 24406 DEBUG External-Active-Directory: User authentication against Active Directory failed since user has invalid credentials, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24406 DEBUG External-Active-Directory: User authentication against Active Directory failed since user has invalid credentials, <log details>

- **Message Code:** 24407

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since user is required to change his password

  Message Description: User authentication against Active Directory failed since user is required to change his password

  Local Target Message Format: <timestamp> <seq_num> 24407 DEBUG External-Active-Directory: User authentication against Active Directory failed since user is required to change his password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24407 DEBUG External-Active-Directory: User authentication against Active Directory failed since user is required to change his password, <log details>

- **Message Code:** 24408

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since user has entered the wrong password

  Message Description: User authentication against Active Directory failed since user has entered the wrong password

  Local Target Message Format: <timestamp> <seq_num> 24408 DEBUG External-Active-Directory: User authentication against Active Directory failed since user has entered the wrong password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24408 DEBUG External-Active-Directory: User authentication against Active Directory failed since user has entered the wrong password, <log details>

- **Message Code:** 24409

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since the user's account is disabled

  Message Description: User authentication against Active Directory failed since the user's account is disabled

  Local Target Message Format: <timestamp> <seq_num> 24409 DEBUG External-Active-Directory: User authentication against Active Directory failed since the user's account is disabled, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24409 DEBUG External-Active-Directory: User authentication against Active Directory failed since the user's account is disabled, <log details>

- **Message Code:** 24410

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since user is considered to be in restricted logon hours

  Message Description: User authentication against Active Directory failed since user is considered to be in restricted logon hours

  Local Target Message Format: <timestamp> <seq_num> 24410 DEBUG External-Active-Directory: User authentication against Active Directory failed since user is considered to be in restricted logon hours, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24410 DEBUG External-Active-Directory: User authentication against Active Directory failed since user is considered to be in restricted logon hours, <log details>

- **Message Code:** 24411

  Severity: DEBUG

  Message Text: Change password against Active Directory failed since user has a non-compliant password

  Message Description: Change password against Active Directory failed since user has a non-compliant password

  Local Target Message Format: <timestamp> <seq_num> 24411 DEBUG External-Active-Directory: Change password against Active Directory failed since user has a non-compliant password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24411 DEBUG External-Active-Directory: Change password against Active Directory failed since user has a non-compliant password, <log details>

- **Message Code:** 24412

  Severity: DEBUG

  Message Text: User not found in Active Directory

  Message Description: User not found in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24412 DEBUG External-Active-Directory: User not found in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24412 DEBUG External-Active-Directory: User not found in Active Directory, <log details>

- **Message Code:** 24413

  Severity: DEBUG

Message Text: User's domain is not recognized by Active Directory

Message Description: User's domain is not recognized by Active Directory

Local Target Message Format: <timestamp> <seq_num> 24413 DEBUG External-Active-Directory: User's domain is not recognized by Active Directory, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24413 DEBUG External-Active-Directory: User's domain is not recognized by Active Directory, <log details>

- **Message Code:** 24414

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since the user's account has expired

  Message Description: User authentication against Active Directory failed since the user's account has expired

  Local Target Message Format: <timestamp> <seq_num> 24414 DEBUG External-Active-Directory: User authentication against Active Directory failed since the user's account has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24414 DEBUG External-Active-Directory: User authentication against Active Directory failed since the user's account has expired, <log details>

- **Message Code:** 24415

  Severity: DEBUG

  Message Text: User authentication against Active Directory failed since user's account is locked out

  Message Description: User authentication against Active Directory failed since user's account is locked out

  Local Target Message Format: <timestamp> <seq_num> 24415 DEBUG External-Active-Directory: User authentication against Active Directory failed since user's account is locked out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24415 DEBUG External-Active-Directory: User authentication against Active Directory failed since user's account is locked out, <log details>

- **Message Code:** 24416

  Severity: INFO

  Message Text: User's Groups retrieval from Active Directory succeeded

  Message Description: User's Groups retrieval from Active Directory succeeded

  Local Target Message Format: <timestamp> <seq_num> 24416 INFO External-Active-Directory: User's Groups retrieval from Active Directory succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24416 INFO External-Active-Directory: User's Groups retrieval from Active Directory succeeded, <log details>

- **Message Code:** 24417

  Severity: ERROR

  Message Text: User's Groups retrieval from Active Directory failed

  Message Description: User's Groups retrieval from Active Directory failed

  Local Target Message Format: <timestamp> <seq_num> 24417 ERROR External-Active-Directory: User's Groups retrieval from Active Directory failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24417 ERROR External-Active-Directory: User's Groups retrieval from Active Directory failed, <log details>

- **Message Code:** 24418

  Severity: ERROR

  Message Text: Machine authentication against Active Directory failed since it is disabled in configuration

  Message Description: Machine authentication against Active Directory failed since it is disabled in configuration

  Local Target Message Format: <timestamp> <seq_num> 24418 ERROR External-Active-Directory: Machine authentication against Active Directory failed since it is disabled in configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24418 ERROR External-Active-Directory: Machine authentication against Active Directory failed since it is disabled in configuration, <log details>

- **Message Code:** 24419

  Severity: ERROR

  Message Text: User's Attributes retrieval from Active Directory failed

  Message Description: User's Attributes retrieval from Active Directory failed

  Local Target Message Format: <timestamp> <seq_num> 24419 ERROR External-Active-Directory: User's Attributes retrieval from Active Directory failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24419 ERROR External-Active-Directory: User's Attributes retrieval from Active Directory failed, <log details>

- **Message Code:** 24420

  Severity: INFO

  Message Text: User's Attributes retrieval from Active Directory succeeded

  Message Description: User's Attributes retrieval from Active Directory succeeded

  Local Target Message Format: <timestamp> <seq_num> 24420 INFO External-Active-Directory: User's Attributes retrieval from Active Directory succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24420 INFO External-Active-Directory: User's Attributes retrieval from Active Directory succeeded, <log details>

- **Message Code:** 24421

  Severity: DEBUG

  Message Text: Change password against Active Directory failed since it is disabled in configuration

  Message Description: Change password against Active Directory failed since it is disabled in configuration

  Local Target Message Format: <timestamp> <seq_num> 24421 DEBUG External-Active-Directory: Change password against Active Directory failed since it is disabled in configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24421 DEBUG External-Active-Directory: Change password against Active Directory failed since it is disabled in configuration, <log details>

- **Message Code:** 24422

  Severity: INFO

  Message Text: ISE has confirmed previous successful machine authentication for user in Active Directory

  Message Description: ISE has confirmed previous successful machine authentication for user in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24422 INFO External-Active-Directory: ISE has confirmed previous successful machine authentication for user in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24422 INFO External-Active-Directory: ISE has confirmed previous successful machine authentication for user in Active Directory, <log details>

- **Message Code:** 24423

  Severity: DEBUG

  Message Text: ISE has not been able to confirm previous successful machine authentication

  Message Description: ISE has not been able to confirm previous successful machine authentication

  Local Target Message Format: <timestamp> <seq_num> 24423 DEBUG External-Active-Directory: ISE has not been able to confirm previous successful machine authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24423 DEBUG External-Active-Directory: ISE has not been able to confirm previous successful machine authentication, <log details>

- **Message Code:** 24424

  Severity: DEBUG

  Message Text: Noncompliant attributes detected in Active Directory

  Message Description: Noncompliant attributes detected in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24424 DEBUG External-Active-Directory: Noncompliant attributes detected in Active Directory, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24424 DEBUG External-Active-Directory: Noncompliant attributes detected in Active Directory, <log details>

- **Message Code:** 24425

  Severity: INFO

  Message Text: User change password against Active Directory succeeded

  Message Description: User change password against Active Directory succeeded

  Local Target Message Format: <timestamp> <seq_num> 24425 INFO External-Active-Directory: User change password against Active Directory succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24425 INFO External-Active-Directory: User change password against Active Directory succeeded, <log details>

- **Message Code:** 24426

  Severity: ERROR

  Message Text: User change password against Active Directory failed

  Message Description: User change password against Active Directory failed

  Local Target Message Format: <timestamp> <seq_num> 24426 ERROR External-Active-Directory: User change password against Active Directory failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24426 ERROR External-Active-Directory: User change password against Active Directory failed, <log details>

- **Message Code:** 24427

  Severity: ERROR

  Message Text: Access to Active Directory failed

  Message Description: Access to Active Directory failed

  Local Target Message Format: <timestamp> <seq_num> 24427 ERROR External-Active-Directory: Access to Active Directory failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24427 ERROR External-Active-Directory: Access to Active Directory failed, <log details>

- **Message Code:** 24428

  Severity: ERROR

  Message Text: Connection related error has occurred in either LRPC, LDAP or KERBEROS

  Message Description: This RPC connection problem may be because the stub received incorrect data

  Local Target Message Format: <timestamp> <seq_num> 24428 ERROR External-Active-Directory: Connection related error has occurred in either LRPC, LDAP or KERBEROS, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24428 ERROR External-Active-Directory: Connection related error has occurred in either LRPC, LDAP or KERBEROS, <log details>

- **Message Code:** 24429

  Severity: ERROR

  Message Text: Could not establish connection with Active Directory

  Message Description: Could not establish connection with Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24429 ERROR External-Active-Directory: Could not establish connection with Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24429 ERROR External-Active-Directory: Could not establish connection with Active Directory, <log details>

- **Message Code:** 24430

  Severity: DEBUG

  Message Text: Authenticating user against Active Directory

  Message Description: Authenticating user against Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24430 DEBUG External-Active-Directory: Authenticating user against Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24430 DEBUG External-Active-Directory: Authenticating user against Active Directory, <log details>

- **Message Code:** 24431

  Severity: DEBUG

  Message Text: Authenticating machine against Active Directory

  Message Description: Authenticating machine against Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24431 DEBUG External-Active-Directory: Authenticating machine against Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24431 DEBUG External-Active-Directory: Authenticating machine against Active Directory, <log details>

- **Message Code:** 24432

  Severity: DEBUG

  Message Text: Looking up user in Active Directory

  Message Description: Looking up user in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24432 DEBUG External-Active-Directory: Looking up user in Active Directory, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24432 DEBUG External-Active-Directory: Looking up user in Active Directory, <log details>

- **Message Code:** 24433

  Severity: DEBUG

  Message Text: Looking up machine in Active Directory

  Message Description: Looking up machine in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24433 DEBUG External-Active-Directory: Looking up machine in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24433 DEBUG External-Active-Directory: Looking up machine in Active Directory, <log details>

- **Message Code:** 24434

  Severity: DEBUG

  Message Text: Performing Change Password in Active Directory

  Message Description: Performing Change Password in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24434 DEBUG External-Active-Directory: Performing Change Password in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24434 DEBUG External-Active-Directory: Performing Change Password in Active Directory, <log details>

- **Message Code:** 24435

  Severity: INFO

  Message Text: Machine Groups retrieval from Active Directory succeeded

  Message Description: Machine Groups retrieval from Active Directory succeeded

  Local Target Message Format: <timestamp> <seq_num> 24435 INFO External-Active-Directory: Machine Groups retrieval from Active Directory succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24435 INFO External-Active-Directory: Machine Groups retrieval from Active Directory succeeded, <log details>

- **Message Code:** 24436

  Severity: ERROR

  Message Text: Machine Lookup in Active Directory failed

  Message Description: Machine Lookup in Active Directory failed

  Local Target Message Format: <timestamp> <seq_num> 24436 ERROR External-Active-Directory: Machine Lookup in Active Directory failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24436 ERROR External-Active-Directory: Machine Lookup in Active Directory failed, <log details>

- **Message Code:** 24437

  Severity: DEBUG

  Message Text: Machine not found in Active Directory

  Message Description: Machine not found in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24437 DEBUG External-Active-Directory: Machine not found in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24437 DEBUG External-Active-Directory: Machine not found in Active Directory, <log details>

- **Message Code:** 24438

  Severity: ERROR

  Message Text: Found multiple occurrences of the machine in Active Directory

  Message Description: Found multiple occurrences of the machine in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24438 ERROR External-Active-Directory: Found multiple occurrences of the machine in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24438 ERROR External-Active-Directory: Found multiple occurrences of the machine in Active Directory, <log details>

- **Message Code:** 24439

  Severity: INFO

  Message Text: Machine Attributes retrieval from Active Directory succeeded

  Message Description: Machine Attributes retrieval from Active Directory succeeded

  Local Target Message Format: <timestamp> <seq_num> 24439 INFO External-Active-Directory: Machine Attributes retrieval from Active Directory succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24439 INFO External-Active-Directory: Machine Attributes retrieval from Active Directory succeeded, <log details>

- **Message Code:** 24440

  Severity: ERROR

  Message Text: Machine primary group name does not exist in Active Directory

  Message Description: Machine primary group name does not exist in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24440 ERROR External-Active-Directory: Machine primary group name does not exist in Active Directory, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24440 ERROR External-Active-Directory: Machine primary group name does not exist in Active Directory, <log details>

- **Message Code:** 24441

  Severity: ERROR

  Message Text: ISE machine account is not permitted to log on

  Message Description: ISE machine account is not permitted to log on

  Local Target Message Format: <timestamp> <seq_num> 24441 ERROR External-Active-Directory: ISE machine account is not permitted to log on, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24441 ERROR External-Active-Directory: ISE machine account is not permitted to log on, <log details>

- **Message Code:** 24442

  Severity: ERROR

  Message Text: User-related object retrieval operation from Active Directory has failed

  Message Description: User-related object retrieval operation from Active Directory has failed

  Local Target Message Format: <timestamp> <seq_num> 24442 ERROR External-Active-Directory: User-related object retrieval operation from Active Directory has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24442 ERROR External-Active-Directory: User-related object retrieval operation from Active Directory has failed, <log details>

- **Message Code:** 24443

  Severity: INFO

  Message Text: User's Groups retrieval from Active Directory succeeded partially

  Message Description: Only a partial retrieval of user's groups has occurred. This is because either Lookup by Group SID has failed or that canonical name attribute was not found.

  Local Target Message Format: <timestamp> <seq_num> 24443 INFO External-Active-Directory: User's Groups retrieval from Active Directory succeeded partially, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24443 INFO External-Active-Directory: User's Groups retrieval from Active Directory succeeded partially, <log details>

- **Message Code:** 24444

  Severity: ERROR

  Message Text: Active Directory operation has failed because of an unspecified error in the ISE

  Message Description: Active Directory operation has failed because of an unspecified error in the ISE

Local Target Message Format: <timestamp> <seq_num> 24444 ERROR External-Active-Directory: Active Directory operation has failed because of an unspecified error in the ISE, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24444 ERROR External-Active-Directory: Active Directory operation has failed because of an unspecified error in the ISE, <log details>

- **Message Code:** 24445

  Severity: INFO

  Message Text: Machine Groups retrieval from Active Directory succeeded partially

  Message Description: Partial retrieval of machine groups because Canonical Name attribute was not found

  Local Target Message Format: <timestamp> <seq_num> 24445 INFO External-Active-Directory: Machine Groups retrieval from Active Directory succeeded partially, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24445 INFO External-Active-Directory: Machine Groups retrieval from Active Directory succeeded partially, <log details>

- **Message Code:** 24446

  Severity: ERROR

  Message Text: Active Directory domain controller is unreachable

  Message Description: Active Directory domain controller is unreachable

  Local Target Message Format: <timestamp> <seq_num> 24446 ERROR External-Active-Directory: Active Directory domain controller is unreachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24446 ERROR External-Active-Directory: Active Directory domain controller is unreachable, <log details>

- **Message Code:** 24447

  Severity: ERROR

  Message Text: ISE appliance machine account in Active Directory is disabled, deleted or reset

  Message Description: ISE appliance machine in Active Directory is disabled, deleted or reset.

  Local Target Message Format: <timestamp> <seq_num> 24447 ERROR External-Active-Directory: ISE appliance machine account in Active Directory is disabled, deleted or reset, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24447 ERROR External-Active-Directory: ISE appliance machine account in Active Directory is disabled, deleted or reset, <log details>

- **Message Code:** 24448

  Severity: ERROR

Message Text: User object retrieval from Active Directory failed because of a timeout error

Message Description: User object retrieval from Active Directory failed because of a timeout error

Local Target Message Format: <timestamp> <seq_num> 24448 ERROR External-Active-Directory: User object retrieval from Active Directory failed because of a timeout error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24448 ERROR External-Active-Directory: User object retrieval from Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24449

  Severity: ERROR

  Message Text: User's Groups retrieval from Active Directory failed because of a timeout error

  Message Description: User's Groups retrieval from Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24449 ERROR External-Active-Directory: User's Groups retrieval from Active Directory failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24449 ERROR External-Active-Directory: User's Groups retrieval from Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24450

  Severity: ERROR

  Message Text: User's Attributes retrieval from Active Directory failed because of a timeout error

  Message Description: User's Attributes retrieval from Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24450 ERROR External-Active-Directory: User's Attributes retrieval from Active Directory failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24450 ERROR External-Active-Directory: User's Attributes retrieval from Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24451

  Severity: ERROR

  Message Text: Machine object retrieval from Active Directory failed because of a timeout error

  Message Description: Machine object retrieval from Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24451 ERROR External-Active-Directory: Machine object retrieval from Active Directory failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24451 ERROR External-Active-Directory: Machine object retrieval from Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24452

  Severity: ERROR

  Message Text: Machine primary group retrieval from Active Directory failed because of a timeout error

  Message Description: Machine primary group retrieval from Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24452 ERROR External-Active-Directory: Machine primary group retrieval from Active Directory failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24452 ERROR External-Active-Directory: Machine primary group retrieval from Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24453

  Severity: ERROR

  Message Text: Machine Attributes retrieval from Active Directory failed because of a timeout error

  Message Description: Machine Attributes retrieval from Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24453 ERROR External-Active-Directory: Machine Attributes retrieval from Active Directory failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24453 ERROR External-Active-Directory: Machine Attributes retrieval from Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24454

  Severity: ERROR

  Message Text: User authentication against Active Directory failed because of a timeout error

  Message Description: User authentication against Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24454 ERROR External-Active-Directory: User authentication against Active Directory failed because of a timeout error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24454 ERROR External-Active-Directory: User authentication against Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24455

  Severity: ERROR

  Message Text: Change password against Active Directory failed because of a timeout error

  Message Description: Change password against Active Directory failed because of a timeout error

  Local Target Message Format: <timestamp> <seq_num> 24455 ERROR External-Active-Directory: Change password against Active Directory failed because of a timeout error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24455 ERROR External-Active-Directory: Change password against Active Directory failed because of a timeout error, <log details>

- **Message Code:** 24456

  Severity: WARN

  Message Text: Not all user Active Directory groups are retrieved successfully. One of the groups was not retrieved by its SID

  Message Description: Not all user Active Directory groups are retrieved successfully. One of the groups was not retrieved by its SID

  Local Target Message Format: <timestamp> <seq_num> 24456 WARN External-Active-Directory: Not all user Active Directory groups are retrieved successfully. One of the groups was not retrieved by its SID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24456 WARN External-Active-Directory: Not all user Active Directory groups are retrieved successfully. One of the groups was not retrieved by its SID, <log details>

- **Message Code:** 24457

  Severity: WARN

  Message Text: Not all user Active Directory groups are retrieved successfully. One or more of the group's canonical name was not retrieved

  Message Description: Not all user Active Directory groups are retrieved successfully. One or more of the group's canonical name was not retrieved

  Local Target Message Format: <timestamp> <seq_num> 24457 WARN External-Active-Directory: Not all user Active Directory groups are retrieved successfully. One or more of the group's canonical name was not retrieved, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24457 WARN External-Active-Directory: Not all user Active Directory groups are retrieved successfully. One or more of the group's canonical name was not retrieved, <log details>

- **Message Code:** 24458

  Severity: WARN

  Message Text: Not all Active Directory attributes are retrieved successfully

  Message Description: Not all Active Directory attributes are retrieved successfully

  Local Target Message Format: <timestamp> <seq_num> 24458 WARN External-Active-Directory: Not all Active Directory attributes are retrieved successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24458 WARN External-Active-Directory: Not all Active Directory attributes are retrieved successfully, <log details>

- **Message Code:** 24459

Severity: WARN

Message Text: Host memberOf groups do not exist or cannot be retrieved

Message Description: Host memberOf groups do not exist or cannot be retrieved

Local Target Message Format: <timestamp> <seq_num> 24459 WARN External-Active-Directory: Host memberOf groups do not exist or cannot be retrieved, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24459 WARN External-Active-Directory: Host memberOf groups do not exist or cannot be retrieved, <log details>

- **Message Code:** 24460

  Severity: ERROR

  Message Text: There are multiple occurrences of the user name in the Active directory

  Message Description: There are multiple occurrences of the user name in the Active directory

  Local Target Message Format: <timestamp> <seq_num> 24460 ERROR External-Active-Directory: There are multiple occurrences of the user name in the Active directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24460 ERROR External-Active-Directory: There are multiple occurrences of the user name in the Active directory, <log details>

- **Message Code:** 24461

  Severity: ERROR

  Message Text: Could not locate the user in the Active directory using User Lookup

  Message Description: Could not locate the user in the Active directory using User Lookup

  Local Target Message Format: <timestamp> <seq_num> 24461 ERROR External-Active-Directory: Could not locate the user in the Active directory using User Lookup, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24461 ERROR External-Active-Directory: Could not locate the user in the Active directory using User Lookup, <log details>

- **Message Code:** 24462

  Severity: ERROR

  Message Text: The ISE Active Directory module does not have sufficient memory

  Message Description: The ISE Active Directory module does not have sufficient memory

  Local Target Message Format: <timestamp> <seq_num> 24462 ERROR External-Active-Directory: The ISE Active Directory module does not have sufficient memory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24462 ERROR External-Active-Directory: The ISE Active Directory module does not have sufficient memory, <log details>

- **Message Code:** 24463

  Severity: ERROR

  Message Text: Internal error in the ISE Active Directory

  Message Description: A function related to the Active Directory may have received an illegal parameter, option, or session handler. Alternatively, this directory may be missing a parameter, option, or session handler.

  Local Target Message Format: <timestamp> <seq_num> 24463 ERROR External-Active-Directory: Internal error in the ISE Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24463 ERROR External-Active-Directory: Internal error in the ISE Active Directory, <log details>

- **Message Code:** 24464

  Severity: ERROR

  Message Text: The Active Directory does not have the required privileges

  Message Description: The Active Directory does not have the required privileges to perform the specified task.

  Local Target Message Format: <timestamp> <seq_num> 24464 ERROR External-Active-Directory: The Active Directory does not have the required privileges, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24464 ERROR External-Active-Directory: The Active Directory does not have the required privileges, <log details>

- **Message Code:** 24465

  Severity: ERROR

  Message Text: ISE is not joined to an Active Directory Domain Controller

  Message Description: ISE is not joined to an Active Directory Domain Controller

  Local Target Message Format: <timestamp> <seq_num> 24465 ERROR External-Active-Directory: ISE is not joined to an Active Directory Domain Controller, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24465 ERROR External-Active-Directory: ISE is not joined to an Active Directory Domain Controller, <log details>

- **Message Code:** 24466

  Severity: ERROR

  Message Text: ISE Active Directory agent is down

  Message Description: ISE Active Directory agent is down

  Local Target Message Format: <timestamp> <seq_num> 24466 ERROR External-Active-Directory: ISE Active Directory agent is down, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24466 ERROR External-Active-Directory: ISE Active Directory agent is down, <log details>

- **Message Code:** 24467

  Severity: ERROR

  Message Text: Could not retrieve the specified object

  Message Description: Could not retrieve the specified object because it belongs to an inaccessible domain

  Local Target Message Format: <timestamp> <seq_num> 24467 ERROR External-Active-Directory: Could not retrieve the specified object, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24467 ERROR External-Active-Directory: Could not retrieve the specified object, <log details>

- **Message Code:** 24468

  Severity: ERROR

  Message Text: Failed to retrieve the user certificate from Active Directory

  Message Description: Failed to retrieve the user certificate from Active Directory.

  Local Target Message Format: <timestamp> <seq_num> 24468 ERROR External-Active-Directory: Failed to retrieve the user certificate from Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24468 ERROR External-Active-Directory: Failed to retrieve the user certificate from Active Directory, <log details>

- **Message Code:** 24469

  Severity: INFO

  Message Text: The user certificate was retrieved from Active Directory successfully

  Message Description: The user certificate was retrieved from Active Directory successfully.

  Local Target Message Format: <timestamp> <seq_num> 24469 INFO External-Active-Directory: The user certificate was retrieved from Active Directory successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24469 INFO External-Active-Directory: The user certificate was retrieved from Active Directory successfully, <log details>

- **Message Code:** 24470

  Severity: INFO

  Message Text: Machine authentication against Active Directory is successful

  Message Description: Machine authentication against Active Directory is successful.

  Local Target Message Format: <timestamp> <seq_num> 24470 INFO External-Active-Directory: Machine authentication against Active Directory is successful, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24470 INFO External-Active-Directory: Machine authentication against Active Directory is successful, <log details>

- **Message Code:** 24471

  Severity: INFO

  Message Text: Active Directory does not support the change EnablePassword option

  Message Description: Active Directory does not support the change EnablePassword option.

  Local Target Message Format: <timestamp> <seq_num> 24471 INFO External-Active-Directory: Active Directory does not support the change EnablePassword option, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24471 INFO External-Active-Directory: Active Directory does not support the change EnablePassword option, <log details>

- **Message Code:** 24472

  Severity: DEBUG

  Message Text: The user or host account is locked out; setting the IdentityAccessRestricted flag to true

  Message Description: The user or host account is locked out; ISE sets the IdentityAccessRestricted flag to true.

  Local Target Message Format: <timestamp> <seq_num> 24472 DEBUG External-Active-Directory: The user or host account is locked out; setting the IdentityAccessRestricted flag to true, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24472 DEBUG External-Active-Directory: The user or host account is locked out; setting the IdentityAccessRestricted flag to true, <log details>

- **Message Code:** 24473

  Severity: DEBUG

  Message Text: The user's password has expired; setting the IdentityAccessRestricted flag to true

  Message Description: The user's password has expired; ISE sets the IdentityAccessRestricted flag to true.

  Local Target Message Format: <timestamp> <seq_num> 24473 DEBUG External-Active-Directory: The user's password has expired; setting the IdentityAccessRestricted flag to true, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24473 DEBUG External-Active-Directory: The user's password has expired; setting the IdentityAccessRestricted flag to true, <log details>

- **Message Code:** 24474

  Severity: DEBUG

  Message Text: The user's or host's account has expired; setting the IdentityAccessRestricted flag to true

Message Description: The user's or host's account has expired; ISE sets the IdentityAccessRestricted flag to true.

Local Target Message Format: <timestamp> <seq_num> 24474 DEBUG External-Active-Directory: The user's or host's account has expired; setting the IdentityAccessRestricted flag to true, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24474 DEBUG External-Active-Directory: The user's or host's account has expired; setting the IdentityAccessRestricted flag to true, <log details>

- **Message Code:** 24475

  Severity: DEBUG

  Message Text: The user's or host's account is disabled; setting the IdentityAccessRestricted flag to true

  Message Description: The user's or host's account is disabled; ISE sets the IdentityAccessRestricted flag to true.

  Local Target Message Format: <timestamp> <seq_num> 24475 DEBUG External-Active-Directory: The user's or host's account is disabled; setting the IdentityAccessRestricted flag to true, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24475 DEBUG External-Active-Directory: The user's or host's account is disabled; setting the IdentityAccessRestricted flag to true, <log details>

- **Message Code:** 24476

  Severity: DEBUG

  Message Text: The user's or host's account is in restricted logon hours; setting the IdentityAccessRestricted flag to true. true

  Message Description: The user's or host's account is in restricted logon hours; ISE sets the IdentityAccessRestricted flag to true.

  Local Target Message Format: <timestamp> <seq_num> 24476 DEBUG External-Active-Directory: The user's or host's account is in restricted logon hours; setting the IdentityAccessRestricted flag to true. true, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24476 DEBUG External-Active-Directory: The user's or host's account is in restricted logon hours; setting the IdentityAccessRestricted flag to true. true, <log details>

- **Message Code:** 24477

  Severity: DEBUG

  Message Text: The user is not permitted to log in to Active Directory using the current workstation; setting the IdentityAccessRestricted flag to true

  Message Description: The user is not permitted to log in to Active Directory using the current workstation; setting the IdentityAccessRestricted flag to true.

Local Target Message Format: <timestamp> <seq_num> 24477 DEBUG External-Active-Directory: The user is not permitted to log in to Active Directory using the current workstation; setting the IdentityAccessRestricted flag to true, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24477 DEBUG External-Active-Directory: The user is not permitted to log in to Active Directory using the current workstation; setting the IdentityAccessRestricted flag to true, <log details>

- **Message Code:** 24478

  Severity: WARN

  Message Text: Error while validating the user or host in Active Directory; the IdentityAccessRestricted flag is not altered

  Message Description: If there is an error while validating the user or host in Active Directory, ISE does not alter the IdentityAccessRestricted flag.

  Local Target Message Format: <timestamp> <seq_num> 24478 WARN External-Active-Directory: Error while validating the user or host in Active Directory; the IdentityAccessRestricted flag is not altered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24478 WARN External-Active-Directory: Error while validating the user or host in Active Directory; the IdentityAccessRestricted flag is not altered, <log details>

- **Message Code:** 24479

  Severity: WARN

  Message Text: Not all machines in the Active Directory groups are retrieved; one or more of the group's canonical name is not retrieved

  Message Description: Not all machines in the Active Directory groups are retrieved; one or more of the group's canonical name is not retrieved.

  Local Target Message Format: <timestamp> <seq_num> 24479 WARN External-Active-Directory: Not all machines in the Active Directory groups are retrieved; one or more of the group's canonical name is not retrieved, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24479 WARN External-Active-Directory: Not all machines in the Active Directory groups are retrieved; one or more of the group's canonical name is not retrieved, <log details>

- **Message Code:** 24480

  Severity: ERROR

  Message Text: The machine-related object retrieval operation from Active Directory has failed

  Message Description: The machine-related object retrieval operation from Active Directory has failed.

  Local Target Message Format: <timestamp> <seq_num> 24480 ERROR External-Active-Directory: The machine-related object retrieval operation from Active Directory has failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24480 ERROR External-Active-Directory: The machine-related object retrieval operation from Active Directory has failed, <log details>

- **Message Code:** 24481

  Severity: ERROR

  Message Text: The machine's attribute retrieval from Active Directory has failed

  Message Description: The machine's attribute retrieval from Active Directory has failed.

  Local Target Message Format: <timestamp> <seq_num> 24481 ERROR External-Active-Directory: The machine's attribute retrieval from Active Directory has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24481 ERROR External-Active-Directory: The machine's attribute retrieval from Active Directory has failed, <log details>

- **Message Code:** 24482

  Severity: INFO

  Message Text: Successfully retrieved the machine certificate from Active Directory

  Message Description: Successfully retrieved the machine certificate from Active Directory.

  Local Target Message Format: <timestamp> <seq_num> 24482 INFO External-Active-Directory: Successfully retrieved the machine certificate from Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24482 INFO External-Active-Directory: Successfully retrieved the machine certificate from Active Directory, <log details>

- **Message Code:** 24483

  Severity: ERROR

  Message Text: Failed to retrieve the machine certificate from Active Directory

  Message Description: Failed to retrieve the machine certificate from Active Directory.

  Local Target Message Format: <timestamp> <seq_num> 24483 ERROR External-Active-Directory: Failed to retrieve the machine certificate from Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24483 ERROR External-Active-Directory: Failed to retrieve the machine certificate from Active Directory, <log details>

- **Message Code:** 24484

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory has failed because the machine's password has expired

Message Description: Machine authentication against Active Directory has failed because the machine's password has expired.

Local Target Message Format: <timestamp> <seq_num> 24484 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's password has expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24484 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's password has expired, <log details>

- **Message Code:** 24485

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory has failed because of wrong password

  Message Description: Machine authentication against Active Directory has failed because of wrong password.

  Local Target Message Format: <timestamp> <seq_num> 24485 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because of wrong password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24485 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because of wrong password, <log details>

- **Message Code:** 24486

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory has failed because the machine's account is disabled

  Message Description: Machine authentication against Active Directory has failed because the machine's account is disabled.

  Local Target Message Format: <timestamp> <seq_num> 24486 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's account is disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24486 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's account is disabled, <log details>

- **Message Code:** 24487

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory failed since machine is considered to be in restricted logon hours

  Message Description: Machine authentication against Active Directory failed since machine is considered to be in restricted logon hours

Local Target Message Format: <timestamp> <seq_num> 24487 DEBUG External-Active-Directory: Machine authentication against Active Directory failed since machine is considered to be in restricted logon hours, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24487 DEBUG External-Active-Directory: Machine authentication against Active Directory failed since machine is considered to be in restricted logon hours, <log details>

- **Message Code:** 24488

  Severity: DEBUG

  Message Text: The machine's domain is not recognized by Active Directory

  Message Description: The machine's domain is not recognized by Active Directory.

  Local Target Message Format: <timestamp> <seq_num> 24488 DEBUG External-Active-Directory: The machine's domain is not recognized by Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24488 DEBUG External-Active-Directory: The machine's domain is not recognized by Active Directory, <log details>

- **Message Code:** 24489

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory has failed because the machine's account has expired

  Message Description: Machine authentication against Active Directory has failed because the machine's account has expired.

  Local Target Message Format: <timestamp> <seq_num> 24489 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's account has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24489 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's account has expired, <log details>

- **Message Code:** 24490

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory has failed because the machine's account is locked out

  Message Description: Machine authentication against Active Directory has failed because the machine's account is locked out.

  Local Target Message Format: <timestamp> <seq_num> 24490 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine's account is locked out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24490 DEBUG

External-Active-Directory: Machine authentication against Active Directory has failed because the machine's account is locked out, <log details>

- **Message Code:** 24491

  Severity: DEBUG

  Message Text: Machine authentication against Active Directory has failed because the machine has invalid credentials

  Message Description: Machine authentication against Active Directory has failed because the machine has invalid credentials.

  Local Target Message Format: <timestamp> <seq_num> 24491 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine has invalid credentials, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24491 DEBUG External-Active-Directory: Machine authentication against Active Directory has failed because the machine has invalid credentials, <log details>

- **Message Code:** 24492

  Severity: ERROR

  Message Text: Machine authentication against Active Directory has failed

  Message Description: Machine authentication against Active Directory has failed.

  Local Target Message Format: <timestamp> <seq_num> 24492 ERROR External-Active-Directory: Machine authentication against Active Directory has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24492 ERROR External-Active-Directory: Machine authentication against Active Directory has failed, <log details>

- **Message Code:** 24493

  Severity: ERROR

  Message Text: ISE has problems communicating with Active Directory using its machine credentials

  Message Description: ISE has problems communicating with Active Directory using its machine credentials.

  Local Target Message Format: <timestamp> <seq_num> 24493 ERROR External-Active-Directory: ISE has problems communicating with Active Directory using its machine credentials, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24493 ERROR External-Active-Directory: ISE has problems communicating with Active Directory using its machine credentials, <log details>

- **Message Code:** 24494

  Severity: ERROR

  Message Text: Active Directory DNS servers are not available

Message Description: Active Directory DNS servers are not available.

Local Target Message Format: <timestamp> <seq_num> 24494 ERROR External-Active-Directory: Active Directory DNS servers are not available, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24494 ERROR External-Active-Directory: Active Directory DNS servers are not available, <log details>

- **Message Code:** 24495

  Severity: ERROR

  Message Text: Active Directory servers are not available

  Message Description: Active Directory servers are not available.

  Local Target Message Format: <timestamp> <seq_num> 24495 ERROR External-Active-Directory: Active Directory servers are not available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24495 ERROR External-Active-Directory: Active Directory servers are not available, <log details>

- **Message Code:** 24496

  Severity: WARN

  Message Text: Authentication rejected due to a white or black list restriction

  Message Description: Authentication rejected due to a white or black list restriction

  Local Target Message Format: <timestamp> <seq_num> 24496 WARN External-Active-Directory: Authentication rejected due to a white or black list restriction, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24496 WARN External-Active-Directory: Authentication rejected due to a white or black list restriction, <log details>

- **Message Code:** 24497

  Severity: ERROR

  Message Text: Selected Active Directory Scope is empty

  Message Description: Selected Active Directory Scope is empty

  Local Target Message Format: <timestamp> <seq_num> 24497 ERROR External-Active-Directory: Selected Active Directory Scope is empty, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24497 ERROR External-Active-Directory: Selected Active Directory Scope is empty, <log details>

- **Message Code:** 24498

  Severity: ERROR

  Message Text: Resolve identity exceeded time limit

  Message Description: User's Attributes retrieval from Active Directory failed because of a timeout error

Local Target Message Format: <timestamp> <seq_num> 24498 ERROR External-Active-Directory: Resolve identity exceeded time limit, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24498 ERROR External-Active-Directory: Resolve identity exceeded time limit, <log details>

- **Message Code:** 24500

  Severity: DEBUG

  Message Text: Authenticating user against the RSA SecurID Server

  Message Description: Authenticating user against the RSA SecurID Server.

  Local Target Message Format: <timestamp> <seq_num> 24500 DEBUG External-RSA-SecurID-Server: Authenticating user against the RSA SecurID Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24500 DEBUG External-RSA-SecurID-Server: Authenticating user against the RSA SecurID Server, <log details>

- **Message Code:** 24501

  Severity: DEBUG

  Message Text: A session is established with the RSA SecurID Server

  Message Description: A session is established with the RSA SecurID Server.

  Local Target Message Format: <timestamp> <seq_num> 24501 DEBUG External-RSA-SecurID-Server: A session is established with the RSA SecurID Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24501 DEBUG External-RSA-SecurID-Server: A session is established with the RSA SecurID Server, <log details>

- **Message Code:** 24502

  Severity: DEBUG

  Message Text: The session with RSA SecurID Server is closed

  Message Description: The session with RSA SecurID Server is closed

  Local Target Message Format: <timestamp> <seq_num> 24502 DEBUG External-RSA-SecurID-Server: The session with RSA SecurID Server is closed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24502 DEBUG External-RSA-SecurID-Server: The session with RSA SecurID Server is closed, <log details>

- **Message Code:** 24503

  Severity: ERROR

  Message Text: Cannot establish a session with the RSA SecurID Server

  Message Description: Cannot establish a session with the RSA SecurID Server.

Local Target Message Format: <timestamp> <seq_num> 24503 ERROR External-RSA-SecurID-Server: Cannot establish a session with the RSA SecurID Server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24503 ERROR External-RSA-SecurID-Server: Cannot establish a session with the RSA SecurID Server, <log details>

- **Message Code:** 24504

  Severity: ERROR

  Message Text: The lock user request has failed

  Message Description: The lock user request has failed.

  Local Target Message Format: <timestamp> <seq_num> 24504 ERROR External-RSA-SecurID-Server: The lock user request has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24504 ERROR External-RSA-SecurID-Server: The lock user request has failed, <log details>

- **Message Code:** 24505

  Severity: DEBUG

  Message Text: User authentication has succeeded

  Message Description: User authentication against the RSA SecurID Server has succeeded.

  Local Target Message Format: <timestamp> <seq_num> 24505 DEBUG External-RSA-SecurID-Server: User authentication has succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24505 DEBUG External-RSA-SecurID-Server: User authentication has succeeded, <log details>

- **Message Code:** 24506

  Severity: DEBUG

  Message Text: Check passcode operation succeeded

  Message Description: Check passcode operation against RSA SecurID Server succeeded

  Local Target Message Format: <timestamp> <seq_num> 24506 DEBUG External-RSA-SecurID-Server: Check passcode operation succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24506 DEBUG External-RSA-SecurID-Server: Check passcode operation succeeded, <log details>

- **Message Code:** 24507

  Severity: DEBUG

  Message Text: Next Tokencode operation succeeded

  Message Description: Next Tokencode operation against RSA SecurID Server succeeded

Local Target Message Format: <timestamp> <seq_num> 24507 DEBUG External-RSA-SecurID-Server: Next Tokencode operation succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24507 DEBUG External-RSA-SecurID-Server: Next Tokencode operation succeeded, <log details>

- **Message Code:** 24508

  Severity: DEBUG

  Message Text: User authentication failed

  Message Description: User authentication against RSA SecurID Server failed

  Local Target Message Format: <timestamp> <seq_num> 24508 DEBUG External-RSA-SecurID-Server: User authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24508 DEBUG External-RSA-SecurID-Server: User authentication failed, <log details>

- **Message Code:** 24509

  Severity: DEBUG

  Message Text: Check passcode resulted in Next Tokencode required

  Message Description: Check passcode resulted in Next Tokencode required

  Local Target Message Format: <timestamp> <seq_num> 24509 DEBUG External-RSA-SecurID-Server: Check passcode resulted in Next Tokencode required, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24509 DEBUG External-RSA-SecurID-Server: Check passcode resulted in Next Tokencode required, <log details>

- **Message Code:** 24510

  Severity: DEBUG

  Message Text: Check passcode resulted in setting New PIN required

  Message Description: Check passcode resulted in setting New PIN required

  Local Target Message Format: <timestamp> <seq_num> 24510 DEBUG External-RSA-SecurID-Server: Check passcode resulted in setting New PIN required, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24510 DEBUG External-RSA-SecurID-Server: Check passcode resulted in setting New PIN required, <log details>

- **Message Code:** 24511

  Severity: ERROR

  Message Text: Check passcode operation against RSA SecurID Server resulted in error

  Message Description: Check passcode operation against RSA SecurID Server resulted in error

Local Target Message Format: <timestamp> <seq_num> 24511 ERROR External-RSA-SecurID-Server: Check passcode operation against RSA SecurID Server resulted in error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24511 ERROR External-RSA-SecurID-Server: Check passcode operation against RSA SecurID Server resulted in error, <log details>

- **Message Code:** 24512

  Severity: ERROR

  Message Text: Next tokencode operation in RSA SecurID Server resulted in error

  Message Description: Next tokencode operation in RSA SecurID Server resulted in error

  Local Target Message Format: <timestamp> <seq_num> 24512 ERROR External-RSA-SecurID-Server: Next tokencode operation in RSA SecurID Server resulted in error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24512 ERROR External-RSA-SecurID-Server: Next tokencode operation in RSA SecurID Server resulted in error, <log details>

- **Message Code:** 24513

  Severity: ERROR

  Message Text: Set New PIN operation in RSA SecurID Server resulted in error

  Message Description: Set New PIN operation in RSA SecurID Server resulted in error

  Local Target Message Format: <timestamp> <seq_num> 24513 ERROR External-RSA-SecurID-Server: Set New PIN operation in RSA SecurID Server resulted in error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24513 ERROR External-RSA-SecurID-Server: Set New PIN operation in RSA SecurID Server resulted in error, <log details>

- **Message Code:** 24514

  Severity: DEBUG

  Message Text: Next tokencode operation in RSA SecurID Server failed

  Message Description: Next tokencode operation in RSA SecurID Server failed

  Local Target Message Format: <timestamp> <seq_num> 24514 DEBUG External-RSA-SecurID-Server: Next tokencode operation in RSA SecurID Server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24514 DEBUG External-RSA-SecurID-Server: Next tokencode operation in RSA SecurID Server failed, <log details>

- **Message Code:** 24515

  Severity: DEBUG

  Message Text: Set New PIN operation in RSA SecurID Server failed

Message Description: Set New PIN operation in RSA SecurID Server failed

Local Target Message Format: <timestamp> <seq_num> 24515 DEBUG External-RSA-SecurID-Server: Set New PIN operation in RSA SecurID Server failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24515 DEBUG External-RSA-SecurID-Server: Set New PIN operation in RSA SecurID Server failed, <log details>

- **Message Code:** 24516

  Severity: DEBUG

  Message Text: New PIN was set successfully

  Message Description: New PIN was set successfully

  Local Target Message Format: <timestamp> <seq_num> 24516 DEBUG External-RSA-SecurID-Server: New PIN was set successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24516 DEBUG External-RSA-SecurID-Server: New PIN was set successfully, <log details>

- **Message Code:** 24517

  Severity: DEBUG

  Message Text: User accepts system's PIN

  Message Description: User chose to accept system's PIN

  Local Target Message Format: <timestamp> <seq_num> 24517 DEBUG External-RSA-SecurID-Server: User accepts system's PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24517 DEBUG External-RSA-SecurID-Server: User accepts system's PIN, <log details>

- **Message Code:** 24518

  Severity: DEBUG

  Message Text: User canceled New PIN operation; User authentication against RSA SecurIDServer failed

  Message Description: User canceled New PIN operation; User authentication against RSA SecurID Server failed

  Local Target Message Format: <timestamp> <seq_num> 24518 DEBUG External-RSA-SecurID-Server: User canceled New PIN operation; User authentication against RSA SecurIDServer failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24518 DEBUG External-RSA-SecurID-Server: User canceled New PIN operation; User authentication against RSA SecurIDServer failed, <log details>

- **Message Code:** 24519

  Severity: DEBUG

  Message Text: User entered invalid PIN; PIN must only contain alpha-numeric characters

Message Description: User entered invalid PIN; PIN must only contain alpha-numeric characters

Local Target Message Format: <timestamp> <seq_num> 24519 DEBUG External-RSA-SecurID-Server: User entered invalid PIN; PIN must only contain alpha-numeric characters, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24519 DEBUG External-RSA-SecurID-Server: User entered invalid PIN; PIN must only contain alpha-numeric characters, <log details>

- **Message Code:** 24520

  Severity: DEBUG

  Message Text: User entered invalid PIN; PIN must only contain numeric characters

  Message Description: User entered invalid PIN; PIN must only contain numeric characters

  Local Target Message Format: <timestamp> <seq_num> 24520 DEBUG External-RSA-SecurID-Server: User entered invalid PIN; PIN must only contain numeric characters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24520 DEBUG External-RSA-SecurID-Server: User entered invalid PIN; PIN must only contain numeric characters, <log details>

- **Message Code:** 24521

  Severity: DEBUG

  Message Text: User entered PIN with invalid length

  Message Description: User entered PIN with invalid length

  Local Target Message Format: <timestamp> <seq_num> 24521 DEBUG External-RSA-SecurID-Server: User entered PIN with invalid length, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24521 DEBUG External-RSA-SecurID-Server: User entered PIN with invalid length, <log details>

- **Message Code:** 24522

  Severity: DEBUG

  Message Text: PIN Accepted. Wait for the token code to change, then reauthenticate using the new passcode.

  Message Description: PIN Accepted. Wait for the token code to change, then reauthenticate using the new passcode.

  Local Target Message Format: <timestamp> <seq_num> 24522 DEBUG External-RSA-SecurID-Server: PIN Accepted. Wait for the token code to change, then reauthenticate using the new passcode., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24522 DEBUG External-RSA-SecurID-Server: PIN Accepted. Wait for the token code to change, then reauthenticate using the new passcode., <log details>

- **Message Code:** 24523

  Severity: DEBUG

  Message Text: Returned challenge asking the user to enter next tokencode

  Message Description: Returned challenge asking the enter next tokencode

  Local Target Message Format: <timestamp> <seq_num> 24523 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to enter next tokencode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24523 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to enter next tokencode, <log details>

- **Message Code:** 24524

  Severity: DEBUG

  Message Text: Received user response for next tokencode challenge

  Message Description: Received user response for next tokencode challenge

  Local Target Message Format: <timestamp> <seq_num> 24524 DEBUG External-RSA-SecurID-Server: Received user response for next tokencode challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24524 DEBUG External-RSA-SecurID-Server: Received user response for next tokencode challenge, <log details>

- **Message Code:** 24525

  Severity: DEBUG

  Message Text: Returned challenge asking the user to accept system's PIN

  Message Description: Returned challenge asking the user to accept system's PIN

  Local Target Message Format: <timestamp> <seq_num> 24525 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to accept system's PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24525 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to accept system's PIN, <log details>

- **Message Code:** 24526

  Severity: DEBUG

  Message Text: Received user response for accept system PIN challenge

  Message Description: Received user response for accept system PIN challenge

  Local Target Message Format: <timestamp> <seq_num> 24526 DEBUG External-RSA-SecurID-Server: Received user response for accept system PIN challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24526 DEBUG External-RSA-SecurID-Server: Received user response for accept system PIN challenge, <log details>

- **Message Code:** 24527

Severity: DEBUG

Message Text: Returned challenge asking the user to enter new PIN

Message Description: Returned challenge asking the user to enter new PIN

Local Target Message Format: <timestamp> <seq_num> 24527 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to enter new PIN, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24527 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to enter new PIN, <log details>

- **Message Code:** 24528

  Severity: DEBUG

  Message Text: Received user response for enter new PIN challenge

  Message Description: Received user response for enter new PIN challenge

  Local Target Message Format: <timestamp> <seq_num> 24528 DEBUG External-RSA-SecurID-Server: Received user response for enter new PIN challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24528 DEBUG External-RSA-SecurID-Server: Received user response for enter new PIN challenge, <log details>

- **Message Code:** 24529

  Severity: DEBUG

  Message Text: Returned challenge displaying the user his new PIN

  Message Description: Returned challenge displaying the user his new PIN

  Local Target Message Format: <timestamp> <seq_num> 24529 DEBUG External-RSA-SecurID-Server: Returned challenge displaying the user his new PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24529 DEBUG External-RSA-SecurID-Server: Returned challenge displaying the user his new PIN, <log details>

- **Message Code:** 24530

  Severity: DEBUG

  Message Text: Received user response for challenge displaying him his new PIN

  Message Description: Received user response for challenge displaying him his new PIN

  Local Target Message Format: <timestamp> <seq_num> 24530 DEBUG External-RSA-SecurID-Server: Received user response for challenge displaying him his new PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24530 DEBUG External-RSA-SecurID-Server: Received user response for challenge displaying him his new PIN, <log details>

- **Message Code:** 24531

Severity: DEBUG

Message Text: Returned challenge asking the user to reenter new PIN

Message Description: Returned challenge asking the user to reenter new PIN

Local Target Message Format: <timestamp> <seq_num> 24531 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to reenter new PIN, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24531 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user to reenter new PIN, <log details>

- **Message Code:** 24532

  Severity: DEBUG

  Message Text: Received user response for challenge asking the user to reenter new PIN

  Message Description: Received user response for challenge asking the user to reenter new PIN

  Local Target Message Format: <timestamp> <seq_num> 24532 DEBUG External-RSA-SecurID-Server: Received user response for challenge asking the user to reenter new PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24532 DEBUG External-RSA-SecurID-Server: Received user response for challenge asking the user to reenter new PIN, <log details>

- **Message Code:** 24533

  Severity: ERROR

  Message Text: User reentered a different PIN

  Message Description: User reentered a different PIN

  Local Target Message Format: <timestamp> <seq_num> 24533 ERROR External-RSA-SecurID-Server: User reentered a different PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24533 ERROR External-RSA-SecurID-Server: User reentered a different PIN, <log details>

- **Message Code:** 24534

  Severity: DEBUG

  Message Text: Returned challenge asking the user whether he is going to accept system's PIN or will enter a new PIN by himself

  Message Description: Returned challenge asking the user whether he is going to accept system's PIN or will enter a new PIN by himself

  Local Target Message Format: <timestamp> <seq_num> 24534 DEBUG External-RSA-SecurID-Server: Returned challenge asking the user whether he is going to accept system's PIN or will enter a new PIN by himself, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24534 DEBUG

External-RSA-SecurID-Server: Returned challenge asking the user whether he is going to accept system's PIN or will enter a new PIN by himself, <log details>

- **Message Code:** 24535

  Severity: DEBUG

  Message Text: Received user response for challenge asking the user to accept system's PIN or enter a new PIN

  Message Description: Received user response for challenge asking the user to accept system's PIN or enter a new PIN

  Local Target Message Format: <timestamp> <seq_num> 24535 DEBUG External-RSA-SecurID-Server: Received user response for challenge asking the user to accept system's PIN or enter a new PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24535 DEBUG External-RSA-SecurID-Server: Received user response for challenge asking the user to accept system's PIN or enter a new PIN, <log details>

- **Message Code:** 24536

  Severity: DEBUG

  Message Text: User chose to enter a new PIN

  Message Description: User chose to enter a new PIN

  Local Target Message Format: <timestamp> <seq_num> 24536 DEBUG External-RSA-SecurID-Server: User chose to enter a new PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24536 DEBUG External-RSA-SecurID-Server: User chose to enter a new PIN, <log details>

- **Message Code:** 24537

  Severity: DEBUG

  Message Text: User chose to accept system's PIN

  Message Description: User chose to accept system's PIN

  Local Target Message Format: <timestamp> <seq_num> 24537 DEBUG External-RSA-SecurID-Server: User chose to accept system's PIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24537 DEBUG External-RSA-SecurID-Server: User chose to accept system's PIN, <log details>

- **Message Code:** 24538

  Severity: DEBUG

  Message Text: RSA Session was invalidated

  Message Description: RSA Session was invalidated due to agent configuration changes during session

Local Target Message Format: <timestamp> <seq_num> 24538 DEBUG External-RSA-SecurID-Server: RSA Session was invalidated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24538 DEBUG External-RSA-SecurID-Server: RSA Session was invalidated, <log details>

- **Message Code:** 24539

  Severity: INFO

  Message Text: RSA agent configuration loaded, RSA agent started

  Message Description: RSA agent configuration loaded, RSA agent started

  Local Target Message Format: <timestamp> <seq_num> 24539 INFO External-RSA-SecurID-Server: RSA agent configuration loaded, RSA agent started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24539 INFO External-RSA-SecurID-Server: RSA agent configuration loaded, RSA agent started, <log details>

- **Message Code:** 24540

  Severity: INFO

  Message Text: RSA agent configuration initialized, RSA agent started

  Message Description: RSA agent configuration initialized, RSA agent started

  Local Target Message Format: <timestamp> <seq_num> 24540 INFO External-RSA-SecurID-Server: RSA agent configuration initialized, RSA agent started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24540 INFO External-RSA-SecurID-Server: RSA agent configuration initialized, RSA agent started, <log details>

- **Message Code:** 24541

  Severity: INFO

  Message Text: RSA agent configuration updated, RSA agent restarted

  Message Description: RSA agent configuration updated, RSA agent restarted

  Local Target Message Format: <timestamp> <seq_num> 24541 INFO External-RSA-SecurID-Server: RSA agent configuration updated, RSA agent restarted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24541 INFO External-RSA-SecurID-Server: RSA agent configuration updated, RSA agent restarted, <log details>

- **Message Code:** 24542

  Severity: INFO

  Message Text: RSA agent configuration deleted, RSA agent stopped

  Message Description: RSA agent configuration deleted, RSA agent stopped

Local Target Message Format: <timestamp> <seq_num> 24542 INFO External-RSA-SecurID-Server: RSA agent configuration deleted, RSA agent stopped, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24542 INFO External-RSA-SecurID-Server: RSA agent configuration deleted, RSA agent stopped, <log details>

- **Message Code:** 24543

  Severity: DEBUG

  Message Text: RSA session timeout, session cancelled

  Message Description: RSA session timeout, session cancelled

  Local Target Message Format: <timestamp> <seq_num> 24543 DEBUG External-RSA-SecurID-Server: RSA session timeout, session cancelled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24543 DEBUG External-RSA-SecurID-Server: RSA session timeout, session cancelled, <log details>

- **Message Code:** 24544

  Severity: ERROR

  Message Text: RSA agent initialization failed

  Message Description: RSA agent initialization failed

  Local Target Message Format: <timestamp> <seq_num> 24544 ERROR External-RSA-SecurID-Server: RSA agent initialization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24544 ERROR External-RSA-SecurID-Server: RSA agent initialization failed, <log details>

- **Message Code:** 24545

  Severity: INFO

  Message Text: The securid file has been removed

  Message Description: The securid file has been removed

  Local Target Message Format: <timestamp> <seq_num> 24545 INFO External-RSA-SecurID-Server: The securid file has been removed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24545 INFO External-RSA-SecurID-Server: The securid file has been removed, <log details>

- **Message Code:** 24546

  Severity: INFO

  Message Text: The sdstatus.12 file has been removed

  Message Description: The sdstatus.12 file has been removed

Local Target Message Format: <timestamp> <seq_num> 24546 INFO External-RSA-SecurID-Server: The sdstatus.12 file has been removed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24546 INFO External-RSA-SecurID-Server: The sdstatus.12 file has been removed, <log details>

- **Message Code:** 24547

  Severity: WARN

  Message Text: RSA request timeout expired. RSA authentication session cancelled

  Message Description: RSA request timeout expired. RSA authentication session cancelled.

  Local Target Message Format: <timestamp> <seq_num> 24547 WARN External-RSA-SecurID-Server: RSA request timeout expired. RSA authentication session cancelled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24547 WARN External-RSA-SecurID-Server: RSA request timeout expired. RSA authentication session cancelled, <log details>

- **Message Code:** 24548

  Severity: ERROR

  Message Text: RSA agent configuration load failed

  Message Description: RSA agent configuration load failed

  Local Target Message Format: <timestamp> <seq_num> 24548 ERROR External-RSA-SecurID-Server: RSA agent configuration load failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24548 ERROR External-RSA-SecurID-Server: RSA agent configuration load failed, <log details>

- **Message Code:** 24549

  Severity: ERROR

  Message Text: RSA agent configuration initialization failed

  Message Description: RSA agent configuration initialization failed

  Local Target Message Format: <timestamp> <seq_num> 24549 ERROR External-RSA-SecurID-Server: RSA agent configuration initialization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24549 ERROR External-RSA-SecurID-Server: RSA agent configuration initialization failed, <log details>

- **Message Code:** 24550

  Severity: ERROR

  Message Text: RSA agent configuration update failed

  Message Description: RSA agent configuration update failed

Local Target Message Format: <timestamp> <seq_num> 24550 ERROR External-RSA-SecurID-Server: RSA agent configuration update failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24550 ERROR External-RSA-SecurID-Server: RSA agent configuration update failed, <log details>

- **Message Code:** 24551

  Severity: WARN

  Message Text: RSA request is declined, because RSA agent initialization has failed

  Message Description: RSA request is declined, because RSA agent initialization has failed.

  Local Target Message Format: <timestamp> <seq_num> 24551 WARN External-RSA-SecurID-Server: RSA request is declined, because RSA agent initialization has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24551 WARN External-RSA-SecurID-Server: RSA request is declined, because RSA agent initialization has failed, <log details>

- **Message Code:** 24552

  Severity: DEBUG

  Message Text: Reject response from the RSA server is considered as User not found

  Message Description: According to the configuration of RSA Identity Store, reject response from the RSA server is considered as User not found.

  Local Target Message Format: <timestamp> <seq_num> 24552 DEBUG External-RSA-SecurID-Server: Reject response from the RSA server is considered as User not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24552 DEBUG External-RSA-SecurID-Server: Reject response from the RSA server is considered as User not found, <log details>

- **Message Code:** 24553

  Severity: DEBUG

  Message Text: User record was cached

  Message Description: Following a successful authentication against the RSA SecurID server, user record was cached.

  Local Target Message Format: <timestamp> <seq_num> 24553 DEBUG External-RSA-SecurID-Server: User record was cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24553 DEBUG External-RSA-SecurID-Server: User record was cached, <log details>

- **Message Code:** 24554

  Severity: DEBUG

Message Text: User record was not cached

Message Description: User record was not cached.

Local Target Message Format: <timestamp> <seq_num> 24554 DEBUG External-RSA-SecurID-Server: User record was not cached, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24554 DEBUG External-RSA-SecurID-Server: User record was not cached, <log details>

- **Message Code:** 24555

  Severity: DEBUG

  Message Text: User record was found in the cache

  Message Description: User record was found and retrieved from the cache

  Local Target Message Format: <timestamp> <seq_num> 24555 DEBUG External-RSA-SecurID-Server: User record was found in the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24555 DEBUG External-RSA-SecurID-Server: User record was found in the cache, <log details>

- **Message Code:** 24556

  Severity: DEBUG

  Message Text: User record was not found in the cache

  Message Description: User record was not found in the cache.

  Local Target Message Format: <timestamp> <seq_num> 24556 DEBUG External-RSA-SecurID-Server: User record was not found in the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24556 DEBUG External-RSA-SecurID-Server: User record was not found in the cache, <log details>

- **Message Code:** 24557

  Severity: DEBUG

  Message Text: An error occurred while searching for user records in the cache

  Message Description: An error occurred while searching for user records in the cache.

  Local Target Message Format: <timestamp> <seq_num> 24557 DEBUG External-RSA-SecurID-Server: An error occurred while searching for user records in the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24557 DEBUG External-RSA-SecurID-Server: An error occurred while searching for user records in the cache, <log details>

- **Message Code:** 24558

  Severity: DEBUG

Message Text: User cache is not enabled in the RSA identity store configuration

Message Description: User cache is not enabled in the RSA Identity Store configuration.

Local Target Message Format: <timestamp> <seq_num> 24558 DEBUG External-RSA-SecurID-Server: User cache is not enabled in the RSA identity store configuration, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24558 DEBUG External-RSA-SecurID-Server: User cache is not enabled in the RSA identity store configuration, <log details>

- **Message Code:** 24559

  Severity: DEBUG

  Message Text: Searching for user in the RSA identity store

  Message Description: Searching for user in the RSA identity store.

  Local Target Message Format: <timestamp> <seq_num> 24559 DEBUG External-RSA-SecurID-Server: Searching for user in the RSA identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24559 DEBUG External-RSA-SecurID-Server: Searching for user in the RSA identity store, <log details>

- **Message Code:** 24560

  Severity: DEBUG

  Message Text: Searching for user record in RSA identity store Passcode cache

  Message Description: Token Cache for RSA identity store is enabled. Searching for user record in RSA identity store Passcode cache in order to authenticate via cache.

  Local Target Message Format: <timestamp> <seq_num> 24560 DEBUG External-RSA-SecurID-Server: Searching for user record in RSA identity store Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24560 DEBUG External-RSA-SecurID-Server: Searching for user record in RSA identity store Passcode cache, <log details>

- **Message Code:** 24561

  Severity: DEBUG

  Message Text: User record was found in Passcode cache

  Message Description: User record was found in RSA identity store Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24561 DEBUG External-RSA-SecurID-Server: User record was found in Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24561 DEBUG External-RSA-SecurID-Server: User record was found in Passcode cache, <log details>

- **Message Code:** 24562

Severity: DEBUG

Message Text: User record was not found in Passcode cache

Message Description: User record was not found in RSA identity store Passcode cache. ISE will try to authenticate user against RSA Identity Store.

Local Target Message Format: <timestamp> <seq_num> 24562 DEBUG External-RSA-SecurID-Server: User record was not found in Passcode cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24562 DEBUG External-RSA-SecurID-Server: User record was not found in Passcode cache, <log details>

- **Message Code:** 24563

  Severity: DEBUG

  Message Text: An error occurred while searching for user record in the Passcode cache

  Message Description: An error occurred while searching for user record in the Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24563 DEBUG External-RSA-SecurID-Server: An error occurred while searching for user record in the Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24563 DEBUG External-RSA-SecurID-Server: An error occurred while searching for user record in the Passcode cache, <log details>

- **Message Code:** 24564

  Severity: DEBUG

  Message Text: Passcode cache is not enabled in the RSA identity store configuration

  Message Description: Passcode cache is not enabled in the RSA Identity Store configuration.

  Local Target Message Format: <timestamp> <seq_num> 24564 DEBUG External-RSA-SecurID-Server: Passcode cache is not enabled in the RSA identity store configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24564 DEBUG External-RSA-SecurID-Server: Passcode cache is not enabled in the RSA identity store configuration, <log details>

- **Message Code:** 24565

  Severity: DEBUG

  Message Text: Authentication passed via Passcode cache

  Message Description: User record was found in Passcode cache, passcode matches the passcode on the authentication request. Authentication passed via Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24565 DEBUG External-RSA-SecurID-Server: Authentication passed via Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24565 DEBUG External-RSA-SecurID-Server: Authentication passed via Passcode cache, <log details>

- **Message Code:** 24566

  Severity: DEBUG

  Message Text: Cached Passcode doesn't match passcode in authentication request. Passcode will be removed from the cache

  Message Description: Cached Passcode doesn't match passcode in authentication request. ISE will try to authenticate user against RSA Identity Store.

  Local Target Message Format: <timestamp> <seq_num> 24566 DEBUG External-RSA-SecurID-Server: Cached Passcode doesn't match passcode in authentication request. Passcode will be removed from the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24566 DEBUG External-RSA-SecurID-Server: Cached Passcode doesn't match passcode in authentication request. Passcode will be removed from the cache, <log details>

- **Message Code:** 24567

  Severity: DEBUG

  Message Text: User record was cached in Passcode cache

  Message Description: Following a successful authentication against the RSA SecurID server, user record was cached in passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24567 DEBUG External-RSA-SecurID-Server: User record was cached in Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24567 DEBUG External-RSA-SecurID-Server: User record was cached in Passcode cache, <log details>

- **Message Code:** 24568

  Severity: DEBUG

  Message Text: User record was not cached in Passcode cache

  Message Description: User record was not cached in Passcode cache

  Local Target Message Format: <timestamp> <seq_num> 24568 DEBUG External-RSA-SecurID-Server: User record was not cached in Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24568 DEBUG External-RSA-SecurID-Server: User record was not cached in Passcode cache, <log details>

- **Message Code:** 24600

  Severity: INFO

  Message Text: RADIUS token identity store is created

  Message Description: RADIUS token identity store is created.

  Local Target Message Format: <timestamp> <seq_num> 24600 INFO Radius-Token: RADIUS token identity store is created, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24600 INFO Radius-Token: RADIUS token identity store is created, <log details>

- **Message Code:** 24601

  Severity: INFO

  Message Text: RADIUS token identity store is destroyed

  Message Description: RADIUS token identity store is destroyed.

  Local Target Message Format: <timestamp> <seq_num> 24601 INFO Radius-Token: RADIUS token identity store is destroyed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24601 INFO Radius-Token: RADIUS token identity store is destroyed, <log details>

- **Message Code:** 24602

  Severity: INFO

  Message Text: RADIUS token identity store is configured with static prompt

  Message Description: RADIUS token identity store is configured with static prompt.

  Local Target Message Format: <timestamp> <seq_num> 24602 INFO Radius-Token: RADIUS token identity store is configured with static prompt, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24602 INFO Radius-Token: RADIUS token identity store is configured with static prompt, <log details>

- **Message Code:** 24603

  Severity: INFO

  Message Text: RADIUS token identity store configured to obtain prompt from RADIUS token server

  Message Description: RADIUS token identity store configured to obtain prompt from RADIUS token server

  Local Target Message Format: <timestamp> <seq_num> 24603 INFO Radius-Token: RADIUS token identity store configured to obtain prompt from RADIUS token server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24603 INFO Radius-Token: RADIUS token identity store configured to obtain prompt from RADIUS token server, <log details>

- **Message Code:** 24604

  Severity: INFO

  Message Text: RADIUS token primary server was created

  Message Description: RADIUS token primary server was created

  Local Target Message Format: <timestamp> <seq_num> 24604 INFO Radius-Token: RADIUS token primary server was created, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24604 INFO Radius-Token: RADIUS token primary server was created, <log details>

- **Message Code:** 24605

  Severity: INFO

  Message Text: RADIUS token secondary server was created

  Message Description: RADIUS token secondary server was created

  Local Target Message Format: <timestamp> <seq_num> 24605 INFO Radius-Token: RADIUS token secondary server was created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24605 INFO Radius-Token: RADIUS token secondary server was created, <log details>

- **Message Code:** 24606

  Severity: INFO

  Message Text: RADIUS token identity store configured to fail on authentication reject

  Message Description: RADIUS token identity store configured to fail on authentication reject

  Local Target Message Format: <timestamp> <seq_num> 24606 INFO Radius-Token: RADIUS token identity store configured to fail on authentication reject, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24606 INFO Radius-Token: RADIUS token identity store configured to fail on authentication reject, <log details>

- **Message Code:** 24607

  Severity: INFO

  Message Text: RADIUS token identity store configured to return unknown user error on authentication reject

  Message Description: RADIUS token identity store configured to return unknown user error on authentication reject

  Local Target Message Format: <timestamp> <seq_num> 24607 INFO Radius-Token: RADIUS token identity store configured to return unknown user error on authentication reject, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24607 INFO Radius-Token: RADIUS token identity store configured to return unknown user error on authentication reject, <log details>

- **Message Code:** 24608

  Severity: ERROR

  Message Text: RADIUS token identity store failed due to wrong input

  Message Description: RADIUS token identity store has failed due to wrong input.

Local Target Message Format: <timestamp> <seq_num> 24608 ERROR Radius-Token: RADIUS token identity store failed due to wrong input, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24608 ERROR Radius-Token: RADIUS token identity store failed due to wrong input, <log details>

- **Message Code:** 24609

  Severity: INFO

  Message Text: RADIUS token identity store is authenticating against the primary server

  Message Description: RADIUS token identity store is authenticating against the primary server.

  Local Target Message Format: <timestamp> <seq_num> 24609 INFO Radius-Token: RADIUS token identity store is authenticating against the primary server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24609 INFO Radius-Token: RADIUS token identity store is authenticating against the primary server, <log details>

- **Message Code:** 24610

  Severity: INFO

  Message Text: RADIUS token identity store is authenticating against the secondary server

  Message Description: RADIUS token identity store is authenticating against the secondary server.

  Local Target Message Format: <timestamp> <seq_num> 24610 INFO Radius-Token: RADIUS token identity store is authenticating against the secondary server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24610 INFO Radius-Token: RADIUS token identity store is authenticating against the secondary server, <log details>

- **Message Code:** 24611

  Severity: ERROR

  Message Text: RADIUS token server configuration error

  Message Description: RADIUS token server configuration error

  Local Target Message Format: <timestamp> <seq_num> 24611 ERROR Radius-Token: RADIUS token server configuration error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24611 ERROR Radius-Token: RADIUS token server configuration error, <log details>

- **Message Code:** 24612

  Severity: INFO

  Message Text: Authentication against the RADIUS token server succeeded

  Message Description: Authentication against the RADIUS token server succeeded.

Local Target Message Format: <timestamp> <seq_num> 24612 INFO Radius-Token: Authentication against the RADIUS token server succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24612 INFO Radius-Token: Authentication against the RADIUS token server succeeded, <log details>

- **Message Code:** 24613

  Severity: ERROR

  Message Text: Authentication against the RADIUS token server failed

  Message Description: Authentication against the RADIUS token server failed.

  Local Target Message Format: <timestamp> <seq_num> 24613 ERROR Radius-Token: Authentication against the RADIUS token server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24613 ERROR Radius-Token: Authentication against the RADIUS token server failed, <log details>

- **Message Code:** 24614

  Severity: INFO

  Message Text: RADIUS token server authentication failure is translated as Unknown user failure

  Message Description: RADIUS token server authentication failure is translated as Unknown user failure.

  Local Target Message Format: <timestamp> <seq_num> 24614 INFO Radius-Token: RADIUS token server authentication failure is translated as Unknown user failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24614 INFO Radius-Token: RADIUS token server authentication failure is translated as Unknown user failure, <log details>

- **Message Code:** 24615

  Severity: INFO

  Message Text: RADIUS token identity store received access challenge response

  Message Description: RADIUS token identity store received access challenge response.

  Local Target Message Format: <timestamp> <seq_num> 24615 INFO Radius-Token: RADIUS token identity store received access challenge response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24615 INFO Radius-Token: RADIUS token identity store received access challenge response, <log details>

- **Message Code:** 24616

  Severity: ERROR

  Message Text: RADIUS token identity store received timeout error

  Message Description: RADIUS token identity store received timeout error

Local Target Message Format: <timestamp> <seq_num> 24616 ERROR Radius-Token: RADIUS token identity store received timeout error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24616 ERROR Radius-Token: RADIUS token identity store received timeout error, <log details>

- **Message Code:** 24617

  Severity: ERROR

  Message Text: RADIUS token identity store received external error

  Message Description: RADIUS token identity store received external error

  Local Target Message Format: <timestamp> <seq_num> 24617 ERROR Radius-Token: RADIUS token identity store received external error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24617 ERROR Radius-Token: RADIUS token identity store received external error, <log details>

- **Message Code:** 24618

  Severity: ERROR

  Message Text: RADIUS token identity store received unknown error

  Message Description: RADIUS token identity store received unknown error

  Local Target Message Format: <timestamp> <seq_num> 24618 ERROR Radius-Token: RADIUS token identity store received unknown error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24618 ERROR Radius-Token: RADIUS token identity store received unknown error, <log details>

- **Message Code:** 24619

  Severity: DEBUG

  Message Text: Non-compliant attributes detected in the RADIUS token identity store

  Message Description: Non-compliant attributes are detected in the RADIUS token identity store.

  Local Target Message Format: <timestamp> <seq_num> 24619 DEBUG Radius-Token: Non-compliant attributes detected in the RADIUS token identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24619 DEBUG Radius-Token: Non-compliant attributes detected in the RADIUS token identity store, <log details>

- **Message Code:** 24620

  Severity: INFO

  Message Text: User name format was changed after authentication with the RADIUS token server

  Message Description: User name format was changed after authentication with the RADIUS token server.

Local Target Message Format: <timestamp> <seq_num> 24620 INFO Radius-Token: User name format was changed after authentication with the RADIUS token server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24620 INFO Radius-Token: User name format was changed after authentication with the RADIUS token server, <log details>

- **Message Code:** 24621

  Severity: INFO

  Message Text: RADIUS token identity store configured to return defined prompt

  Message Description: RADIUS token identity store has been configured to return defined prompt.

  Local Target Message Format: <timestamp> <seq_num> 24621 INFO Radius-Token: RADIUS token identity store configured to return defined prompt, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24621 INFO Radius-Token: RADIUS token identity store configured to return defined prompt, <log details>

- **Message Code:** 24622

  Severity: INFO

  Message Text: RADIUS token identity store configured to return prompt from the RADIUS token server

  Message Description: RADIUS token identity store has been configured to return prompt from the RADIUS token server.

  Local Target Message Format: <timestamp> <seq_num> 24622 INFO Radius-Token: RADIUS token identity store configured to return prompt from the RADIUS token server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24622 INFO Radius-Token: RADIUS token identity store configured to return prompt from the RADIUS token server, <log details>

- **Message Code:** 24623

  Severity: DEBUG

  Message Text: User record was cached

  Message Description: User record was cached after successful authentication against Radius Token Server

  Local Target Message Format: <timestamp> <seq_num> 24623 DEBUG Radius-Token: User record was cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24623 DEBUG Radius-Token: User record was cached, <log details>

- **Message Code:** 24624

  Severity: DEBUG

  Message Text: User record was not cached

  Message Description: User record was not cached.

Local Target Message Format: <timestamp> <seq_num> 24624 DEBUG Radius-Token: User record was not cached, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24624 DEBUG Radius-Token: User record was not cached, <log details>

- **Message Code:** 24625

  Severity: DEBUG

  Message Text: User record found in the cache

  Message Description: User record was found and retrieved from the cache.

  Local Target Message Format: <timestamp> <seq_num> 24625 DEBUG Radius-Token: User record found in the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24625 DEBUG Radius-Token: User record found in the cache, <log details>

- **Message Code:** 24626

  Severity: DEBUG

  Message Text: User record not found in the cache

  Message Description: User record was not found in the cache.

  Local Target Message Format: <timestamp> <seq_num> 24626 DEBUG Radius-Token: User record not found in the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24626 DEBUG Radius-Token: User record not found in the cache, <log details>

- **Message Code:** 24627

  Severity: DEBUG

  Message Text: An error occurred while searching for user records in the cache

  Message Description: An error occurred while searching for user records in the cache.

  Local Target Message Format: <timestamp> <seq_num> 24627 DEBUG Radius-Token: An error occurred while searching for user records in the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24627 DEBUG Radius-Token: An error occurred while searching for user records in the cache, <log details>

- **Message Code:** 24628

  Severity: DEBUG

  Message Text: User cache not enabled in the RADIUS token identity store configuration

  Message Description: User cache is not enabled in the RADIUS token identity store configuration.

Local Target Message Format: <timestamp> <seq_num> 24628 DEBUG Radius-Token: User cache not enabled in the RADIUS token identity store configuration, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24628 DEBUG Radius-Token: User cache not enabled in the RADIUS token identity store configuration, <log details>

- **Message Code:** 24629

  Severity: DEBUG

  Message Text: Searching for user in the RADIUS token identity store

  Message Description: Searching for user in the RADIUS token identity store.

  Local Target Message Format: <timestamp> <seq_num> 24629 DEBUG Radius-Token: Searching for user in the RADIUS token identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24629 DEBUG Radius-Token: Searching for user in the RADIUS token identity store, <log details>

- **Message Code:** 24630

  Severity: ERROR

  Message Text: Failed to get Server IP by name

  Message Description: Failed to get Server IP by name

  Local Target Message Format: <timestamp> <seq_num> 24630 ERROR Radius-Token: Failed to get Server IP by name, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24630 ERROR Radius-Token: Failed to get Server IP by name, <log details>

- **Message Code:** 24631

  Severity: DEBUG

  Message Text: Looking up User in Internal Guests IDStore

  Message Description: Looking up User in Internal Guests IDStore

  Local Target Message Format: <timestamp> <seq_num> 24631 DEBUG Local-user-DB: Looking up User in Internal Guests IDStore, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24631 DEBUG Local-user-DB: Looking up User in Internal Guests IDStore, <log details>

- **Message Code:** 24632

  Severity: DEBUG

  Message Text: Found User in Internal Guests IDStore

  Message Description: Found User in Internal Guests IDStore

Local Target Message Format: <timestamp> <seq_num> 24632 DEBUG Local-user-DB: Found User in Internal Guests IDStore, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24632 DEBUG Local-user-DB: Found User in Internal Guests IDStore, <log details>

- **Message Code:** 24633

  Severity: DEBUG

  Message Text: The user is not found in the internal guests identity store

  Message Description: The specified user is not found in the internal guests identity store.

  Local Target Message Format: <timestamp> <seq_num> 24633 DEBUG Local-user-DB: The user is not found in the internal guests identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24633 DEBUG Local-user-DB: The user is not found in the internal guests identity store, <log details>

- **Message Code:** 24634

  Severity: DEBUG

  Message Text: Searching for user record in RADIUS token identity store Passcode cache

  Message Description: Token Cache for RADIUS token identity store is enabled. Searching for user record in RADIUS token identity store Passcode cache in order to authenticate via cache.

  Local Target Message Format: <timestamp> <seq_num> 24634 DEBUG Radius-Token: Searching for user record in RADIUS token identity store Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24634 DEBUG Radius-Token: Searching for user record in RADIUS token identity store Passcode cache, <log details>

- **Message Code:** 24635

  Severity: DEBUG

  Message Text: User record was found in Passcode cache

  Message Description: User record was found in RADIUS token identity store Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24635 DEBUG Radius-Token: User record was found in Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24635 DEBUG Radius-Token: User record was found in Passcode cache, <log details>

- **Message Code:** 24636

  Severity: DEBUG

  Message Text: User record was not found in Passcode cache

  Message Description: User record was not found in RADIUS token identity store Passcode cache. ISE will try to authenticate user against RADIUS token Identity Store.

Local Target Message Format: <timestamp> <seq_num> 24636 DEBUG Radius-Token: User record was not found in Passcode cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24636 DEBUG Radius-Token: User record was not found in Passcode cache, <log details>

- **Message Code:** 24637

  Severity: DEBUG

  Message Text: An error occurred while searching for user record in the Passcode cache

  Message Description: An error occurred while searching for user record in the Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24637 DEBUG Radius-Token: An error occurred while searching for user record in the Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24637 DEBUG Radius-Token: An error occurred while searching for user record in the Passcode cache, <log details>

- **Message Code:** 24638

  Severity: DEBUG

  Message Text: Passcode cache is not enabled in the RADIUS token identity store configuration

  Message Description: Passcode cache is not enabled in the RADIUS token Identity Store configuration.

  Local Target Message Format: <timestamp> <seq_num> 24638 DEBUG Radius-Token: Passcode cache is not enabled in the RADIUS token identity store configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24638 DEBUG Radius-Token: Passcode cache is not enabled in the RADIUS token identity store configuration, <log details>

- **Message Code:** 24639

  Severity: DEBUG

  Message Text: Authentication passed via Passcode cache

  Message Description: User record was found in Passcode cache, passcode matches the passcode on the authentication request. Authentication passed via Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24639 DEBUG Radius-Token: Authentication passed via Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24639 DEBUG Radius-Token: Authentication passed via Passcode cache, <log details>

- **Message Code:** 24640

  Severity: DEBUG

  Message Text: Cached Passcode doesn't match passcode in authentication request. Passcode will be removed from the cache

Message Description: Cached Passcode doesn't match passcode in authentication request. ISE will try to authenticate user against RADIUS token Identity Store.

Local Target Message Format: <timestamp> <seq_num> 24640 DEBUG Radius-Token: Cached Passcode doesn't match passcode in authentication request. Passcode will be removed from the cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24640 DEBUG Radius-Token: Cached Passcode doesn't match passcode in authentication request. Passcode will be removed from the cache, <log details>

- **Message Code:** 24641

  Severity: DEBUG

  Message Text: User record was cached in Passcode cache

  Message Description: Following a successful authentication against the RADIUS token SecurID server, user record was cached in passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24641 DEBUG Radius-Token: User record was cached in Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24641 DEBUG Radius-Token: User record was cached in Passcode cache, <log details>

- **Message Code:** 24642

  Severity: DEBUG

  Message Text: User record was not cached in Passcode cache

  Message Description: User record was not cached in Passcode cache.

  Local Target Message Format: <timestamp> <seq_num> 24642 DEBUG Radius-Token: User record was not cached in Passcode cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24642 DEBUG Radius-Token: User record was not cached in Passcode cache, <log details>

- **Message Code:** 24700

  Severity: DEBUG

  Message Text: Identity resolution by certificate succeeded

  Message Description: Identity resolution by certificate succeeded

  Local Target Message Format: <timestamp> <seq_num> 24700 DEBUG External-Active-Directory: Identity resolution by certificate succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24700 DEBUG External-Active-Directory: Identity resolution by certificate succeeded, <log details>

- **Message Code:** 24701

Severity: DEBUG

Message Text: Identity resolution by certificate failed

Message Description: Identity resolution by certificate failed

Local Target Message Format: <timestamp> <seq_num> 24701 DEBUG External-Active-Directory: Identity resolution by certificate failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24701 DEBUG External-Active-Directory: Identity resolution by certificate failed, <log details>

- **Message Code:** 24702

  Severity: DEBUG

  Message Text: Identity resolution by certificate found no matching account

  Message Description: Identity resolution by certificate found no matching account

  Local Target Message Format: <timestamp> <seq_num> 24702 DEBUG External-Active-Directory: Identity resolution by certificate found no matching account, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24702 DEBUG External-Active-Directory: Identity resolution by certificate found no matching account, <log details>

- **Message Code:** 24703

  Severity: DEBUG

  Message Text: Identity resolution by certificate found ambiguous accounts

  Message Description: Identity resolution by certificate found ambiguous accounts

  Local Target Message Format: <timestamp> <seq_num> 24703 DEBUG External-Active-Directory: Identity resolution by certificate found ambiguous accounts, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24703 DEBUG External-Active-Directory: Identity resolution by certificate found ambiguous accounts, <log details>

- **Message Code:** 24704

  Severity: DEBUG

  Message Text: Authentication failed because identity credentials are ambiguous

  Message Description: Authentication found several accounts matching to the given credentials (i.e identity name and password)

  Local Target Message Format: <timestamp> <seq_num> 24704 DEBUG External-Active-Directory: Authentication failed because identity credentials are ambiguous, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24704 DEBUG External-Active-Directory: Authentication failed because identity credentials are ambiguous, <log details>

- **Message Code:** 24705

Severity: DEBUG

Message Text: Authentication failed because ISE server is not joined to required domains

Message Description: Authentication failed because ISE server is not joined to required domains

Local Target Message Format: <timestamp> <seq_num> 24705 DEBUG External-Active-Directory: Authentication failed because ISE server is not joined to required domains, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24705 DEBUG External-Active-Directory: Authentication failed because ISE server is not joined to required domains, <log details>

- **Message Code:** 24706

  Severity: DEBUG

  Message Text: Authentication failed because NTLM was blocked

  Message Description: Authentication failed because NTLM was blocked

  Local Target Message Format: <timestamp> <seq_num> 24706 DEBUG External-Active-Directory: Authentication failed because NTLM was blocked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24706 DEBUG External-Active-Directory: Authentication failed because NTLM was blocked, <log details>

- **Message Code:** 24707

  Severity: DEBUG

  Message Text: Authentication failed because all identity names have been rejected

  Message Description: Authentication failed all identity names has been rejected according AD Identity Store Advanced Settings

  Local Target Message Format: <timestamp> <seq_num> 24707 DEBUG External-Active-Directory: Authentication failed because all identity names have been rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24707 DEBUG External-Active-Directory: Authentication failed because all identity names have been rejected, <log details>

- **Message Code:** 24708

  Severity: DEBUG

  Message Text: User not found in Active Directory. Some authentication domains were not available

  Message Description: User not found in Active Directory. Some authentication domains were not available during identity resolution

  Local Target Message Format: <timestamp> <seq_num> 24708 DEBUG External-Active-Directory: User not found in Active Directory. Some authentication domains were not available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24708 DEBUG

External-Active-Directory: User not found in Active Directory. Some authentication domains were not available, <log details>

- **Message Code:** 24709

  Severity: DEBUG

  Message Text: Host not found in Active Directory. Some authentication domains were not available

  Message Description: Host not found in Active Directory. Some authentication domains were not available during identity resolution

  Local Target Message Format: <timestamp> <seq_num> 24709 DEBUG External-Active-Directory: Host not found in Active Directory. Some authentication domains were not available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24709 DEBUG External-Active-Directory: Host not found in Active Directory. Some authentication domains were not available, <log details>

- **Message Code:** 24710

  Severity: DEBUG

  Message Text: Identity resolution is configured to drop request if required domain is not available

  Message Description: Identity resolution is configured to drop request if required domain is not available

  Local Target Message Format: <timestamp> <seq_num> 24710 DEBUG External-Active-Directory: Identity resolution is configured to drop request if required domain is not available, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24710 DEBUG External-Active-Directory: Identity resolution is configured to drop request if required domain is not available, <log details>

- **Message Code:** 24711

  Severity: DEBUG

  Message Text: Domain controller cannot pass request through the trust path to the account domain

  Message Description: Domain controller cannot pass request through the trust path from the join point domain to the domain where user account is located

  Local Target Message Format: <timestamp> <seq_num> 24711 DEBUG External-Active-Directory: Domain controller cannot pass request through the trust path to the account domain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24711 DEBUG External-Active-Directory: Domain controller cannot pass request through the trust path to the account domain, <log details>

- **Message Code:** 24712

  Severity: DEBUG

  Message Text: Authentication failed because domain trust is restricted

  Message Description: Authentication failed because domain trust is restricted

Local Target Message Format: <timestamp> <seq_num> 24712 DEBUG External-Active-Directory: Authentication failed because domain trust is restricted, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24712 DEBUG External-Active-Directory: Authentication failed because domain trust is restricted, <log details>

- **Message Code:** 24713

  Severity: DEBUG

  Message Text: ISE peer has confirmed previous successful machine authentication for user in Active Directory

  Message Description: ISE peer has confirmed previous successful machine authentication for user in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24713 DEBUG External-Active-Directory: ISE peer has confirmed previous successful machine authentication for user in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24713 DEBUG External-Active-Directory: ISE peer has confirmed previous successful machine authentication for user in Active Directory, <log details>

- **Message Code:** 24714

  Severity: DEBUG

  Message Text: ISE peers have not confirmed previous successful machine authentication for user in Active Directory

  Message Description: ISE peers have not confirmed previous successful machine authentication for user in Active Directory

  Local Target Message Format: <timestamp> <seq_num> 24714 DEBUG External-Active-Directory: ISE peers have not confirmed previous successful machine authentication for user in Active Directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24714 DEBUG External-Active-Directory: ISE peers have not confirmed previous successful machine authentication for user in Active Directory, <log details>

- **Message Code:** 24715

  Severity: DEBUG

  Message Text: ISE has not confirmed locally previous successful machine authentication for user in Active Directory

  Message Description: ISE has not confirmed locally previous successful machine authentication for user in Active Directory. ACS is quering peers for confirmation

  Local Target Message Format: <timestamp> <seq_num> 24715 DEBUG External-Active-Directory: ISE has not confirmed locally previous successful machine authentication for user in Active Directory, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24715 DEBUG External-Active-Directory: ISE has not confirmed locally previous successful machine authentication for user in Active Directory, <log details>

- **Message Code:** 24800

  Severity: INFO

  Message Text: SAML Portal metadata was exported

  Message Description: SAML Portal metadata was exported

  Local Target Message Format: <timestamp> <seq_num> 24800 INFO System-Management: SAML Portal metadata was exported, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24800 INFO System-Management: SAML Portal metadata was exported, <log details>

- **Message Code:** 24801

  Severity: INFO

  Message Text: Unable to decode SAML request

  Message Description: Unable to decode SAML request

  Local Target Message Format: <timestamp> <seq_num> 24801 INFO External-SAML-IdP: Unable to decode SAML request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24801 INFO External-SAML-IdP: Unable to decode SAML request, <log details>

- **Message Code:** 24802

  Severity: INFO

  Message Text: Unknown SAML attribute value type assertion used for 'username'

  Message Description: Unknown SAML attribute value type assertion used for 'username'

  Local Target Message Format: <timestamp> <seq_num> 24802 INFO External-SAML-IdP: Unknown SAML attribute value type assertion used for 'username', <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24802 INFO External-SAML-IdP: Unknown SAML attribute value type assertion used for 'username', <log details>

- **Message Code:** 24803

  Severity: INFO

  Message Text: Unable to find 'username' attribute assertion

  Message Description: Unable to find 'username' attribute assertion

  Local Target Message Format: <timestamp> <seq_num> 24803 INFO External-SAML-IdP: Unable to find 'username' attribute assertion, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24803 INFO External-SAML-IdP: Unable to find 'username' attribute assertion, <log details>

- **Message Code:** 24804

  Severity: INFO

  Message Text: SAML message intended destination (required by binding) was not present

  Message Description: SAML message intended destination (required by binding) was not present

  Local Target Message Format: <timestamp> <seq_num> 24804 INFO External-SAML-IdP: SAML message intended destination (required by binding) was not present, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24804 INFO External-SAML-IdP: SAML message intended destination (required by binding) was not present, <log details>

- **Message Code:** 24805

  Severity: INFO

  Message Text: SAML message intended destination endpoint did not match recipient endpoint

  Message Description: SAML message intended destination endpoint did not match recipient endpoint

  Local Target Message Format: <timestamp> <seq_num> 24805 INFO External-SAML-IdP: SAML message intended destination endpoint did not match recipient endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24805 INFO External-SAML-IdP: SAML message intended destination endpoint did not match recipient endpoint, <log details>

- **Message Code:** 24806

  Severity: WARN

  Message Text: SAML IdentityProvider Certificate is not valid

  Message Description: SAML IdentityProvider Certificate is not valid

  Local Target Message Format: <timestamp> <seq_num> 24806 WARN External-SAML-IdP: SAML IdentityProvider Certificate is not valid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24806 WARN External-SAML-IdP: SAML IdentityProvider Certificate is not valid, <log details>

- **Message Code:** 24807

  Severity: WARN

  Message Text: SAML IdentityProvider Certificate was not checked

  Message Description: SAML IdentityProvider Certificate was not checked

  Local Target Message Format: <timestamp> <seq_num> 24807 WARN External-SAML-IdP: SAML IdentityProvider Certificate was not checked, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24807 WARN External-SAML-IdP: SAML IdentityProvider Certificate was not checked, <log details>

- **Message Code:** 24808

  Severity: WARN

  Message Text: SAML IdentityProvider Certificate is expired

  Message Description: SAML IdentityProvider Certificate is expired

  Local Target Message Format: <timestamp> <seq_num> 24808 WARN External-SAML-IdP: SAML IdentityProvider Certificate is expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24808 WARN External-SAML-IdP: SAML IdentityProvider Certificate is expired, <log details>

- **Message Code:** 24809

  Severity: WARN

  Message Text: SAML IdentityProvider Certificate is revoked

  Message Description: SAML IdentityProvider Certificate is revoked

  Local Target Message Format: <timestamp> <seq_num> 24809 WARN External-SAML-IdP: SAML IdentityProvider Certificate is revoked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24809 WARN External-SAML-IdP: SAML IdentityProvider Certificate is revoked, <log details>

- **Message Code:** 24810

  Severity: WARN

  Message Text: SAML IdentityProvider CA Certificate is not valid

  Message Description: SAML IdentityProvider CA Certificate is not valid

  Local Target Message Format: <timestamp> <seq_num> 24810 WARN External-SAML-IdP: SAML IdentityProvider CA Certificate is not valid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24810 WARN External-SAML-IdP: SAML IdentityProvider CA Certificate is not valid, <log details>

- **Message Code:** 24811

  Severity: INFO

  Message Text: The request could not be performed due to an error on the part of the requester

  Message Description: The request could not be performed due to an error on the part of the requester

  Local Target Message Format: <timestamp> <seq_num> 24811 INFO External-SAML-IdP: The request could not be performed due to an error on the part of the requester, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24811 INFO External-SAML-IdP: The request could not be performed due to an error on the part of the requester, <log details>

- **Message Code:** 24812

  Severity: INFO

  Message Text: The request could not be performed due to an error on the part of the SAML responder or SAML authority

  Message Description: The request could not be performed due to an error on the part of the SAML responder or SAML authority

  Local Target Message Format: <timestamp> <seq_num> 24812 INFO External-SAML-IdP: The request could not be performed due to an error on the part of the SAML responder or SAML authority, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24812 INFO External-SAML-IdP: The request could not be performed due to an error on the part of the SAML responder or SAML authority, <log details>

- **Message Code:** 24813

  Severity: INFO

  Message Text: The SAML responder could not process the request because the version of the request message was incorrect

  Message Description: The SAML responder could not process the request because the version of the request message was incorrect

  Local Target Message Format: <timestamp> <seq_num> 24813 INFO External-SAML-IdP: The SAML responder could not process the request because the version of the request message was incorrect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24813 INFO External-SAML-IdP: The SAML responder could not process the request because the version of the request message was incorrect, <log details>

- **Message Code:** 24814

  Severity: INFO

  Message Text: The responding provider was unable to successfully authenticate the principal

  Message Description: The responding provider was unable to successfully authenticate the principal

  Local Target Message Format: <timestamp> <seq_num> 24814 INFO External-SAML-IdP: The responding provider was unable to successfully authenticate the principal, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24814 INFO External-SAML-IdP: The responding provider was unable to successfully authenticate the principal, <log details>

- **Message Code:** 24815

Severity: INFO

Message Text: Unexpected or invalid content was encountered within a saml:Attribute or saml:AttributeValue element

Message Description: Unexpected or invalid content was encountered within a saml:Attribute or saml:AttributeValue element

Local Target Message Format: <timestamp> <seq_num> 24815 INFO External-SAML-IdP: Unexpected or invalid content was encountered within a saml:Attribute or saml:AttributeValue element, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24815 INFO External-SAML-IdP: Unexpected or invalid content was encountered within a saml:Attribute or saml:AttributeValue element, <log details>

- **Message Code:** 24816

  Severity: INFO

  Message Text: The SAML responder or SAML authority is able to process the request but has chosen not to respond.

  Message Description: The SAML responder or SAML authority is able to process the request but has chosen not to respond. This status code MAY be used when there is concern about the security context of the request message or the sequence of request messages received from a particular requester

  Local Target Message Format: <timestamp> <seq_num> 24816 INFO External-SAML-IdP: The SAML responder or SAML authority is able to process the request but has chosen not to respond., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24816 INFO External-SAML-IdP: The SAML responder or SAML authority is able to process the request but has chosen not to respond., <log details>

- **Message Code:** 24817

  Severity: INFO

  Message Text: The SAML responder or SAML authority does not support the request

  Message Description: The SAML responder or SAML authority does not support the request

  Local Target Message Format: <timestamp> <seq_num> 24817 INFO External-SAML-IdP: The SAML responder or SAML authority does not support the request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24817 INFO External-SAML-IdP: The SAML responder or SAML authority does not support the request, <log details>

- **Message Code:** 24818

  Severity: INFO

  Message Text: The SAML responder cannot properly fulfil the request using the protocol binding specified in the request

  Message Description: The SAML responder cannot properly fulfil the request using the protocol binding specified in the request

Local Target Message Format: <timestamp> <seq_num> 24818 INFO External-SAML-IdP: The SAML responder cannot properly fulfil the request using the protocol binding specified in the request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24818 INFO External-SAML-IdP: The SAML responder cannot properly fulfil the request using the protocol binding specified in the request, <log details>

- **Message Code:** 24819

  Severity: INFO

  Message Text: Failed to retrieve signing certificate from the SAML response

  Message Description: Failed to retrieve signing certificate from the SAML response

  Local Target Message Format: <timestamp> <seq_num> 24819 INFO External-SAML-IdP: Failed to retrieve signing certificate from the SAML response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24819 INFO External-SAML-IdP: Failed to retrieve signing certificate from the SAML response, <log details>

- **Message Code:** 24820

  Severity: DEBUG

  Message Text: Assertion does not contain Issuer

  Message Description: Assertion must contain Issuer

  Local Target Message Format: <timestamp> <seq_num> 24820 DEBUG External-SAML-IdP: Assertion does not contain Issuer, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24820 DEBUG External-SAML-IdP: Assertion does not contain Issuer, <log details>

- **Message Code:** 24821

  Severity: DEBUG

  Message Text: Assertion does not contain authentication statement

  Message Description: Assertion must contain authentication statement

  Local Target Message Format: <timestamp> <seq_num> 24821 DEBUG External-SAML-IdP: Assertion does not contain authentication statement, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24821 DEBUG External-SAML-IdP: Assertion does not contain authentication statement, <log details>

- **Message Code:** 24822

  Severity: DEBUG

  Message Text: Assertion does not contain audience restriction conditions

  Message Description: Assertion must contain audience restriction conditions

Local Target Message Format: <timestamp> <seq_num> 24822 DEBUG External-SAML-IdP: Assertion does not contain audience restriction conditions, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24822 DEBUG External-SAML-IdP: Assertion does not contain audience restriction conditions, <log details>

- **Message Code:** 24823

  Severity: DEBUG

  Message Text: Assertion does not contain matching service provider identifier in the audience restriction conditions

  Message Description: Assertion must contain matching service provider identifier in the audience restriction conditions

  Local Target Message Format: <timestamp> <seq_num> 24823 DEBUG External-SAML-IdP: Assertion does not contain matching service provider identifier in the audience restriction conditions, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24823 DEBUG External-SAML-IdP: Assertion does not contain matching service provider identifier in the audience restriction conditions, <log details>

- **Message Code:** 24824

  Severity: DEBUG

  Message Text: Subject confirmation does not contain subject confirmation data

  Message Description: Subject confirmation must contain subject confirmation data

  Local Target Message Format: <timestamp> <seq_num> 24824 DEBUG External-SAML-IdP: Subject confirmation does not contain subject confirmation data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24824 DEBUG External-SAML-IdP: Subject confirmation does not contain subject confirmation data, <log details>

- **Message Code:** 24825

  Severity: DEBUG

  Message Text: The response must contain single assertion

  Message Description: The response must contain single assertion

  Local Target Message Format: <timestamp> <seq_num> 24825 DEBUG External-SAML-IdP: The response must contain single assertion, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24825 DEBUG External-SAML-IdP: The response must contain single assertion, <log details>

- **Message Code:** 24826

  Severity: DEBUG

  Message Text: Recipient does not match assertion consumption URL

Message Description: Recipient must match assertion consumption URL

Local Target Message Format: <timestamp> <seq_num> 24826 DEBUG External-SAML-IdP: Recipient does not match assertion consumption URL, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24826 DEBUG External-SAML-IdP: Recipient does not match assertion consumption URL, <log details>

- **Message Code:** 24827

  Severity: DEBUG

  Message Text: Subject confirmation data does not contain NotOnOrAfter

  Message Description: Subject confirmation data must contain NotOnOrAfter

  Local Target Message Format: <timestamp> <seq_num> 24827 DEBUG External-SAML-IdP: Subject confirmation data does not contain NotOnOrAfter, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24827 DEBUG External-SAML-IdP: Subject confirmation data does not contain NotOnOrAfter, <log details>

- **Message Code:** 24828

  Severity: DEBUG

  Message Text: Assertion is expired

  Message Description: Assertion is expired

  Local Target Message Format: <timestamp> <seq_num> 24828 DEBUG External-SAML-IdP: Assertion is expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24828 DEBUG External-SAML-IdP: Assertion is expired, <log details>

- **Message Code:** 24829

  Severity: DEBUG

  Message Text: Subject confirmation data IP address does not match end user IP address

  Message Description: Subject confirmation data IP address does not match end user IP address

  Local Target Message Format: <timestamp> <seq_num> 24829 DEBUG External-SAML-IdP: Subject confirmation data IP address does not match end user IP address, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24829 DEBUG External-SAML-IdP: Subject confirmation data IP address does not match end user IP address, <log details>

- **Message Code:** 24830

  Severity: DEBUG

  Message Text: Subject confirmation data does not contain InResponseTo

  Message Description: Subject confirmation data must contain InResponseTo

Local Target Message Format: <timestamp> <seq_num> 24830 DEBUG External-SAML-IdP: Subject confirmation data does not contain InResponseTo, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24830 DEBUG External-SAML-IdP: Subject confirmation data does not contain InResponseTo, <log details>

- **Message Code:** 24831

  Severity: DEBUG

  Message Text: The InResponseTo does not match the original request id

  Message Description: The InResponseTo must match the original request id

  Local Target Message Format: <timestamp> <seq_num> 24831 DEBUG External-SAML-IdP: The InResponseTo does not match the original request id, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24831 DEBUG External-SAML-IdP: The InResponseTo does not match the original request id, <log details>

- **Message Code:** 24832

  Severity: DEBUG

  Message Text: Issuer format is not equal to urn:oasis:names:tc:SAML:2.0:nameid-format:entity

  Message Description: Issuer format must be equal to urn:oasis:names:tc:SAML:2.0:nameid-format:entity

  Local Target Message Format: <timestamp> <seq_num> 24832 DEBUG External-SAML-IdP: Issuer format is not equal to urn:oasis:names:tc:SAML:2.0:nameid-format:entity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24832 DEBUG External-SAML-IdP: Issuer format is not equal to urn:oasis:names:tc:SAML:2.0:nameid-format:entity, <log details>

- **Message Code:** 24833

  Severity: DEBUG

  Message Text: Issuer does not match Identity Provider ID

  Message Description: Issuer does not match Identity Provider ID

  Local Target Message Format: <timestamp> <seq_num> 24833 DEBUG External-SAML-IdP: Issuer does not match Identity Provider ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24833 DEBUG External-SAML-IdP: Issuer does not match Identity Provider ID, <log details>

- **Message Code:** 24834

  Severity: DEBUG

  Message Text: Assertion does not contain subject

  Message Description: Assertion must contain subject

Local Target Message Format: <timestamp> <seq_num> 24834 DEBUG External-SAML-IdP: Assertion does not contain subject, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24834 DEBUG External-SAML-IdP: Assertion does not contain subject, <log details>

- **Message Code:** 24835

  Severity: DEBUG

  Message Text: Assertion does not contain subject confirmation

  Message Description: Assertion must contain subject confirmation

  Local Target Message Format: <timestamp> <seq_num> 24835 DEBUG External-SAML-IdP: Assertion does not contain subject confirmation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24835 DEBUG External-SAML-IdP: Assertion does not contain subject confirmation, <log details>

- **Message Code:** 24836

  Severity: DEBUG

  Message Text: Assertion does not contain bearer subject confirmation

  Message Description: Assertion must contain bearer subject confirmation

  Local Target Message Format: <timestamp> <seq_num> 24836 DEBUG External-SAML-IdP: Assertion does not contain bearer subject confirmation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24836 DEBUG External-SAML-IdP: Assertion does not contain bearer subject confirmation, <log details>

- **Message Code:** 24837

  Severity: DEBUG

  Message Text: The signed response does not contain a Destination

  Message Description: The signed response must contain a Destination

  Local Target Message Format: <timestamp> <seq_num> 24837 DEBUG External-SAML-IdP: The signed response does not contain a Destination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24837 DEBUG External-SAML-IdP: The signed response does not contain a Destination, <log details>

- **Message Code:** 24838

  Severity: DEBUG

  Message Text: The Destination on the response does not match the assertion consumer URL

  Message Description: The Destination on the response must match the assertion consumer URL

Local Target Message Format: <timestamp> <seq_num> 24838 DEBUG External-SAML-IdP: The Destination on the response does not match the assertion consumer URL, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24838 DEBUG External-SAML-IdP: The Destination on the response does not match the assertion consumer URL, <log details>

- **Message Code:** 24839

  Severity: DEBUG

  Message Text: The response does not contain assertion

  Message Description: The response must contain assertion

  Local Target Message Format: <timestamp> <seq_num> 24839 DEBUG External-SAML-IdP: The response does not contain assertion, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24839 DEBUG External-SAML-IdP: The response does not contain assertion, <log details>

- **Message Code:** 24840

  Severity: DEBUG

  Message Text: The response signature is invalid

  Message Description: The response signature is invalid

  Local Target Message Format: <timestamp> <seq_num> 24840 DEBUG External-SAML-IdP: The response signature is invalid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24840 DEBUG External-SAML-IdP: The response signature is invalid, <log details>

- **Message Code:** 24841

  Severity: DEBUG

  Message Text: Response signature did not validate against the IdP signature certificate

  Message Description: Response signature did not validate against the signature certificate configured on SAML Identity Provider in ISE

  Local Target Message Format: <timestamp> <seq_num> 24841 DEBUG External-SAML-IdP: Response signature did not validate against the IdP signature certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24841 DEBUG External-SAML-IdP: Response signature did not validate against the IdP signature certificate, <log details>

- **Message Code:** 24842

  Severity: DEBUG

  Message Text: The assertion signature on the response is invalid

  Message Description: The assertion signature on the response is invalid

Local Target Message Format: <timestamp> <seq_num> 24842 DEBUG External-SAML-IdP: The assertion signature on the response is invalid, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24842 DEBUG External-SAML-IdP: The assertion signature on the response is invalid, <log details>

- **Message Code:** 24843

  Severity: DEBUG

  Message Text: Assertion signature is not not validated against the IdP signature certificate

  Message Description: Assertion signature did not validate against the signature certificate configured on SAML Identity Provider in ISE

  Local Target Message Format: <timestamp> <seq_num> 24843 DEBUG External-SAML-IdP: Assertion signature is not not validated against the IdP signature certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24843 DEBUG External-SAML-IdP: Assertion signature is not not validated against the IdP signature certificate, <log details>

- **Message Code:** 24844

  Severity: DEBUG

  Message Text: Neither SAML response nor assertion are signed

  Message Description: Neither SAML response nor assertion are signed

  Local Target Message Format: <timestamp> <seq_num> 24844 DEBUG External-SAML-IdP: Neither SAML response nor assertion are signed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24844 DEBUG External-SAML-IdP: Neither SAML response nor assertion are signed, <log details>

- **Message Code:** 24845

  Severity: DEBUG

  Message Text: SAML response can contain only one signing certificate

  Message Description: SAML response contains several certificates, can not determine certificate for signature validation

  Local Target Message Format: <timestamp> <seq_num> 24845 DEBUG External-SAML-IdP: SAML response can contain only one signing certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24845 DEBUG External-SAML-IdP: SAML response can contain only one signing certificate, <log details>

- **Message Code:** 24846

  Severity: DEBUG

  Message Text: Several certificates are configured on IdP,however can not determine certificate for signature

Message Description: Several certificates configured on SAML Identity Provider in ISE but SAML response doesn't contain signing certificate. Can not determine certificate for signature validation

Local Target Message Format: <timestamp> <seq_num> 24846 DEBUG External-SAML-IdP: Several certificates are configured on IdP,however can not determine certificate for signature, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24846 DEBUG External-SAML-IdP: Several certificates are configured on IdP,however can not determine certificate for signature, <log details>

- **Message Code:** 24847

  Severity: DEBUG

  Message Text: Certificate is invalid

  Message Description: Certificate is invalid

  Local Target Message Format: <timestamp> <seq_num> 24847 DEBUG External-SAML-IdP: Certificate is invalid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24847 DEBUG External-SAML-IdP: Certificate is invalid, <log details>

- **Message Code:** 24848

  Severity: DEBUG

  Message Text: Failed to get signing certificate from IdP configuration

  Message Description: Unexpected problem with Identity Provider configuration in ISE, Failed to get signing certificate

  Local Target Message Format: <timestamp> <seq_num> 24848 DEBUG External-SAML-IdP: Failed to get signing certificate from IdP configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24848 DEBUG External-SAML-IdP: Failed to get signing certificate from IdP configuration, <log details>

- **Message Code:** 24849

  Severity: DEBUG

  Message Text: Connecting to external ODBC database

  Message Description: ISE is going to establish a new connection to external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24849 DEBUG External-ODBC: Connecting to external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24849 DEBUG External-ODBC: Connecting to external ODBC database, <log details>

- **Message Code:** 24850

  Severity: DEBUG

Message Text: Successfully connected to external ODBC database

Message Description: ISE successfully established a new connection to external ODBC database

Local Target Message Format: <timestamp> <seq_num> 24850 DEBUG External-ODBC: Successfully connected to external ODBC database, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24850 DEBUG External-ODBC: Successfully connected to external ODBC database, <log details>

- **Message Code:** 24851

  Severity: DEBUG

  Message Text: Connection to external ODBC database failed

  Message Description: ISE failed to establish a new connection to external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24851 DEBUG External-ODBC: Connection to external ODBC database failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24851 DEBUG External-ODBC: Connection to external ODBC database failed, <log details>

- **Message Code:** 24852

  Severity: DEBUG

  Message Text: Perform plain text password authentication in external ODBC database

  Message Description: ISE is starting plain text password authentication against the external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24852 DEBUG External-ODBC: Perform plain text password authentication in external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24852 DEBUG External-ODBC: Perform plain text password authentication in external ODBC database, <log details>

- **Message Code:** 24853

  Severity: DEBUG

  Message Text: Plain text password authentication in external ODBC database succeeded

  Message Description: Plain text password authentication in external ODBC database succeeded

  Local Target Message Format: <timestamp> <seq_num> 24853 DEBUG External-ODBC: Plain text password authentication in external ODBC database succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24853 DEBUG External-ODBC: Plain text password authentication in external ODBC database succeeded, <log details>

- **Message Code:** 24854

  Severity: DEBUG

Message Text: Plain text password authentication in external ODBC database failed

Message Description: Plain text password authentication in external ODBC database failed

Local Target Message Format: <timestamp> <seq_num> 24854 DEBUG External-ODBC: Plain text password authentication in external ODBC database failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24854 DEBUG External-ODBC: Plain text password authentication in external ODBC database failed, <log details>

- **Message Code:** 24855

  Severity: DEBUG

  Message Text: Expect external ODBC database stored procedure to return results in a recordset

  Message Description: Expect external ODBC database stored procedure to return results in a recordset

  Local Target Message Format: <timestamp> <seq_num> 24855 DEBUG External-ODBC: Expect external ODBC database stored procedure to return results in a recordset, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24855 DEBUG External-ODBC: Expect external ODBC database stored procedure to return results in a recordset, <log details>

- **Message Code:** 24856

  Severity: DEBUG

  Message Text: Expect external ODBC database stored procedure to return results in output parameters

  Message Description: Expect external ODBC database stored procedure to return results in output parameters

  Local Target Message Format: <timestamp> <seq_num> 24856 DEBUG External-ODBC: Expect external ODBC database stored procedure to return results in output parameters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24856 DEBUG External-ODBC: Expect external ODBC database stored procedure to return results in output parameters, <log details>

- **Message Code:** 24857

  Severity: DEBUG

  Message Text: Failed processing external ODBC database stored procedure results in a returned recordset

  Message Description: Failed processing external ODBC database stored procedure results in a returned recordset

  Local Target Message Format: <timestamp> <seq_num> 24857 DEBUG External-ODBC: Failed processing external ODBC database stored procedure results in a returned recordset, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24857 DEBUG External-ODBC: Failed processing external ODBC database stored procedure results in a returned recordset, <log details>

- **Message Code:** 24858

  Severity: DEBUG

Message Text: Failed processing external ODBC database stored procedure results in a returned output parameters

Message Description: Failed processing external ODBC database stored procedure results in a returned output parameters

Local Target Message Format: <timestamp> <seq_num> 24858 DEBUG External-ODBC: Failed processing external ODBC database stored procedure results in a returned output parameters, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24858 DEBUG External-ODBC: Failed processing external ODBC database stored procedure results in a returned output parameters, <log details>

- **Message Code:** 24859

  Severity: DEBUG

  Message Text: Failed calling external ODBC database stored procedure

  Message Description: ISE failed to call external ODBC database stored procedure configured for specific credential check type

  Local Target Message Format: <timestamp> <seq_num> 24859 DEBUG External-ODBC: Failed calling external ODBC database stored procedure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24859 DEBUG External-ODBC: Failed calling external ODBC database stored procedure, <log details>

- **Message Code:** 24860

  Severity: DEBUG

  Message Text: ODBC database indicated plain text password authentication failure

  Message Description: ODBC database indicated plain text password authentication failure

  Local Target Message Format: <timestamp> <seq_num> 24860 DEBUG External-ODBC: ODBC database indicated plain text password authentication failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24860 DEBUG External-ODBC: ODBC database indicated plain text password authentication failure, <log details>

- **Message Code:** 24861

  Severity: DEBUG

  Message Text: Perform fetch of plain text password from external ODBC database

  Message Description: ISE is starting fetching plain text password from the external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24861 DEBUG External-ODBC: Perform fetch of plain text password from external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24861 DEBUG External-ODBC: Perform fetch of plain text password from external ODBC database, <log details>

- **Message Code:** 24862

  Severity: DEBUG

  Message Text: Fetch plain text password from external ODBC database succeeded

  Message Description: Fetch plain text password from external ODBC database succeeded

  Local Target Message Format: <timestamp> <seq_num> 24862 DEBUG External-ODBC: Fetch plain text password from external ODBC database succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24862 DEBUG External-ODBC: Fetch plain text password from external ODBC database succeeded, <log details>

- **Message Code:** 24863

  Severity: DEBUG

  Message Text: Fetch plain text password from external ODBC database failed

  Message Description: Fetch plain text password from external ODBC database failed

  Local Target Message Format: <timestamp> <seq_num> 24863 DEBUG External-ODBC: Fetch plain text password from external ODBC database failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24863 DEBUG External-ODBC: Fetch plain text password from external ODBC database failed, <log details>

- **Message Code:** 24864

  Severity: DEBUG

  Message Text: ODBC database indicated fetching plain text password failure

  Message Description: ODBC database indicated fetching plain text password failure

  Local Target Message Format: <timestamp> <seq_num> 24864 DEBUG External-ODBC: ODBC database indicated fetching plain text password failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24864 DEBUG External-ODBC: ODBC database indicated fetching plain text password failure, <log details>

- **Message Code:** 24865

  Severity: DEBUG

  Message Text: Perform lookup of the user external ODBC database

  Message Description: ISE is starting lookup of the user the external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24865 DEBUG External-ODBC: Perform lookup of the user external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24865 DEBUG External-ODBC: Perform lookup of the user external ODBC database, <log details>

- **Message Code:** 24866

Severity: DEBUG

Message Text: Lookup of the user in external ODBC database succeeded

Message Description: Lookup of the user in external ODBC database succeede

Local Target Message Format: <timestamp> <seq_num> 24866 DEBUG External-ODBC: Lookup of the user in external ODBC database succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24866 DEBUG External-ODBC: Lookup of the user in external ODBC database succeeded, <log details>

- **Message Code:** 24867

  Severity: DEBUG

  Message Text: Lookup of the user in external ODBC database failed

  Message Description: Lookup of the user in external ODBC database failed

  Local Target Message Format: <timestamp> <seq_num> 24867 DEBUG External-ODBC: Lookup of the user in external ODBC database failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24867 DEBUG External-ODBC: Lookup of the user in external ODBC database failed, <log details>

- **Message Code:** 24868

  Severity: DEBUG

  Message Text: ODBC database indicated user lookup failure

  Message Description: ODBC database indicated user lookup failure

  Local Target Message Format: <timestamp> <seq_num> 24868 DEBUG External-ODBC: ODBC database indicated user lookup failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24868 DEBUG External-ODBC: ODBC database indicated user lookup failure, <log details>

- **Message Code:** 24869

  Severity: DEBUG

  Message Text: Perform fetching of the user groups in external ODBC database

  Message Description: ISE is starting fetching of the user groups in external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24869 DEBUG External-ODBC: Perform fetching of the user groups in external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24869 DEBUG External-ODBC: Perform fetching of the user groups in external ODBC database, <log details>

- **Message Code:** 24870

  Severity: DEBUG

Message Text: Fetching of the user groups in external ODBC database succeeded

Message Description: Fetching of the user groups in external ODBC database succeeded

Local Target Message Format: <timestamp> <seq_num> 24870 DEBUG External-ODBC: Fetching of the user groups in external ODBC database succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24870 DEBUG External-ODBC: Fetching of the user groups in external ODBC database succeeded, <log details>

- **Message Code:** 24871

  Severity: DEBUG

  Message Text: Fetching of the user groups in external ODBC database failed

  Message Description: Fetching of the user groups in external ODBC database failed

  Local Target Message Format: <timestamp> <seq_num> 24871 DEBUG External-ODBC: Fetching of the user groups in external ODBC database failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24871 DEBUG External-ODBC: Fetching of the user groups in external ODBC database failed, <log details>

- **Message Code:** 24872

  Severity: DEBUG

  Message Text: Perform fetching of the user attributes in external ODBC database

  Message Description: ISE is starting fetching of the user attributes in external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24872 DEBUG External-ODBC: Perform fetching of the user attributes in external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24872 DEBUG External-ODBC: Perform fetching of the user attributes in external ODBC database, <log details>

- **Message Code:** 24873

  Severity: DEBUG

  Message Text: Fetching of the user attributes in external ODBC database succeeded

  Message Description: Fetching of the user attributes in external ODBC database succeeded

  Local Target Message Format: <timestamp> <seq_num> 24873 DEBUG External-ODBC: Fetching of the user attributes in external ODBC database succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24873 DEBUG External-ODBC: Fetching of the user attributes in external ODBC database succeeded, <log details>

- **Message Code:** 24874

  Severity: DEBUG

  Message Text: Fetching of the user attributes in external ODBC database failed

Message Description: Fetching of the user attributes in external ODBC database failed

Local Target Message Format: <timestamp> <seq_num> 24874 DEBUG External-ODBC: Fetching of the user attributes in external ODBC database failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24874 DEBUG External-ODBC: Fetching of the user attributes in external ODBC database failed, <log details>

- **Message Code:** 24875

  Severity: DEBUG

  Message Text: Faied to process results of fetching of the user attributes from external ODBC database

  Message Description: Faied to process results of fetching of the user attributes from external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24875 DEBUG External-ODBC: Faied to process results of fetching of the user attributes from external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24875 DEBUG External-ODBC: Faied to process results of fetching of the user attributes from external ODBC database, <log details>

- **Message Code:** 24876

  Severity: DEBUG

  Message Text: Faied to process results of fetching of the user groups from external ODBC database

  Message Description: Faied to process results of fetching of the user groups from external ODBC database

  Local Target Message Format: <timestamp> <seq_num> 24876 DEBUG External-ODBC: Faied to process results of fetching of the user groups from external ODBC database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24876 DEBUG External-ODBC: Faied to process results of fetching of the user groups from external ODBC database, <log details>

- **Message Code:** 24877

  Severity: INFO

  Message Text: Subject formats persistent or transient are not supported as Identity Attribute

  Message Description: Subject format in assertions is persistent or transient. These formats are not supported as Identity Attribute

  Local Target Message Format: <timestamp> <seq_num> 24877 INFO External-SAML-IdP: Subject formats persistent or transient are not supported as Identity Attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24877 INFO External-SAML-IdP: Subject formats persistent or transient are not supported as Identity Attribute, <log details>

- **Message Code:** 24878

  Severity: DEBUG

Message Text: Retry failed ODBC operation

Message Description: Previous ODBC operation failed and retry is possible. Pefrom the next retry

Local Target Message Format: <timestamp> <seq_num> 24878 DEBUG External-ODBC: Retry failed ODBC operation, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24878 DEBUG External-ODBC: Retry failed ODBC operation, <log details>

- **Message Code:** 24879

  Severity: INFO

  Message Text: Identity provider metadata is not set

  Message Description: Identity provider metadata is not loaded

  Local Target Message Format: <timestamp> <seq_num> 24879 INFO External-SAML-IdP: Identity provider metadata is not set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24879 INFO External-SAML-IdP: Identity provider metadata is not set, <log details>

- **Message Code:** 24880

  Severity: WARN

  Message Text: ODBC operation failed due to timeout elapsed

  Message Description: ODBC operation failed due to timeout elapsed

  Local Target Message Format: <timestamp> <seq_num> 24880 WARN External-ODBC: ODBC operation failed due to timeout elapsed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24880 WARN External-ODBC: ODBC operation failed due to timeout elapsed, <log details>

- **Message Code:** 24890

  Severity: WARN

  Message Text: Social Login operation failed

  Message Description: Social Login operation failed. Check the message details for more information

  Local Target Message Format: <timestamp> <seq_num> 24890 WARN External-Social-Login: Social Login operation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 24890 WARN External-Social-Login: Social Login operation failed, <log details>

- **Message Code:** 24716

  Severity: INFO

  Message Text: Active Directory Kerberos ticket authentication succeeded

Message Description: Active Directory Kerberos ticket authentication succeeded

Local Target Message Format: <timestamp> <seq_num>24716 INFO External-Active-Directory Active Directory Kerberos ticket authentication succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24716 INFO External-Active-Directory Active Directory Kerberos ticket authentication succeeded, <log details>

- **Message Code:** 24717

  Severity: ERROR

  Message Text: Active Directory Kerberos ticket authentication failed

  Message Description: Active Directory Kerberos ticket authentication failed

  Local Target Message Format: <timestamp> <seq_num>24717 ERROR External-Active-Directory Active Directory Kerberos ticket authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24717 ERROR External-Active-Directory Active Directory Kerberos ticket authentication failed, <log details>

- **Message Code:** 24718

  Severity: ERROR

  Message Text: Active Directory Kerberos ticket expired

  Message Description: Active Directory Kerberos ticket expired

  Local Target Message Format: <timestamp> <seq_num>24718 ERROR External-Active-Directory Active Directory Kerberos ticket expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24718 ERROR External-Active-Directory Active Directory Kerberos ticket expired, <log details>

- **Message Code:** 24719

  Severity: DEBUG

  Message Text: Active Directory Kerberos ticket authentication failed because of the ISE account password mismatch, integrity check failure or expired ticket

  Message Description: Active Directory Kerberos ticket authentication failed because of the ISE account password mismatch, integrity check failure or expired ticket

  Local Target Message Format: <timestamp> <seq_num>24719 DEBUG External-Active-Directory Active Directory Kerberos ticket authentication failed because of the ISE account password mismatch, integrity check failure or expired ticket, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24719 DEBUG External-Active-Directory Active Directory Kerberos ticket authentication failed because of the ISE account password mismatch, integrity check failure or expired ticket, <log details>

- **Message Code:** 24900

Severity: ERROR

Message Text: Loading LDAP ID Store failed because of an unknown or missing CA for primary or secondary connection

Message Description: nan

Local Target Message Format: <timestamp> <seq_num>24900 ERROR ID-Stores-Configuration Loading LDAP ID Store failed because of an unknown or missing CA for primary or secondary connection, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24900 ERROR ID-Stores-Configuration Loading LDAP ID Store failed because of an unknown or missing CA for primary or secondary connection, <log details>

- **Message Code:** 24901

  Severity: ERROR

  Message Text: Loading ID Store Sequence failed because of missing or corrupted ID Store

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>24901 ERROR ID-Stores-Configuration Loading ID Store Sequence failed because of missing or corrupted ID Store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24901 ERROR ID-Stores-Configuration Loading ID Store Sequence failed because of missing or corrupted ID Store, <log details>

- **Message Code:** 24910

  Severity: DEBUG

  Message Text: OIDC session context was successfully created.

  Message Description: OIDC session context was successfully created and saved to ignite cache.

  Local Target Message Format: <timestamp> <seq_num>24910 DEBUG External-OIDC OIDC session context was successfully created., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24910 DEBUG External-OIDC OIDC session context was successfully created., <log details>

- **Message Code:** 24911

  Severity: WARNING

  Message Text: Failed to create OIDC session context.

  Message Description: Failed to create OIDC session context.

  Local Target Message Format: <timestamp> <seq_num>24911 WARNING External-OIDC Failed to create OIDC session context., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24911 WARNING External-OIDC Failed to create OIDC session context., <log details>

- **Message Code:** 24912

  Severity: DEBUG

  Message Text: OIDC access token was successfully refreshed.

  Message Description: OIDC access token was successfully refreshed.

  Local Target Message Format: <timestamp> <seq_num>24912 DEBUG External-OIDC OIDC access token was successfully refreshed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24912 DEBUG External-OIDC OIDC access token was successfully refreshed., <log details>

- **Message Code:** 24913

  Severity: DEBUG

  Message Text: Failed to refresh OIDC access token. OIDC session context was deleted.

  Message Description: Failed to refresh OIDC access token. OIDC session context was deleted.

  Local Target Message Format: <timestamp> <seq_num>24913 DEBUG External-OIDC Failed to refresh OIDC access token. OIDC session context was deleted., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24913 DEBUG External-OIDC Failed to refresh OIDC access token. OIDC session context was deleted., <log details>

- **Message Code:** 24914

  Severity: DEBUG

  Message Text: OIDC session context was successfully updated.

  Message Description: OIDC session context was successfully updated.

  Local Target Message Format: <timestamp> <seq_num>24914 DEBUG External-OIDC OIDC session context was successfully updated., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24914 DEBUG External-OIDC OIDC session context was successfully updated., <log details>

- **Message Code:** 24915

  Severity: DEBUG

  Message Text: Failed to update OIDC session context. OIDC session context was deleted.

  Message Description: Failed to update OIDC session context. OIDC session context was deleted.

  Local Target Message Format: <timestamp> <seq_num>24915 DEBUG External-OIDC Failed to update OIDC session context. OIDC session context was deleted., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24915 DEBUG External-OIDC Failed to update OIDC session context. OIDC session context was deleted., <log details>

- **Message Code:** 24916

Severity: INFO

Message Text: Expired OIDC sessions deleted.

Message Description: Expired OIDC sessions deleted.

Local Target Message Format: <timestamp> <seq_num>24916 INFO External-OIDC Expired OIDC sessions deleted., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24916 INFO External-OIDC Expired OIDC sessions deleted., <log details>

- **Message Code:** 24917

  Severity: ERROR

  Message Text: Failed to delete expired OIDC sessions.

  Message Description: Failed to delete expired OIDC sessions.

  Local Target Message Format: <timestamp> <seq_num>24917 ERROR External-OIDC Failed to delete expired OIDC sessions., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24917 ERROR External-OIDC Failed to delete expired OIDC sessions., <log details>

- **Message Code:** 24918

  Severity: DEBUG

  Message Text: IDP attribute or group change detected. OIDC session context was deleted and CoA was issued.

  Message Description: IDP attribute or group change detected. OIDC session context was deleted and CoA was issued.

  Local Target Message Format: <timestamp> <seq_num>24918 DEBUG External-OIDC IDP attribute or group change detected. OIDC session context was deleted and CoA was issued., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24918 DEBUG External-OIDC IDP attribute or group change detected. OIDC session context was deleted and CoA was issued., <log details>

- **Message Code:** 24919

  Severity: WARNING

  Message Text: IDP attribute or group change detected. Failed to delete OIDC session context. CoA was issued.

  Message Description: IDP attribute or group change detected. Failed to delete OIDC session context. CoA was issued.

  Local Target Message Format: <timestamp> <seq_num>24919 WARNING External-OIDC IDP attribute or group change detected. Failed to delete OIDC session context. CoA was issued., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24919 WARNING External-OIDC

IDP attribute or group change detected. Failed to delete OIDC session context. CoA was issued., <log details>

- **Message Code:** 24920

  Severity: WARNING

  Message Text: IDP attribute or group change detected. OIDC session context was deleted. Failed to issue CoA.

  Message Description: IDP attribute or group change detected. OIDC session context was deleted. Failed to issue CoA.

  Local Target Message Format: <timestamp> <seq_num>24920 WARNING External-OIDC IDP attribute or group change detected. OIDC session context was deleted. Failed to issue CoA., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24920 WARNING External-OIDC IDP attribute or group change detected. OIDC session context was deleted. Failed to issue CoA., <log details>

- **Message Code:** 24921

  Severity: ERROR

  Message Text: OIDC sessions context cache is not available.

  Message Description: OIDC sessions context cache is not available.

  Local Target Message Format: <timestamp> <seq_num>24921 ERROR External-OIDC OIDC sessions context cache is not available., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24921 ERROR External-OIDC OIDC sessions context cache is not available., <log details>

- **Message Code:** 24922

  Severity: ERROR

  Message Text: OIDC IDP configuration not found in the database.

  Message Description: OIDC IDP configuration not found in the database.

  Local Target Message Format: <timestamp> <seq_num>24922 ERROR External-OIDC OIDC IDP configuration not found in the database., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24922 ERROR External-OIDC OIDC IDP configuration not found in the database., <log details>

- **Message Code:** 24797

  Severity: WARN

  Message Text: Signed assertion is required by ISE configuration but SAML assertion is not signed

  Message Description: Signed assertion is required by ISE configuration but SAML assertion is not signed

Local Target Message Format: <timestamp> <seq_num>24797 WARN External-SAML-IdP Signed assertion is required by ISE configuration but SAML assertion is not signed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24797 WARN External-SAML-IdP Signed assertion is required by ISE configuration but SAML assertion is not signed, <log details>

- **Message Code:** 24798

  Severity: WARN

  Message Text: Signed response is required by ISE configuration but SAML response is not signed

  Message Description: Signed response is required by ISE configuration but SAML response is not signed

  Local Target Message Format: <timestamp> <seq_num>24798 WARN External-SAML-IdP Signed response is required by ISE configuration but SAML response is not signed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24798 WARN External-SAML-IdP Signed response is required by ISE configuration but SAML response is not signed, <log details>

- **Message Code:** 24799

  Severity: WARN

  Message Text: Encrypted assertion is required by ISE configuration but SAML assertion is not encrypted

  Message Description: Encrypted assertion is required by ISE configuration but SAML assertion is not encrypted

  Local Target Message Format: <timestamp> <seq_num>24799 WARN External-SAML-IdP Encrypted assertion is required by ISE configuration but SAML assertion is not encrypted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>24799 WARN External-SAML-IdP Encrypted assertion is required by ISE configuration but SAML assertion is not encrypted, <log details>

- **Message Code:** 24045

  Severity: ERROR

  Message Text: Secure LDAP connection failed because server certificate is revoked

  Message Description: Secure LDAP connection failed because server certificate is revoked.

  Local Target Message Format: <timestamp> <seq_num>External-LDAP Secure LDAP connection failed because server certificate is revoked ERROR Secure LDAP connection failed because server certificate is revoked., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>External-LDAP Secure LDAP connection failed because server certificate is revoked ERROR Secure LDAP connection failed because server certificate is revoked., <log details>

- **Message Code:** 24046

  Severity: ERROR

Message Text: Secure LDAP connection failed because it was unable to download CRL for the CA that signed server certificate

Message Description: Secure LDAP connection failed because it was unable to download CRL for the CA that signed server certificate

Local Target Message Format: <timestamp> <seq_num>External-LDAP Secure LDAP connection failed because it was unable to download CRL for the CA that signed server certificate ERROR Secure LDAP connection failed because it was unable to download CRL for the CA that signed server certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>External-LDAP Secure LDAP connection failed because it was unable to download CRL for the CA that signed server certificate ERROR Secure LDAP connection failed because it was unable to download CRL for the CA that signed server certificate, <log details>

- **Message Code:** 24047

  Severity: ERROR

  Message Text: Secure LDAP connection failed because server certificate is rejected

  Message Description: Secure LDAP connection failed because server certificate is rejected

  Local Target Message Format: <timestamp> <seq_num>External-LDAP Secure LDAP connection failed because server certificate is rejected ERROR Secure LDAP connection failed because server certificate is rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>External-LDAP Secure LDAP connection failed because server certificate is rejected ERROR Secure LDAP connection failed because server certificate is rejected, <log details>

Internal MDM

- **Message Code:** 89050

  Severity: INFO

  Message Text: Administrative action submitted

  Message Description: An administrative action (of given type) has been submitted

  Local Target Message Format: <timestamp> <seq_num> 89050 INFO MDM: Administrative action submitted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89050 INFO MDM: Administrative action submitted, <log details>

- **Message Code:** 89051

  Severity: INFO

  Message Text: Administrative action delivered to mobile device

Message Description: Indicates that the mobile device has acknowledged the administrative action (of given type)

Local Target Message Format: <timestamp> <seq_num> 89051 INFO MDM: Administrative action delivered to mobile device, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89051 INFO MDM: Administrative action delivered to mobile device, <log details>

- **Message Code:** 89052

  Severity: ERROR

  Message Text: Administrative action failed

  Message Description: Indicates that the mobile device has failed the administrative action (of given type)

  Local Target Message Format: <timestamp> <seq_num> 89052 ERROR MDM: Administrative action failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89052 ERROR MDM: Administrative action failed, <log details>

- **Message Code:** 89100

  Severity: INFO

  Message Text: Mobile device enrollment initiated

  Message Description: Indicates that the Mobile Device enrollment has started

  Local Target Message Format: <timestamp> <seq_num> 89100 INFO MDM: Mobile device enrollment initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89100 INFO MDM: Mobile device enrollment initiated, <log details>

- **Message Code:** 89101

  Severity: ERROR

  Message Text: Mobile device enrollment failed

  Message Description: Mobile device enrollment terminated due to a reason

  Local Target Message Format: <timestamp> <seq_num> 89101 ERROR MDM: Mobile device enrollment failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89101 ERROR MDM: Mobile device enrollment failed, <log details>

- **Message Code:** 89102

  Severity: INFO

  Message Text: Mobile device enrolled successfully

Message Description: Mobile Device is successfully enrolled

Local Target Message Format: <timestamp> <seq_num> 89102 INFO MDM: Mobile device enrolled successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89102 INFO MDM: Mobile device enrolled successfully, <log details>

- **Message Code:** 89103

  Severity: INFO

  Message Text: Mobile device deregistered

  Message Description: Unenrollment of a Mobile Device has completed

  Local Target Message Format: <timestamp> <seq_num> 89103 INFO MDM: Mobile device deregistered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89103 INFO MDM: Mobile device deregistered, <log details>

- **Message Code:** 89104

  Severity: INFO

  Message Text: Mobile Device Service initialized

  Message Description: Mobile Device Service initialization is completed

  Local Target Message Format: <timestamp> <seq_num> 89104 INFO MDM: Mobile Device Service initialized, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89104 INFO MDM: Mobile Device Service initialized, <log details>

- **Message Code:** 89105

  Severity: ERROR

  Message Text: Mobile Device Service initialization failed

  Message Description: Mobile Device Service is unable to start

  Local Target Message Format: <timestamp> <seq_num> 89105 ERROR MDM: Mobile Device Service initialization failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89105 ERROR MDM: Mobile Device Service initialization failed, <log details>

- **Message Code:** 89106

  Severity: INFO

  Message Text: Mobile Device Service stopped

  Message Description: Mobile Device Service is terminated

Local Target Message Format: <timestamp> <seq_num> 89106 INFO MDM: Mobile Device Service stopped, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89106 INFO MDM: Mobile Device Service stopped, <log details>

- **Message Code:** 89107

  Severity: ERROR

  Message Text: Unable to send notifications to mobile device

  Message Description: Indicates failures to notify mobile devices via Push Notification Systems

  Local Target Message Format: <timestamp> <seq_num> 89107 ERROR MDM: Unable to send notifications to mobile device, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89107 ERROR MDM: Unable to send notifications to mobile device, <log details>

- **Message Code:** 89108

  Severity: WARN

  Message Text: APNS Certificate is about to expire

  Message Description: Indicates that the APNS Certificate used for Notification services is about to expire soon

  Local Target Message Format: <timestamp> <seq_num> 89108 WARN MDM: APNS Certificate is about to expire, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89108 WARN MDM: APNS Certificate is about to expire, <log details>

- **Message Code:** 89109

  Severity: WARN

  Message Text: Endpoint certificate is going to expire soon.

  Message Description: Indicates that an endpoint certificate used for MDM operations is about to expire soon, within 1/2 of the configured renewal period, suggesting that its automatic renewal had previously failed.

  Local Target Message Format: <timestamp> <seq_num> 89109 WARN MDM: Endpoint certificate is going to expire soon., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89109 WARN MDM: Endpoint certificate is going to expire soon., <log details>

- **Message Code:** 89110

  Severity: ERROR

  Message Text: Mobile Device check-in request is not authorized.

Message Description: Indicates that the Mobile Device check-in request has not been authorized due to unknown/revoked/expired client certificate.

Local Target Message Format: <timestamp> <seq_num> 89110 ERROR MDM: Mobile Device check-in request is not authorized., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89110 ERROR MDM: Mobile Device check-in request is not authorized., <log details>

- **Message Code:** 89111

  Severity: INFO

  Message Text: Mobile Device check-in request is authorized.

  Message Description: Indicates that the Mobile Device check-in request has been authorized.

  Local Target Message Format: <timestamp> <seq_num> 89111 INFO MDM: Mobile Device check-in request is authorized., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89111 INFO MDM: Mobile Device check-in request is authorized., <log details>

- **Message Code:** 89112

  Severity: INFO

  Message Text: Endpoint certificate is renewed.

  Message Description: Indicates that an endpoint certificate used for MDM operations is renewed.

  Local Target Message Format: <timestamp> <seq_num> 89112 INFO MDM: Endpoint certificate is renewed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89112 INFO MDM: Endpoint certificate is renewed., <log details>

- **Message Code:** 89113

  Severity: WARN

  Message Text: Inactive Mobile Device is detected

  Message Description: Indicates the mobile device is no longer active and possibly unenrolled

  Local Target Message Format: <timestamp> <seq_num> 89113 WARN MDM: Inactive Mobile Device is detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89113 WARN MDM: Inactive Mobile Device is detected, <log details>

- **Message Code:** 89114

  Severity: INFO

  Message Text: GeoLocation coordinates received

Message Description: Indicates that the mobile device has responded with geolocation coordinates

Local Target Message Format: <timestamp> <seq_num> 89114 INFO MDM: GeoLocation coordinates received, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89114 INFO MDM: GeoLocation coordinates received, <log details>

- **Message Code:** 89115

  Severity: INFO

  Message Text: Profile Installed

  Message Description: Indicates that the mobile device has installed a profile. Profile information is provided in event details attribute

  Local Target Message Format: <timestamp> <seq_num> 89115 INFO MDM: Profile Installed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89115 INFO MDM: Profile Installed, <log details>

- **Message Code:** 89116

  Severity: INFO

  Message Text: Profile Removed

  Message Description: Indicates that the mobile device has removed a profile. Profile information is provided in event details attribute

  Local Target Message Format: <timestamp> <seq_num> 89116 INFO MDM: Profile Removed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89116 INFO MDM: Profile Removed, <log details>

- **Message Code:** 89117

  Severity: INFO

  Message Text: Application Installed

  Message Description: Indicates that the mobile device has installed an application. Application information is provided in event details attribute

  Local Target Message Format: <timestamp> <seq_num> 89117 INFO MDM: Application Installed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89117 INFO MDM: Application Installed, <log details>

- **Message Code:** 89118

  Severity: INFO

Message Text: Application Removed

Message Description: Indicates that the mobile device has removed an application. Application information is provided in event details attribute

Local Target Message Format: <timestamp> <seq_num> 89118 INFO MDM: Application Removed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89118 INFO MDM: Application Removed, <log details>

- **Message Code:** 89119

  Severity: WARN

  Message Text: Device reassessment has failed.

  Message Description: Indicates that periodic, administrator or user initiated device reassessment has failed. The event details include the failure reason.

  Local Target Message Format: <timestamp> <seq_num> 89119 WARN MDM: Device reassessment has failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89119 WARN MDM: Device reassessment has failed., <log details>

- **Message Code:** 89132

  Severity: WARN

  Message Text: Endpoint certificate is going to expire soon.

  Message Description: Indicates that an endpoint certificate used for MDM operations is about to expire soon, within 1/4 of the configured renewal period, suggesting that its automatic renewal according to the configured renewal period had previously failed.

  Local Target Message Format: <timestamp> <seq_num> 89132 WARN MDM: Endpoint certificate is going to expire soon., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89132 WARN MDM: Endpoint certificate is going to expire soon., <log details>

- **Message Code:** 89133

  Severity: ERROR

  Message Text: Endpoint certificate has expired.

  Message Description: Indicates that an endpoint certificate used for MDM operations has expired. The mobile device must be re-enrolled.

  Local Target Message Format: <timestamp> <seq_num> 89133 ERROR MDM: Endpoint certificate has expired., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89133 ERROR MDM: Endpoint certificate has expired., <log details>

- **Message Code:** 89142

  Severity: ERROR

  Message Text: Provisioning operation failed.

  Message Description: Indicates that a provisioning operation (profile/application) has failed. Profile/Application information and the failure reason is provided in the event details.

  Local Target Message Format: <timestamp> <seq_num> 89142 ERROR MDM: Provisioning operation failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89142 ERROR MDM: Provisioning operation failed., <log details>

- **Message Code:** 89143

  Severity: INFO

  Message Text: Mobile device record is updated with new device information

  Message Description: Indicates that the mobile device information (OS version, AnyConnect version, etc) has been retrieved and the database record is updated. The updated information is provided in the event details.

  Local Target Message Format: <timestamp> <seq_num> 89143 INFO MDM: Mobile device record is updated with new device information, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89143 INFO MDM: Mobile device record is updated with new device information, <log details>

- **Message Code:** 89144

  Severity: WARN

  Message Text: Endpoint certificate renewal has failed.

  Message Description: Indicates that renewal of an endpoint certificate used for MDM operations has failed. Certificate renewal will be reattempted during the next periodic reassessment.

  Local Target Message Format: <timestamp> <seq_num> 89144 WARN MDM: Endpoint certificate renewal has failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89144 WARN MDM: Endpoint certificate renewal has failed., <log details>

- **Message Code:** 89149

  Severity: INFO

  Message Text: Mobile device is compliant

  Message Description: Indicates the device is compliant with mobile device management policies

  Local Target Message Format: <timestamp> <seq_num> 89149 INFO MDM: Mobile device is compliant, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89149 INFO MDM: Mobile device is compliant, <log details>

- **Message Code:** 89150

  Severity: INFO

  Message Text: Mobile device is not compliant

  Message Description: Indicates the device is not compliant with mobile device management policies

  Local Target Message Format: <timestamp> <seq_num> 89150 INFO MDM: Mobile device is not compliant, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89150 INFO MDM: Mobile device is not compliant, <log details>

- **Message Code:** 89151

  Severity: WARN

  Message Text: Certificate issued by external CA can be revoked because the mobile device no longer uses it.

  Message Description: Indicates that a client certificate generated by an external CA is no longer needed on the mobile device. It can be manually revoked for additional security.

  Local Target Message Format: <timestamp> <seq_num> 89151 WARN MDM: Certificate issued by external CA can be revoked because the mobile device no longer uses it., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89151 WARN MDM: Certificate issued by external CA can be revoked because the mobile device no longer uses it., <log details>

- **Message Code:** 89152

  Severity: INFO

  Message Text: Mobile device unenrollment initiated

  Message Description: Indicates that the Mobile Device unenrollment has started

  Local Target Message Format: <timestamp> <seq_num> 89152 INFO MDM: Mobile device unenrollment initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89152 INFO MDM: Mobile device unenrollment initiated, <log details>

- **Message Code:** 89153

  Severity: ERROR

  Message Text: Certificates missing for Notification Systems.

  Message Description: Indicates that one or more identity certificates required for authenticating ISE to Mobile Device Notification Systems have not been configured.

Local Target Message Format: <timestamp> <seq_num> 89153 ERROR MDM: Certificates missing for Notification Systems., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89153 ERROR MDM: Certificates missing for Notification Systems., <log details>

- **Message Code:** 89154

  Severity: ERROR

  Message Text: Apple Volume Purchase Plan (VPP) service token is invalid.

  Message Description: Indicates that service token for Apple Volume Purchase Plan (VPP) is invalid.

  Local Target Message Format: <timestamp> <seq_num> 89154 ERROR MDM: Apple Volume Purchase Plan (VPP) service token is invalid., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89154 ERROR MDM: Apple Volume Purchase Plan (VPP) service token is invalid., <log details>

- **Message Code:** 89155

  Severity: ERROR

  Message Text: Failed to access Apple Volume Purchase Plan (VPP) services.

  Message Description: Errors encountered accessing Apple Volume Purchase Plan (VPP) service. More information is provided in the event details.

  Local Target Message Format: <timestamp> <seq_num> 89155 ERROR MDM: Failed to access Apple Volume Purchase Plan (VPP) services., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89155 ERROR MDM: Failed to access Apple Volume Purchase Plan (VPP) services., <log details>

- **Message Code:** 89156

  Severity: ERROR

  Message Text: CMCS server unreachable

  Message Description: ISE is unable to communicate with the Cisco MDM Cloud Service

  Local Target Message Format: <timestamp> <seq_num> 89156 ERROR MDM: CMCS server unreachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89156 ERROR MDM: CMCS server unreachable, <log details>

- **Message Code:** 89157

  Severity: ERROR

  Message Text: CMCS authentication failure

  Message Description: ISE is unable to authenticate with the Cisco MDM Cloud Service

Local Target Message Format: <timestamp> <seq_num> 89157 ERROR MDM: CMCS authentication failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89157 ERROR MDM: CMCS authentication failure, <log details>

- **Message Code:** 89158

  Severity: ERROR

  Message Text: APNS server unreachable

  Message Description: ISE is unable to communicate with the Apple Push Notification System (APNS)

  Local Target Message Format: <timestamp> <seq_num> 89158 ERROR MDM: APNS server unreachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89158 ERROR MDM: APNS server unreachable, <log details>

- **Message Code:** 89159

  Severity: ERROR

  Message Text: APNS authentication failure

  Message Description: ISE is unable to authenticate with the Apple Push Notification System (APNS)

  Local Target Message Format: <timestamp> <seq_num> 89159 ERROR MDM: APNS authentication failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89159 ERROR MDM: APNS authentication failure, <log details>

- **Message Code:** 89160

  Severity: INFO

  Message Text: MDM User Authentication completed

  Message Description: The User Authentication part of mobile device enrollment has completed

  Local Target Message Format: <timestamp> <seq_num> 89160 INFO MDM: MDM User Authentication completed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89160 INFO MDM: MDM User Authentication completed, <log details>

Internal Operations Diagnostics

- **Message Code:** 30000

  Severity: FATAL

Message Text: Unknown fatal management error

Message Description: MGMT fatal unknown error.To recover try to re-run ISE

Local Target Message Format: <timestamp> <seq_num> 30000 FATAL MGMT: Unknown fatal management error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 30000 FATAL MGMT: Unknown fatal management error, <log details>

- **Message Code:** 31000

  Severity: ERROR

  Message Text: Could not initialize notification dispatcher

  Message Description: Could not initialize notification dispatcher

  Local Target Message Format: <timestamp> <seq_num> 31000 ERROR Notification-Dispatcher: Could not initialize notification dispatcher, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31000 ERROR Notification-Dispatcher: Could not initialize notification dispatcher, <log details>

- **Message Code:** 31001

  Severity: ERROR

  Message Text: Could not send configuration notification message

  Message Description: Could not send configuration notification message

  Local Target Message Format: <timestamp> <seq_num> 31001 ERROR Notification-Dispatcher: Could not send configuration notification message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31001 ERROR Notification-Dispatcher: Could not send configuration notification message, <log details>

- **Message Code:** 31100

  Severity: DEBUG

  Message Text: Applying configuration changes initiated

  Message Description: Applying configuration changes in Runtime initiated

  Local Target Message Format: <timestamp> <seq_num> 31100 DEBUG Configuration-Notifications: Applying configuration changes initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31100 DEBUG Configuration-Notifications: Applying configuration changes initiated, <log details>

- **Message Code:** 31101

  Severity: DEBUG

  Message Text: Applying configuration changes succeeded

Message Description: Applying configuration changes in Runtime succeeded. A new configuration version was activated

Local Target Message Format: <timestamp> <seq_num> 31101 DEBUG Configuration-Notifications: Applying configuration changes succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31101 DEBUG Configuration-Notifications: Applying configuration changes succeeded, <log details>

- **Message Code:** 31102

  Severity: FATAL

  Message Text: Applying configuration changes failed

  Message Description: Applying configuration changes failed. Runtime process will restart.

  Local Target Message Format: <timestamp> <seq_num> 31102 FATAL Configuration-Notifications: Applying configuration changes failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31102 FATAL Configuration-Notifications: Applying configuration changes failed, <log details>

- **Message Code:** 31103

  Severity: DEBUG

  Message Text: Start up configuration load succeeded

  Message Description: Start up configuration load succeeded

  Local Target Message Format: <timestamp> <seq_num> 31103 DEBUG Configuration-Notifications: Start up configuration load succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31103 DEBUG Configuration-Notifications: Start up configuration load succeeded, <log details>

- **Message Code:** 31104

  Severity: FATAL

  Message Text: Start up configuration load failed

  Message Description: Start up configuration load failed. Runtime process will go down

  Local Target Message Format: <timestamp> <seq_num> 31104 FATAL Configuration-Notifications: Start up configuration load failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31104 FATAL Configuration-Notifications: Start up configuration load failed, <log details>

- **Message Code:** 31105

  Severity: WARN

  Message Text: Transaction is ignored

Message Description: A transaction with wrong ID is ignored. Runtime is waiting for transaction with another ID.

Local Target Message Format: <timestamp> <seq_num> 31105 WARN Configuration-Notifications: Transaction is ignored, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31105 WARN Configuration-Notifications: Transaction is ignored, <log details>

- **Message Code:** 31106

  Severity: FATAL

  Message Text: Configuration management could not translate configuration change. Runtime configuration changes will not take effect

  Message Description: Configuration management could not translate configuration change. Runtime configuration changes will not take effect

  Local Target Message Format: <timestamp> <seq_num> 31106 FATAL Configuration-Notifications: Configuration management could not translate configuration change. Runtime configuration changes will not take effect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31106 FATAL Configuration-Notifications: Configuration management could not translate configuration change. Runtime configuration changes will not take effect, <log details>

- **Message Code:** 31107

  Severity: INFO

  Message Text: Cold configuration restart complete

  Message Description: Cold configuration restart complete

  Local Target Message Format: <timestamp> <seq_num> 31107 INFO Configuration-Notifications: Cold configuration restart complete, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31107 INFO Configuration-Notifications: Cold configuration restart complete, <log details>

- **Message Code:** 31108

  Severity: FATAL

  Message Text: Cold configuration restart failed

  Message Description: Cold configuration restart failed. Runtime process will restart.

  Local Target Message Format: <timestamp> <seq_num> 31108 FATAL Configuration-Notifications: Cold configuration restart failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31108 FATAL Configuration-Notifications: Cold configuration restart failed, <log details>

- **Message Code:** 31109

Severity: INFO

Message Text: Warm configuration restart complete

Message Description: Warm configuration restart complete

Local Target Message Format: <timestamp> <seq_num> 31109 INFO Configuration-Notifications: Warm configuration restart complete, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31109 INFO Configuration-Notifications: Warm configuration restart complete, <log details>

- **Message Code:** 31110

  Severity: WARN

  Message Text: Warm configuration restart failed

  Message Description: Warm configuration restart failed. Falling back to the cold configuration restart

  Local Target Message Format: <timestamp> <seq_num> 31110 WARN Configuration-Notifications: Warm configuration restart failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31110 WARN Configuration-Notifications: Warm configuration restart failed, <log details>

- **Message Code:** 31111

  Severity: WARN

  Message Text: The Runtime notifications are out of sync

  Message Description: The Runtime notifications are out of sync. Issuing a sync message to Management.

  Local Target Message Format: <timestamp> <seq_num> 31111 WARN Configuration-Notifications: The Runtime notifications are out of sync, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31111 WARN Configuration-Notifications: The Runtime notifications are out of sync, <log details>

- **Message Code:** 31200

  Severity: ERROR

  Message Text: Encountered invalid/Null Log Record encountered

  Message Description: Invalid or null log record

  Local Target Message Format: <timestamp> <seq_num> 31200 ERROR Audit-Flow: Encountered invalid/Null Log Record encountered, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31200 ERROR Audit-Flow: Encountered invalid/Null Log Record encountered, <log details>

- **Message Code:** 31201

  Severity: ERROR

Message Text: Encountered invalid or null system message

Message Description: Could not create corresponding system message from opcode

Local Target Message Format: <timestamp> <seq_num> 31201 ERROR Audit-Flow: Encountered invalid or null system message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31201 ERROR Audit-Flow: Encountered invalid or null system message, <log details>

- **Message Code:** 31202

  Severity: ERROR

  Message Text: Encountered invalid or null user context

  Message Description: Encountered invalid or null user context

  Local Target Message Format: <timestamp> <seq_num> 31202 ERROR Audit-Flow: Encountered invalid or null user context, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31202 ERROR Audit-Flow: Encountered invalid or null user context, <log details>

- **Message Code:** 31203

  Severity: ERROR

  Message Text: Encountered error while recording the audit record for successful login

  Message Description: Encountered error while recording the audit record for successful login

  Local Target Message Format: <timestamp> <seq_num> 31203 ERROR Audit-Flow: Encountered error while recording the audit record for successful login, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31203 ERROR Audit-Flow: Encountered error while recording the audit record for successful login, <log details>

- **Message Code:** 31204

  Severity: ERROR

  Message Text: Encountered error while recording the audit record for failed login

  Message Description: Encountered error while recording the audit record for failed login

  Local Target Message Format: <timestamp> <seq_num> 31204 ERROR Audit-Flow: Encountered error while recording the audit record for failed login, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31204 ERROR Audit-Flow: Encountered error while recording the audit record for failed login, <log details>

- **Message Code:** 31205

  Severity: ERROR

  Message Text: Encountered error while recording the audit record for logout

Message Description: Encountered error while recording the audit record for logout

Local Target Message Format: <timestamp> <seq_num> 31205 ERROR Audit-Flow: Encountered error while recording the audit record for logout, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31205 ERROR Audit-Flow: Encountered error while recording the audit record for logout, <log details>

- **Message Code:** 31206

  Severity: ERROR

  Message Text: Encountered error while recording the audit record for failover mode

  Message Description: Encountered error while recording the audit record for failover mode

  Local Target Message Format: <timestamp> <seq_num> 31206 ERROR Audit-Flow: Encountered error while recording the audit record for failover mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31206 ERROR Audit-Flow: Encountered error while recording the audit record for failover mode, <log details>

- **Message Code:** 31207

  Severity: ERROR

  Message Text: Encountered error while recording the audit record for session timeout

  Message Description: Encountered error while recording the audit record for session timeout

  Local Target Message Format: <timestamp> <seq_num> 31207 ERROR Audit-Flow: Encountered error while recording the audit record for session timeout, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31207 ERROR Audit-Flow: Encountered error while recording the audit record for session timeout, <log details>

- **Message Code:** 31500

  Severity: INFO

  Message Text: Started Management

  Message Description: Started Management

  Local Target Message Format: <timestamp> <seq_num> 31500 INFO Startup-Shutdown: Started Management, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31500 INFO Startup-Shutdown: Started Management, <log details>

- **Message Code:** 31501

  Severity: INFO

  Message Text: Stopped Management

  Message Description: Stopped Management

Local Target Message Format: <timestamp> <seq_num> 31501 INFO Startup-Shutdown: Stopped Management, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31501 INFO Startup-Shutdown: Stopped Management, <log details>

- **Message Code:** 31502

  Severity: INFO

  Message Text: Started Runtime

  Message Description: Started Runtime

  Local Target Message Format: <timestamp> <seq_num> 31502 INFO Startup-Shutdown: Started Runtime, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31502 INFO Startup-Shutdown: Started Runtime, <log details>

- **Message Code:** 31503

  Severity: INFO

  Message Text: Stopped Runtime

  Message Description: Stopped Runtime

  Local Target Message Format: <timestamp> <seq_num> 31503 INFO Startup-Shutdown: Stopped Runtime, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31503 INFO Startup-Shutdown: Stopped Runtime, <log details>

- **Message Code:** 31504

  Severity: FATAL

  Message Text: The cryptographic module could not initialize

  Message Description: The cryptographic module could not initialize

  Local Target Message Format: <timestamp> <seq_num> 31504 FATAL Startup-Shutdown: The cryptographic module could not initialize, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 31504 FATAL Startup-Shutdown: The cryptographic module could not initialize, <log details>

- **Message Code:** 31505

  Severity: INFO

  Message Text: Started Protocols Engine

  Message Description: Started Protocols Engine

Local Target Message Format: <timestamp> <seq_num>31505 INFO Startup-Shutdown Started Protocols Engine, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>31505 INFO Startup-Shutdown Started Protocols Engine, <log details>

- **Message Code:** 31506

  Severity: INFO

  Message Text: Stopped Protocols Engine

  Message Description: Stopped Protocols Engine

  Local Target Message Format: <timestamp> <seq_num>31506 INFO Startup-Shutdown Stopped Protocols Engine, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>31506 INFO Startup-Shutdown Stopped Protocols Engine, <log details>

- **Message Code:** 32000

  Severity: INFO

  Message Text: Started logging component

  Message Description: Started logging component

  Local Target Message Format: <timestamp> <seq_num> 32000 INFO Logging: Started logging component, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32000 INFO Logging: Started logging component, <log details>

- **Message Code:** 32001

  Severity: INFO

  Message Text: Shut down logging component

  Message Description: Shut down logging component

  Local Target Message Format: <timestamp> <seq_num> 32001 INFO Logging: Shut down logging component, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32001 INFO Logging: Shut down logging component, <log details>

- **Message Code:** 32002

  Severity: DEBUG

  Message Text: Using startup default configuration

  Message Description: Using startup default configuration

Local Target Message Format: <timestamp> <seq_num> 32002 DEBUG Logging: Using startup default configuration, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32002 DEBUG Logging: Using startup default configuration, <log details>

- **Message Code:** 32005

  Severity: WARN

  Message Text: Could not log message to logger

  Message Description: Could not log message to logger

  Local Target Message Format: <timestamp> <seq_num> 32005 WARN Logging: Could not log message to logger, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32005 WARN Logging: Could not log message to logger, <log details>

- **Message Code:** 32006

  Severity: WARN

  Message Text: Could not log to critical logger

  Message Description: Could not log to critical logger

  Local Target Message Format: <timestamp> <seq_num> 32006 WARN Logging: Could not log to critical logger, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32006 WARN Logging: Could not log to critical logger, <log details>

- **Message Code:** 32008

  Severity: DEBUG

  Message Text: Logging component now ready to receive configuration changes

  Message Description: Logging successfully subscribed to receive logging configuration changes

  Local Target Message Format: <timestamp> <seq_num> 32008 DEBUG Logging: Logging component now ready to receive configuration changes, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32008 DEBUG Logging: Logging component now ready to receive configuration changes, <log details>

- **Message Code:** 32012

  Severity: ERROR

  Message Text: Could not write to local storage file

  Message Description: Could not write to local storage CSV file

Local Target Message Format: <timestamp> <seq_num> 32012 ERROR Logging: Could not write to local storage file, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32012 ERROR Logging: Could not write to local storage file, <log details>

- **Message Code:** 32013

  Severity: ERROR

  Message Text: Could not create a local storage file

  Message Description: Could not create a local storage CSV file

  Local Target Message Format: <timestamp> <seq_num> 32013 ERROR Logging: Could not create a local storage file, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32013 ERROR Logging: Could not create a local storage file, <log details>

- **Message Code:** 32014

  Severity: ERROR

  Message Text: Could not delete a local storage CSV file

  Message Description: Could not delete a local storage CSV file

  Local Target Message Format: <timestamp> <seq_num> 32014 ERROR Logging: Could not delete a local storage CSV file, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32014 ERROR Logging: Could not delete a local storage CSV file, <log details>

- **Message Code:** 32015

  Severity: DEBUG

  Message Text: Local storage file deleted

  Message Description: Local storage CSV file deleted

  Local Target Message Format: <timestamp> <seq_num> 32015 DEBUG Logging: Local storage file deleted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32015 DEBUG Logging: Local storage file deleted, <log details>

- **Message Code:** 32016

  Severity: FATAL

  Message Text: System reached low disk space limit

  Message Description: System reached low disk space limit. Change local storage cleanup settings to free space

Local Target Message Format: <timestamp> <seq_num> 32016 FATAL Logging: System reached low disk space limit, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32016 FATAL Logging: System reached low disk space limit, <log details>

- **Message Code:** 32017

  Severity: FATAL

  Message Text: Could not to open a UDP socket

  Message Description: Could not open a UDP socket

  Local Target Message Format: <timestamp> <seq_num> 32017 FATAL Logging: Could not to open a UDP socket, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32017 FATAL Logging: Could not to open a UDP socket, <log details>

- **Message Code:** 32018

  Severity: WARN

  Message Text: Could not send data on socket

  Message Description: Could not send data on socket

  Local Target Message Format: <timestamp> <seq_num> 32018 WARN Logging: Could not send data on socket, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32018 WARN Logging: Could not send data on socket, <log details>

- **Message Code:** 32025

  Severity: DEBUG

  Message Text: Rolled over local storage file

  Message Description: Rolled over local storage CSV file

  Local Target Message Format: <timestamp> <seq_num> 32025 DEBUG Logging: Rolled over local storage file, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32025 DEBUG Logging: Rolled over local storage file, <log details>

- **Message Code:** 32026

  Severity: ERROR

  Message Text: Could not roll over local storage file

  Message Description: Could not roll over local storage CSV file

Local Target Message Format: <timestamp> <seq_num> 32026 ERROR Logging: Could not roll over local storage file, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32026 ERROR Logging: Could not roll over local storage file, <log details>

- **Message Code:** 33101

  Severity: INFO

  Message Text: Created new ISE configuration session

  Message Description: acs-config CLI was invoked

  Local Target Message Format: <timestamp> <seq_num> 33101 INFO CLI: Created new ISE configuration session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33101 INFO CLI: Created new ISE configuration session, <log details>

- **Message Code:** 33102

  Severity: INFO

  Message Text: Successful user login to ISE configuration mode

  Message Description: ISE administrator logged in to ISE configuration mode

  Local Target Message Format: <timestamp> <seq_num> 33102 INFO CLI: Successful user login to ISE configuration mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33102 INFO CLI: Successful user login to ISE configuration mode, <log details>

- **Message Code:** 33103

  Severity: INFO

  Message Text: User login to ISE configuration mode failed

  Message Description: Login to ISE configuration mode failed

  Local Target Message Format: <timestamp> <seq_num> 33103 INFO CLI: User login to ISE configuration mode failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33103 INFO CLI: User login to ISE configuration mode failed, <log details>

- **Message Code:** 33104

  Severity: INFO

  Message Text: Closed ISE configuration session

  Message Description: Closed ISE configuration session. Possibly because of request timeout

Local Target Message Format: <timestamp> <seq_num> 33104 INFO CLI: Closed ISE configuration session, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33104 INFO CLI: Closed ISE configuration session, <log details>

- **Message Code:** 33105

  Severity: INFO

  Message Text: Set debug log level

  Message Description: Set debug log level through CLI for a specific component. (See attribute.)

  Local Target Message Format: <timestamp> <seq_num> 33105 INFO CLI: Set debug log level, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33105 INFO CLI: Set debug log level, <log details>

- **Message Code:** 33106

  Severity: INFO

  Message Text: Set default debug log level

  Message Description: Reset debug log level to the default level ('warn') for a single component or a group of components

  Local Target Message Format: <timestamp> <seq_num> 33106 INFO CLI: Set default debug log level, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33106 INFO CLI: Set default debug log level, <log details>

- **Message Code:** 33107

  Severity: DEBUG

  Message Text: Show debugging log status

  Message Description: Invoked show debugging log CLI. (See attribute component)

  Local Target Message Format: <timestamp> <seq_num> 33107 DEBUG CLI: Show debugging log status, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33107 DEBUG CLI: Show debugging log status, <log details>

- **Message Code:** 33108

  Severity: INFO

  Message Text: Reset admin password to its default value

  Message Description: The CLI reset the ACSAdmin user to its default value

Local Target Message Format: <timestamp> <seq_num> 33108 INFO CLI: Reset admin password to its default value, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33108 INFO CLI: Reset admin password to its default value, <log details>

- **Message Code:** 33201

  Severity: ERROR

  Message Text: AD Operation failure

  Message Description: ISE failed during any of the following: While initiating an event to join Active Directory domain. While disconnecting from Active Directory domain. While getting status from Active Directory domain.

  Local Target Message Format: <timestamp> <seq_num> 33201 ERROR Configuration-Notifications: AD Operation failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33201 ERROR Configuration-Notifications: AD Operation failure, <log details>

- **Message Code:** 33202

  Severity: INFO

  Message Text: AD Operation Success

  Message Description: ISE initiated an event for the following reasons: To join the AD domain. To disconnect from the AD domain. To get the status from the AD domain.

  Local Target Message Format: <timestamp> <seq_num> 33202 INFO Configuration-Notifications: AD Operation Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33202 INFO Configuration-Notifications: AD Operation Success, <log details>

- **Message Code:** 33203

  Severity: INFO

  Message Text: Hit Count reset

  Message Description: Administrator requested to reset hit count counters for all configured policies

  Local Target Message Format: <timestamp> <seq_num> 33203 INFO Notification-Dispatcher: Hit Count reset, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33203 INFO Notification-Dispatcher: Hit Count reset, <log details>

- **Message Code:** 33204

  Severity: INFO

  Message Text: Hit Count recollect

Message Description: Periodic request initiated to collect and accumulate the hit count counter values for all configured policies

Local Target Message Format: <timestamp> <seq_num> 33204 INFO Notification-Dispatcher: Hit Count recollect, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33204 INFO Notification-Dispatcher: Hit Count recollect, <log details>

- **Message Code:** 33205

  Severity: ERROR

  Message Text: General PI error

  Message Description: Unexpected error found by the ISE web service provisioning component.

  Local Target Message Format: <timestamp> <seq_num> 33205 ERROR PI: General PI error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33205 ERROR PI: General PI error, <log details>

- **Message Code:** 33206

  Severity: INFO

  Message Text: AD Operation information

  Message Description: ISE information during any of the following: While initiating an event to join Active Directory domain. While disconnecting from Active Directory domain. While getting status from Active Directory domain.

  Local Target Message Format: <timestamp> <seq_num> 33206 INFO Configuration-Notifications: AD Operation information, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33206 INFO Configuration-Notifications: AD Operation information, <log details>

- **Message Code:** 33207

  Severity: WARN

  Message Text: AD Operation warning

  Message Description: ISE encountered warnings during getting status from Active Directory domain.

  Local Target Message Format: <timestamp> <seq_num> 33207 WARN Configuration-Notifications: AD Operation warning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33207 WARN Configuration-Notifications: AD Operation warning, <log details>

- **Message Code:** 33208

  Severity: DEBUG

Message Text: Result for testing connection against AD

Message Description: ISE reports on test connection against active directory server.

Local Target Message Format: <timestamp> <seq_num> 33208 DEBUG Configuration-Notifications: Result for testing connection against AD, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33208 DEBUG Configuration-Notifications: Result for testing connection against AD, <log details>

- **Message Code:** 33209

  Severity: DEBUG

  Message Text: Result for testing connection against LDAP

  Message Description: ISE reports on test connection against LDAP server.

  Local Target Message Format: <timestamp> <seq_num> 33209 DEBUG Configuration-Notifications: Result for testing connection against LDAP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33209 DEBUG Configuration-Notifications: Result for testing connection against LDAP, <log details>

- **Message Code:** 33210

  Severity: DEBUG

  Message Text: LDAP traffic info

  Message Description: LDAP traffic info against LDAP server.

  Local Target Message Format: <timestamp> <seq_num> 33210 DEBUG Configuration-Notifications: LDAP traffic info, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33210 DEBUG Configuration-Notifications: LDAP traffic info, <log details>

- **Message Code:** 33211

  Severity: INFO

  Message Text: ISE is using a self signed certificate for Management Interface authentication

  Message Description: ISE is using a self signed certificate for Management Interface authentication

  Local Target Message Format: <timestamp> <seq_num> 33211 INFO System-Management: ISE is using a self signed certificate for Management Interface authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33211 INFO System-Management: ISE is using a self signed certificate for Management Interface authentication, <log details>

- **Message Code:** 33212

  Severity: WARN

Message Text: Due to system failure, ISE could not load the associated certificate for the Management Interface

Message Description: Due to system failure, ISE could not load the associated certificate for the Management Interface. The default self signed certificate is used.

Local Target Message Format: <timestamp> <seq_num> 33212 WARN System-Management: Due to system failure, ISE could not load the associated certificate for the Management Interface, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33212 WARN System-Management: Due to system failure, ISE could not load the associated certificate for the Management Interface, <log details>

- **Message Code:** 33300

  Severity: ERROR

  Message Text: General GUI error

  Message Description: Unexpected error found by ISE graphical user interface.

  Local Target Message Format: <timestamp> <seq_num> 33300 ERROR Graphical-user-interface: General GUI error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33300 ERROR Graphical-user-interface: General GUI error, <log details>

- **Message Code:** 32500

  Severity: ERROR

  Message Text: General database error

  Message Description: General database error

  Local Target Message Format: <timestamp> <seq_num> 32500 ERROR Local-DB: General database error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32500 ERROR Local-DB: General database error, <log details>

- **Message Code:** 32600

  Severity: INFO

  Message Text: Connected message bus

  Message Description: Connected message bus

  Local Target Message Format: <timestamp> <seq_num> 32600 INFO Message-Bus: Connected message bus, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32600 INFO Message-Bus: Connected message bus, <log details>

- **Message Code:** 32601

Severity: ERROR

Message Text: Could not start message bus

Message Description: Could not start message bus

Local Target Message Format: <timestamp> <seq_num> 32601 ERROR Message-Bus: Could not start message bus, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32601 ERROR Message-Bus: Could not start message bus, <log details>

- **Message Code:** 32602

  Severity: INFO

  Message Text: Retrying message bus connection

  Message Description: Retrying message bus connection

  Local Target Message Format: <timestamp> <seq_num> 32602 INFO Message-Bus: Retrying message bus connection, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32602 INFO Message-Bus: Retrying message bus connection, <log details>

- **Message Code:** 32603

  Severity: ERROR

  Message Text: Dropped connection. Reconnecting

  Message Description: Dropped connection. Reconnecting

  Local Target Message Format: <timestamp> <seq_num> 32603 ERROR Message-Bus: Dropped connection. Reconnecting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32603 ERROR Message-Bus: Dropped connection. Reconnecting, <log details>

- **Message Code:** 32604

  Severity: ERROR

  Message Text: Unknown bus error

  Message Description: Unknown bus error

  Local Target Message Format: <timestamp> <seq_num> 32604 ERROR Message-Bus: Unknown bus error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32604 ERROR Message-Bus: Unknown bus error, <log details>

- **Message Code:** 32605

  Severity: ERROR

Message Text: Unknown attribute

Message Description: Unknown attribute

Local Target Message Format: <timestamp> <seq_num> 32605 ERROR Message-Bus: Unknown attribute, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32605 ERROR Message-Bus: Unknown attribute, <log details>

- **Message Code:** 32606

  Severity: ERROR

  Message Text: Dropped unknown message type

  Message Description: Dropped unknown message type

  Local Target Message Format: <timestamp> <seq_num> 32606 ERROR Message-Bus: Dropped unknown message type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32606 ERROR Message-Bus: Dropped unknown message type, <log details>

- **Message Code:** 32607

  Severity: INFO

  Message Text: Missing attribute

  Message Description: Missing attribute

  Local Target Message Format: <timestamp> <seq_num> 32607 INFO Message-Bus: Missing attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32607 INFO Message-Bus: Missing attribute, <log details>

- **Message Code:** 32700

  Severity: WARN

  Message Text: Failover mode caused by an internal error. Configuration changes may not take effect

  Message Description: Failover mode caused by an internal error. Configuration changes may not take effect

  Local Target Message Format: <timestamp> <seq_num> 32700 WARN Administrator-Login: Failover mode caused by an internal error. Configuration changes may not take effect, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 32700 WARN Administrator-Login: Failover mode caused by an internal error. Configuration changes may not take effect, <log details>

- **Message Code:** 33400

  Severity: INFO

Message Text: Certificate Revocation List was added

Message Description: Certificate Revocation List was downloaded and will be used by ISE

Local Target Message Format: <timestamp> <seq_num> 33400 INFO CRL: Certificate Revocation List was added, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33400 INFO CRL: Certificate Revocation List was added, <log details>

- **Message Code:** 33450

  Severity: INFO

  Message Text: Received a request to clear OCSP cache

  Message Description: Received a request to clear OCSP cache

  Local Target Message Format: <timestamp> <seq_num> 33450 INFO OCSP: Received a request to clear OCSP cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33450 INFO OCSP: Received a request to clear OCSP cache, <log details>

- **Message Code:** 33451

  Severity: INFO

  Message Text: Successfully clear OCSP cache

  Message Description: Successfully clear OCSP cache

  Local Target Message Format: <timestamp> <seq_num> 33451 INFO OCSP: Successfully clear OCSP cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33451 INFO OCSP: Successfully clear OCSP cache, <log details>

- **Message Code:** 33452

  Severity: ERROR

  Message Text: Failed to clear OCSP cache

  Message Description: Failed to clear OCSP cache

  Local Target Message Format: <timestamp> <seq_num> 33452 ERROR OCSP: Failed to clear OCSP cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33452 ERROR OCSP: Failed to clear OCSP cache, <log details>

- **Message Code:** 33500

  Severity: ERROR

  Message Text: Could not initialize EAP-TLS

Message Description: The EAP-TLS module could not initialize and will be disabled.

Local Target Message Format: <timestamp> <seq_num> 33500 ERROR EAP: Could not initialize EAP-TLS, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33500 ERROR EAP: Could not initialize EAP-TLS, <log details>

- **Message Code:** 33501

  Severity: ERROR

  Message Text: Could not initialize EAP-FAST

  Message Description: The EAP-FAST module could not initialize and will be disabled

  Local Target Message Format: <timestamp> <seq_num> 33501 ERROR EAP: Could not initialize EAP-FAST, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33501 ERROR EAP: Could not initialize EAP-FAST, <log details>

- **Message Code:** 33502

  Severity: ERROR

  Message Text: Could not initialize PEAP

  Message Description: The PEAP module could not initialize and will be disabled

  Local Target Message Format: <timestamp> <seq_num> 33502 ERROR EAP: Could not initialize PEAP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33502 ERROR EAP: Could not initialize PEAP, <log details>

- **Message Code:** 33503

  Severity: WARN

  Message Text: A blank CTL was configured for EAP-TLS

  Message Description: The EAP-TLS module has initialized with a blank CTL

  Local Target Message Format: <timestamp> <seq_num> 33503 WARN EAP: A blank CTL was configured for EAP-TLS, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33503 WARN EAP: A blank CTL was configured for EAP-TLS, <log details>

- **Message Code:** 33504

  Severity: WARN

  Message Text: CTL initialization failed

Message Description: The EAP-TLS or EAP-FAST module could not initialize part of the CTL configuration.

Local Target Message Format: <timestamp> <seq_num> 33504 WARN EAP: CTL initialization failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33504 WARN EAP: CTL initialization failed, <log details>

- **Message Code:** 33505

  Severity: WARN

  Message Text: Could not initialize EAP-TLS server-certificate

  Message Description: The EAP-TLS module could not initialize the server-certificate because of a configuration problem.

  Local Target Message Format: <timestamp> <seq_num> 33505 WARN EAP: Could not initialize EAP-TLS server-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33505 WARN EAP: Could not initialize EAP-TLS server-certificate, <log details>

- **Message Code:** 33506

  Severity: WARN

  Message Text: Could not initialize EAP-FAST server-certificate

  Message Description: The EAP-FAST module could not initialize the server-certificate because of a configuration problem. This problem affects only the authenticated provisioning mode of EAP-FAST.

  Local Target Message Format: <timestamp> <seq_num> 33506 WARN EAP: Could not initialize EAP-FAST server-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33506 WARN EAP: Could not initialize EAP-FAST server-certificate, <log details>

- **Message Code:** 33507

  Severity: WARN

  Message Text: Could not initialize PEAP server-certificate

  Message Description: The EAP-TLS module could not initialize the server-certificate because of a configuration problem.

  Local Target Message Format: <timestamp> <seq_num> 33507 WARN EAP: Could not initialize PEAP server-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33507 WARN EAP: Could not initialize PEAP server-certificate, <log details>

- **Message Code:** 33508

Severity: WARN

Message Text: Could not initialize the complete EAP-TLS server-certificate chain

Message Description: The EAP-TLS module could not initialize the server-certificate complete chain because of a configuration problem.

Local Target Message Format: <timestamp> <seq_num> 33508 WARN EAP: Could not initialize the complete EAP-TLS server-certificate chain, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33508 WARN EAP: Could not initialize the complete EAP-TLS server-certificate chain, <log details>

- **Message Code:** 33509

  Severity: WARN

  Message Text: PEAP failed to completely initialize the server-certificate chain

  Message Description: The PEAP module could not initialize the server-certificate complete chain because of a configuration problem.

  Local Target Message Format: <timestamp> <seq_num> 33509 WARN EAP: PEAP failed to completely initialize the server-certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33509 WARN EAP: PEAP failed to completely initialize the server-certificate chain, <log details>

- **Message Code:** 33510

  Severity: WARN

  Message Text: Could not initialize the complete EAP-FAST server-certificate chain

  Message Description: The EAP-FAST module could not initialize the server-certificate complete chain because of a configuration problem.

  Local Target Message Format: <timestamp> <seq_num> 33510 WARN EAP: Could not initialize the complete EAP-FAST server-certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 33510 WARN EAP: Could not initialize the complete EAP-FAST server-certificate chain, <log details>

- **Message Code:** 33511

  Severity: WARN

  Message Text: Could not initialize TEAP server-certificate

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33511 WARN EAP Could not initialize TEAP server-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33511 WARN EAP Could not initialize TEAP server-certificate, <log details>

- **Message Code:** 33512

  Severity: WARN

  Message Text: Could not initialize the complete TEAP server-certificate chain

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33512 WARN EAP Could not initialize the complete TEAP server-certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33512 WARN EAP Could not initialize the complete TEAP server-certificate chain, <log details>

- **Message Code:** 33513

  Severity: ERROR

  Message Text: Could not initialize TEAP

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33513 ERROR EAP Could not initialize TEAP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33513 ERROR EAP Could not initialize TEAP, <log details>

- **Message Code:** 33514

  Severity: DEBUG

  Message Text: Sent TEAP Result TLV indicating success

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33514 DEBUG EAP Sent TEAP Result TLV indicating success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33514 DEBUG EAP Sent TEAP Result TLV indicating success, <log details>

- **Message Code:** 33515

  Severity: DEBUG

  Message Text: Sent TEAP Result TLV indicating failure

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33515 DEBUG EAP Sent TEAP Result TLV indicating failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33515 DEBUG EAP Sent TEAP Result TLV indicating failure, <log details>

- **Message Code:** 33516

Severity: DEBUG

Message Text: Sent TEAP Intermediate Result TLV indicating success

Message Description: nan

Local Target Message Format: <timestamp> <seq_num>33516 DEBUG EAP Sent TEAP Intermediate Result TLV indicating success, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33516 DEBUG EAP Sent TEAP Intermediate Result TLV indicating success, <log details>

- **Message Code:** 33517

  Severity: DEBUG

  Message Text: Sent TEAP Intermediate Result TLV indicating failure

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33517 DEBUG EAP Sent TEAP Intermediate Result TLV indicating failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33517 DEBUG EAP Sent TEAP Intermediate Result TLV indicating failure, <log details>

- **Message Code:** 33518

  Severity: WARN

  Message Text: No cipher for full handshake TEAP authentication

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>33518 WARN EAP No cipher for full handshake TEAP authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>33518 WARN EAP No cipher for full handshake TEAP authentication, <log details>

- **Message Code:** 34000

  Severity: INFO

  Message Text: Appending transaction

  Message Description: The transaction was applied to the configuration and appended to the transaction log

  Local Target Message Format: <timestamp> <seq_num> 34000 INFO Replication: Appending transaction, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34000 INFO Replication: Appending transaction, <log details>

- **Message Code:** 34001

Severity: INFO

Message Text: Dispatching transaction

Message Description: The transaction was sent to Secondary nodes for replication

Local Target Message Format: <timestamp> <seq_num> 34001 INFO Replication: Dispatching transaction, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34001 INFO Replication: Dispatching transaction, <log details>

- **Message Code:** 34002

  Severity: INFO

  Message Text: Received transaction

  Message Description: The transaction was received from the Primary node

  Local Target Message Format: <timestamp> <seq_num> 34002 INFO Replication: Received transaction, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34002 INFO Replication: Received transaction, <log details>

- **Message Code:** 34003

  Severity: INFO

  Message Text: Applied transaction

  Message Description: The replicated transaction was applied to the local configuration

  Local Target Message Format: <timestamp> <seq_num> 34003 INFO Replication: Applied transaction, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34003 INFO Replication: Applied transaction, <log details>

- **Message Code:** 34005

  Severity: FATAL

  Message Text: Policy cache sync failed

  Message Description: Failed to synchronize policy cache

  Local Target Message Format: <timestamp> <seq_num> 34005 FATAL Replication: Policy cache sync failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34005 FATAL Replication: Policy cache sync failed, <log details>

- **Message Code:** 34050

  Severity: INFO

Message Text: RT Control port is up

Message Description: RT is listening on RT Control port.

Local Target Message Format: <timestamp> <seq_num> 34050 INFO RT-Control: RT Control port is up, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34050 INFO RT-Control: RT Control port is up, <log details>

- **Message Code:** 34051

  Severity: ERROR

  Message Text: RT Control port is blocked

  Message Description: RT failed to open the RT Control port. RT Control services are not available. RT will try to open the port again.

  Local Target Message Format: <timestamp> <seq_num> 34051 ERROR RT-Control: RT Control port is blocked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34051 ERROR RT-Control: RT Control port is blocked, <log details>

- **Message Code:** 34110

  Severity: ERROR

  Message Text: Error processing the REST request

  Message Description: Server has encountered error while processing the REST request

  Local Target Message Format: <timestamp> <seq_num> 34110 ERROR REST: Error processing the REST request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34110 ERROR REST: Error processing the REST request, <log details>

- **Message Code:** 34111

  Severity: INFO

  Message Text: Successfully processed the REST request

  Message Description: REST Request is successfully processed

  Local Target Message Format: <timestamp> <seq_num> 34111 INFO REST: Successfully processed the REST request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34111 INFO REST: Successfully processed the REST request, <log details>

- **Message Code:** 34112

  Severity: ERROR

Message Text: Invalid REST request data

Message Description: REST Request data has invalid syntax

Local Target Message Format: <timestamp> <seq_num> 34112 ERROR REST: Invalid REST request data, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34112 ERROR REST: Invalid REST request data, <log details>

- **Message Code:** 34113

  Severity: WARN

  Message Text: Specified resource not found

  Message Description: Specified resource is not found

  Local Target Message Format: <timestamp> <seq_num> 34113 WARN REST: Specified resource not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34113 WARN REST: Specified resource not found, <log details>

- **Message Code:** 34114

  Severity: WARN

  Message Text: Specified resource already exists

  Message Description: Specified resource already exists

  Local Target Message Format: <timestamp> <seq_num> 34114 WARN REST: Specified resource already exists, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34114 WARN REST: Specified resource already exists, <log details>

- **Message Code:** 34115

  Severity: WARN

  Message Text: Specified associated resource does not exist

  Message Description: Specified associated resource does not exist

  Local Target Message Format: <timestamp> <seq_num> 34115 WARN REST: Specified associated resource does not exist, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34115 WARN REST: Specified associated resource does not exist, <log details>

- **Message Code:** 34116

  Severity: WARN

  Message Text: Specified policy is not found

Message Description: Specified policy is not found

Local Target Message Format: <timestamp> <seq_num> 34116 WARN REST: Specified policy is not found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34116 WARN REST: Specified policy is not found, <log details>

- **Message Code:** 34117

  Severity: ERROR

  Message Text: Error connecting to remote feed URL

  Message Description: This message is generated when remote feed site is down

  Local Target Message Format: <timestamp> <seq_num> 34117 ERROR Client Provisioning: Error connecting to remote feed URL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34117 ERROR Client Provisioning: Error connecting to remote feed URL, <log details>

- **Message Code:** 34118

  Severity: ERROR

  Message Text: Error processing package from Cisco download feed site

  Message Description: Error processing package from Cisco download feed site

  Local Target Message Format: <timestamp> <seq_num> 34118 ERROR Client Provisioning: Error processing package from Cisco download feed site, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34118 ERROR Client Provisioning: Error processing package from Cisco download feed site, <log details>

- **Message Code:** 34119

  Severity: ERROR

  Message Text: Profile received an error response from NAC Manager for notification event

  Message Description: Profiler sends a notification event to NAC Manager, but the notification fails because NAC Manager cannot process it. Check NAC Manager logs for details

  Local Target Message Format: <timestamp> <seq_num> 34119 ERROR Profiler: Profile received an error response from NAC Manager for notification event, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34119 ERROR Profiler: Profile received an error response from NAC Manager for notification event, <log details>

- **Message Code:** 34120

  Severity: ERROR

  Message Text: Profiler failed to get the connection to NAC Manager

Message Description: Profiler sends a notification event to NAC Manager, but the notification fails because could not connect to NAC Manager

Local Target Message Format: <timestamp> <seq_num> 34120 ERROR Profiler: Profiler failed to get the connection to NAC Manager, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34120 ERROR Profiler: Profiler failed to get the connection to NAC Manager, <log details>

- **Message Code:** 34123

  Severity: FATAL

  Message Text: The virtual memory usage is high indicating the process may be running out of memory resources

  Message Description: The virtual memory is high indicating the process may be running out of memory resources

  Local Target Message Format: <timestamp> <seq_num> 34123 FATAL System-Management: The virtual memory usage is high indicating the process may be running out of memory resources, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34123 FATAL System-Management: The virtual memory usage is high indicating the process may be running out of memory resources, <log details>

- **Message Code:** 34124

  Severity: FATAL

  Message Text: Due to low memory resources the amount of concurrent EAP sessions will be limited

  Message Description: Due to low memory resources the amount of concurrent EAP sessions will be limited

  Local Target Message Format: <timestamp> <seq_num> 34124 FATAL System-Management: Due to low memory resources the amount of concurrent EAP sessions will be limited, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34124 FATAL System-Management: Due to low memory resources the amount of concurrent EAP sessions will be limited, <log details>

- **Message Code:** 34125

  Severity: FATAL

  Message Text: Due to low memory resources a CRL could not be updated.

  Message Description: Due to low memory resources a CRL could not be updated.

  Local Target Message Format: <timestamp> <seq_num> 34125 FATAL System-Management: Due to low memory resources a CRL could not be updated., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34125 FATAL System-Management: Due to low memory resources a CRL could not be updated., <log details>

- **Message Code:** 34126

  Severity: WARN

  Message Text: Remote syslog target is unavailable

  Message Description: Remote syslog target is unavailable

  Local Target Message Format: <timestamp> <seq_num> 34126 WARN System-Management: Remote syslog target is unavailable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34126 WARN System-Management: Remote syslog target is unavailable, <log details>

- **Message Code:** 34127

  Severity: WARN

  Message Text: Remote syslog target connection resume

  Message Description: Remote syslog target connection resume

  Local Target Message Format: <timestamp> <seq_num> 34127 WARN System-Management: Remote syslog target connection resume, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34127 WARN System-Management: Remote syslog target connection resume, <log details>

- **Message Code:** 34128

  Severity: DEBUG

  Message Text: Remote syslog target buffer is cleared

  Message Description: Remote syslog target buffer is cleared due to configuration change

  Local Target Message Format: <timestamp> <seq_num> 34128 DEBUG System-Management: Remote syslog target buffer is cleared, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34128 DEBUG System-Management: Remote syslog target buffer is cleared, <log details>

- **Message Code:** 34129

  Severity: WARN

  Message Text: Could not initialize syslog client certificate

  Message Description: Could not initialize syslog client certificate because of configuration problem

  Local Target Message Format: <timestamp> <seq_num> 34129 WARN System-Management: Could not initialize syslog client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34129 WARN System-Management: Could not initialize syslog client certificate, <log details>

- **Message Code:** 34130

Severity: WARN

Message Text: CTL for syslog server certificate is empty

Message Description: CTL for syslog server certificate is empty. No syslog server will be accepted

Local Target Message Format: <timestamp> <seq_num> 34130 WARN System-Management: CTL for syslog server certificate is empty, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34130 WARN System-Management: CTL for syslog server certificate is empty, <log details>

- **Message Code:** 34131

  Severity: WARN

  Message Text: Could not initialize the complete syslog client certificate chain

  Message Description: Could not initialize the complete syslog client certificate chain because of a configuration problem

  Local Target Message Format: <timestamp> <seq_num> 34131 WARN System-Management: Could not initialize the complete syslog client certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34131 WARN System-Management: Could not initialize the complete syslog client certificate chain, <log details>

- **Message Code:** 34132

  Severity: INFO

  Message Text: TLS handshake with syslog server succeeded

  Message Description: TLS handshake with syslog server succeeded

  Local Target Message Format: <timestamp> <seq_num> 34132 INFO System-Management: TLS handshake with syslog server succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34132 INFO System-Management: TLS handshake with syslog server succeeded, <log details>

- **Message Code:** 34133

  Severity: WARN

  Message Text: TLS handshake with syslog server failed

  Message Description: TLS handshake with syslog server failed

  Local Target Message Format: <timestamp> <seq_num> 34133 WARN System-Management: TLS handshake with syslog server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34133 WARN System-Management: TLS handshake with syslog server failed, <log details>

- **Message Code:** 34134

Severity: WARN

Message Text: Could not initialize CTL for syslog server certificate verification

Message Description: Could not initialize CTL for syslog server certificate verification

Local Target Message Format: <timestamp> <seq_num> 34134 WARN System-Management: Could not initialize CTL for syslog server certificate verification, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34134 WARN System-Management: Could not initialize CTL for syslog server certificate verification, <log details>

- **Message Code:** 34135

  Severity: WARN

  Message Text: Syslog server is slow or down. Buffered syslog messages are being deleted.

  Message Description: Syslog sever is slow, down or unable to read syslog messages. Buffered syslog messages are being deleted. This may be due to server, network or load balancer issues.

  Local Target Message Format: <timestamp> <seq_num> 34135 WARN System-Management: Syslog server is slow or down. Buffered syslog messages are being deleted., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34135 WARN System-Management: Syslog server is slow or down. Buffered syslog messages are being deleted., <log details>

- **Message Code:** 34137

  Severity: WARN

  Message Text: Secure syslog server rejected ISE syslog client certificate

  Message Description: Secure syslog server rejected ISE syslog client certificate

  Local Target Message Format: <timestamp> <seq_num> 34137 WARN System-Management: Secure syslog server rejected ISE syslog client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34137 WARN System-Management: Secure syslog server rejected ISE syslog client certificate, <log details>

- **Message Code:** 34138

  Severity: WARN

  Message Text: ISE failed secure syslog connection because of unsupported certificate in syslog server certificate chain

  Message Description: ISE failed secure syslog connection because of unsupported certificate in syslog server certificate chain

  Local Target Message Format: <timestamp> <seq_num> 34138 WARN System-Management: ISE failed secure syslog connection because of unsupported certificate in syslog server certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34138 WARN System-Management:

ISE failed secure syslog connection because of unsupported certificate in syslog server certificate chain, <log details>

- **Message Code:** 34139

  Severity: WARN

  Message Text: ISE failed secure syslog connection because it was unable to download CRL for the CA that signed syslog server certificate

  Message Description: ISE failed secure syslog connection because it was unable to download CRL for the CA that signed syslog server certificate

  Local Target Message Format: <timestamp> <seq_num> 34139 WARN System-Management: ISE failed secure syslog connection because it was unable to download CRL for the CA that signed syslog server certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34139 WARN System-Management: ISE failed secure syslog connection because it was unable to download CRL for the CA that signed syslog server certificate, <log details>

- **Message Code:** 34140

  Severity: WARN

  Message Text: ISE failed secure syslog connection because of unknown certificate in syslog server certificate chain

  Message Description: ISE failed secure syslog connection because of unknown certificate in syslog server certificate chain

  Local Target Message Format: <timestamp> <seq_num> 34140 WARN System-Management: ISE failed secure syslog connection because of unknown certificate in syslog server certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34140 WARN System-Management: ISE failed secure syslog connection because of unknown certificate in syslog server certificate chain, <log details>

- **Message Code:** 34141

  Severity: WARN

  Message Text: ISE failed secure syslog connection because of expired certificate in syslog server certificate chain

  Message Description: ISE failed secure syslog connection because of expired certificate in syslog server certificate chain

  Local Target Message Format: <timestamp> <seq_num> 34141 WARN System-Management: ISE failed secure syslog connection because of expired certificate in syslog server certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34141 WARN System-Management: ISE failed secure syslog connection because of expired certificate in syslog server certificate chain, <log details>

- **Message Code:** 34142

  Severity: WARN

  Message Text: ISE failed secure syslog connection because of expired CRL for the CA that signed syslog server certificate

  Message Description: ISE failed secure syslog connection because of expired CRL for the CA that signed syslog server certificate

  Local Target Message Format: <timestamp> <seq_num> 34142 WARN System-Management: ISE failed secure syslog connection because of expired CRL for the CA that signed syslog server certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34142 WARN System-Management: ISE failed secure syslog connection because of expired CRL for the CA that signed syslog server certificate, <log details>

- **Message Code:** 34143

  Severity: WARN

  Message Text: ISE failed secure syslog connection because of revoked certificate in syslog server certificate chain

  Message Description: ISE failed secure syslog connection because of revoked certificate in syslog server certificate chain

  Local Target Message Format: <timestamp> <seq_num> 34143 WARN System-Management: ISE failed secure syslog connection because of revoked certificate in syslog server certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34143 WARN System-Management: ISE failed secure syslog connection because of revoked certificate in syslog server certificate chain, <log details>

- **Message Code:** 34144

  Severity: WARN

  Message Text: ISE failed secure syslog connection because of bad certificate in syslog server certificate chain

  Message Description: ISE failed secure syslog connection because of bad certificate in syslog server certificate chain

  Local Target Message Format: <timestamp> <seq_num> 34144 WARN System-Management: ISE failed secure syslog connection because of bad certificate in syslog server certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34144 WARN System-Management: ISE failed secure syslog connection because of bad certificate in syslog server certificate chain, <log details>

- **Message Code:** 34145

  Severity: WARN

Message Text: Secure syslog connection reconnect due to OCSP found revoked certificate

Message Description: OCSP check result is that the certificate used for syslog connection is revoke

Local Target Message Format: <timestamp> <seq_num> 34145 WARN System-Management: Secure syslog connection reconnect due to OCSP found revoked certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34145 WARN System-Management: Secure syslog connection reconnect due to OCSP found revoked certificate, <log details>

- **Message Code:** 34146

  Severity: WARN

  Message Text: Secure syslog connection reconnect due to CRL found revoked certificate

  Message Description: CRL check result is that the certificate used for syslog connection is revoke

  Local Target Message Format: <timestamp> <seq_num> 34146 WARN System-Management: Secure syslog connection reconnect due to CRL found revoked certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34146 WARN System-Management: Secure syslog connection reconnect due to CRL found revoked certificate, <log details>

- **Message Code:** 34147

  Severity: WARN

  Message Text: JGroups TLS Handshake Failed

  Message Description: JGroups TLS Handshake Failed

  Local Target Message Format: <timestamp> <seq_num> 34147 WARN System-Management: JGroups TLS Handshake Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34147 WARN System-Management: JGroups TLS Handshake Failed, <log details>

- **Message Code:** 34148

  Severity: INFO

  Message Text: JGroups TLS Handshake Succeeded

  Message Description: JGroups TLS Handshake Succeeded

  Local Target Message Format: <timestamp> <seq_num> 34148 INFO System-Management: JGroups TLS Handshake Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34148 INFO System-Management: JGroups TLS Handshake Succeeded, <log details>

- **Message Code:** 34149

  Severity: WARN

  Message Text: HTTPS TLS Handshake Failed

Message Description: HTTPS TLS Handshake Failed

Local Target Message Format: <timestamp> <seq_num> 34149 WARN System-Management: HTTPS TLS Handshake Failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34149 WARN System-Management: HTTPS TLS Handshake Failed, <log details>

- **Message Code:** 34150

  Severity: INFO

  Message Text: HTTPS TLS Handshake Succeeded

  Message Description: HTTPS TLS Handshake Succeeded

  Local Target Message Format: <timestamp> <seq_num> 34150 INFO System-Management: HTTPS TLS Handshake Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34150 INFO System-Management: HTTPS TLS Handshake Succeeded, <log details>

- **Message Code:** 34151

  Severity: WARN

  Message Text: Certificate Validation Failed

  Message Description: Certificate Validation Failed

  Local Target Message Format: <timestamp> <seq_num> 34151 WARN System-Management: Certificate Validation Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34151 WARN System-Management: Certificate Validation Failed, <log details>

- **Message Code:** 34152

  Severity: INFO

  Message Text: Certificate Validation Succeeded

  Message Description: Certificate Validation Succeeded

  Local Target Message Format: <timestamp> <seq_num> 34152 INFO System-Management: Certificate Validation Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34152 INFO System-Management: Certificate Validation Succeeded, <log details>

- **Message Code:** 34153

  Severity: WARN

  Message Text: Secure LDAP ID Store Connecion Failed

  Message Description: Secure LDAP ID Store Connecion Failed

Local Target Message Format: <timestamp> <seq_num> 34153 WARN System-Management: Secure LDAP ID Store Connecion Failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34153 WARN System-Management: Secure LDAP ID Store Connecion Failed, <log details>

- **Message Code:** 34154

  Severity: INFO

  Message Text: Secure LDAP ID Store Connecion Succeeded

  Message Description: Secure LDAP ID Store Connecion Succeeded

  Local Target Message Format: <timestamp> <seq_num> 34154 INFO System-Management: Secure LDAP ID Store Connecion Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34154 INFO System-Management: Secure LDAP ID Store Connecion Succeeded, <log details>

- **Message Code:** 34155

  Severity: ERROR

  Message Text: Endpoint with the same Mac Address already exists

  Message Description: Endpoint with the same Mac Address already exists

  Local Target Message Format: <timestamp> <seq_num> 34155 ERROR REST: Endpoint with the same Mac Address already exists, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34155 ERROR REST: Endpoint with the same Mac Address already exists, <log details>

- **Message Code:** 34156

  Severity: INFO

  Message Text: CARS Network configuration has been reset

  Message Description: CARS Network configuration has been reset

  Local Target Message Format: <timestamp> <seq_num> 34156 INFO System-Management: CARS Network configuration has been reset, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34156 INFO System-Management: CARS Network configuration has been reset, <log details>

- **Message Code:** 34157

  Severity: ERROR

  Message Text: Could not initialize EAP-TTLS

  Message Description: The EAP-TTLS module could not initialize and will be disabled.

Local Target Message Format: <timestamp> <seq_num> 34157 ERROR EAP: Could not initialize EAP-TTLS, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34157 ERROR EAP: Could not initialize EAP-TTLS, <log details>

- **Message Code:** 34158

  Severity: WARN

  Message Text: Could not initialize EAP-TTLS server-certificate

  Message Description: The EAP-TTLS module could not initialize the server-certificate because of a configuration problem.

  Local Target Message Format: <timestamp> <seq_num> 34158 WARN EAP: Could not initialize EAP-TTLS server-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34158 WARN EAP: Could not initialize EAP-TTLS server-certificate, <log details>

- **Message Code:** 34159

  Severity: INFO

  Message Text: LDAPS connection established successfully

  Message Description: LDAPS connection established successfully

  Local Target Message Format: <timestamp> <seq_num> 34159 INFO System-Management: LDAPS connection established successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34159 INFO System-Management: LDAPS connection established successfully, <log details>

- **Message Code:** 34160

  Severity: INFO

  Message Text: LDAPS connection terminated successfully

  Message Description: LDAPS connection terminated successfully

  Local Target Message Format: <timestamp> <seq_num> 34160 INFO System-Management: LDAPS connection terminated successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34160 INFO System-Management: LDAPS connection terminated successfully, <log details>

- **Message Code:** 34161

  Severity: WARN

  Message Text: LDAPS connection establishment failed with SSL error

  Message Description: LDAPS connection establishment failed with SSL error

Local Target Message Format: <timestamp> <seq_num> 34161 WARN System-Management: LDAPS connection establishment failed with SSL error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34161 WARN System-Management: LDAPS connection establishment failed with SSL error, <log details>

- **Message Code:** 34162

  Severity: WARN

  Message Text: LDAPS connection terminated with SSL error

  Message Description: LDAPS connection terminated with SSL error

  Local Target Message Format: <timestamp> <seq_num> 34162 WARN System-Management: LDAPS connection terminated with SSL error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34162 WARN System-Management: LDAPS connection terminated with SSL error, <log details>

- **Message Code:** 34163

  Severity: WARN

  Message Text: LDAPS connection establishment failed with non-SSL error

  Message Description: LDAPS connection establishment failed with non-SSL error

  Local Target Message Format: <timestamp> <seq_num> 34163 WARN System-Management: LDAPS connection establishment failed with non-SSL error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34163 WARN System-Management: LDAPS connection establishment failed with non-SSL error, <log details>

- **Message Code:** 34164

  Severity: WARN

  Message Text: LDAPS connection terminated with non-SSL error

  Message Description: LDAPS connection terminated with non-SSL error

  Local Target Message Format: <timestamp> <seq_num> 34164 WARN System-Management: LDAPS connection terminated with non-SSL error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 34164 WARN System-Management: LDAPS connection terminated with non-SSL error, <log details>

- **Message Code:** 34165

  Severity: WARN

  Message Text: Docker Metrics

  Message Description: Docker Metrics

Local Target Message Format: <timestamp> <seq_num>System-Management Docker Metrics WARN Docker Metrics, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>System-Management Docker Metrics WARN Docker Metrics, <log details>

- **Message Code:** 34166

  Severity: INFO

  Message Text: Open secure connection with TLS peer

  Message Description: Secure connection established with TLS peer

  Local Target Message Format: <timestamp> <seq_num>34166 INFO System-Management Open secure connection with TLS peer, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>34166 INFO System-Management Open secure connection with TLS peer, <log details>

- **Message Code:** 34167

  Severity: INFO

  Message Text: Shutdown secure connection with TLS peer

  Message Description: Secure connection with TLS peer shutdown

  Local Target Message Format: <timestamp> <seq_num>34167 INFO System-Management Shutdown secure connection with TLS peer, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>34167 INFO System-Management Shutdown secure connection with TLS peer, <log details>

- **Message Code:** 34170

  Severity: WARN

  Message Text: Active pxGrid cloud node was unable to connect to cloud. Switchover will be attempted if standby pxGrid cloud node is available.

  Message Description: Active pxGrid cloud node was unable to connect to cloud. Switchover will be attempted if standby pxGrid cloud node is available.

  Local Target Message Format: <timestamp> <seq_num>34170 WARN System-Management Active pxGrid cloud node was unable to connect to cloud. Switchover will be attempted if standby pxGrid cloud node is available., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>34170 WARN System-Management Active pxGrid cloud node was unable to connect to cloud. Switchover will be attempted if standby pxGrid cloud node is available., <log details>

IPsec

- **Message Code:** 93001

  Severity: INFO

  Message Text: IPSec Operation Message

  Message Description: IPSec message

  Local Target Message Format: <timestamp> <seq_num>IPSec IPSec Operation Message INFO IPSec message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec IPSec Operation Message INFO IPSec message, <log details>

- **Message Code:** 93002

  Severity: ERROR

  Message Text: IPSec tunnel proposal mismatch

  Message Description: IPSec tunnel proposal mismatch

  Local Target Message Format: <timestamp> <seq_num>IPSec IPSec tunnel proposal mismatch ERROR IPSec tunnel proposal mismatch, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec IPSec tunnel proposal mismatch ERROR IPSec tunnel proposal mismatch, <log details>

- **Message Code:** 93003

  Severity: INFO

  Message Text: IPSec connection established

  Message Description: IPSec connection established

  Local Target Message Format: <timestamp> <seq_num>IPSec IPSec connection established INFO IPSec connection established, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec IPSec connection established INFO IPSec connection established, <log details>

- **Message Code:** 93004

  Severity: INFO

  Message Text: IPSec connection initiation

  Message Description: IPSec connection initiation

  Local Target Message Format: <timestamp> <seq_num>IPSec IPSec connection initiation INFO IPSec connection initiation, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec IPSec connection initiation INFO IPSec connection initiation, <log details>

- **Message Code:** 93005

  Severity: ERROR

  Message Text: Authentication failed

  Message Description: Authentication failed

  Local Target Message Format: <timestamp> <seq_num>IPSec Authentication failed ERROR Authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec Authentication failed ERROR Authentication failed, <log details>

- **Message Code:** 93006

  Severity: ERROR

  Message Text: No issuer certificate found

  Message Description: No issuer certificate

  Local Target Message Format: <timestamp> <seq_num>IPSec No issuer certificate found ERROR No issuer certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec No issuer certificate found ERROR No issuer certificate, <log details>

- **Message Code:** 93007

  Severity: ERROR

  Message Text: No trusted public key found

  Message Description: No trusted public key found

  Local Target Message Format: <timestamp> <seq_num>IPSec No trusted public key found ERROR No trusted public key found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>IPSec No trusted public key found ERROR No trusted public key found, <log details>

Licensing

- **Message Code:** 35000

  Severity: WARN

  Message Text: Smart Licensing registration failed

  Message Description: Smart Licensing registration failed

Local Target Message Format: <timestamp> <seq_num> 35000 WARN Licensing: Smart Licensing registration failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35000 WARN Licensing: Smart Licensing registration failed, <log details>

- **Message Code:** 35001

  Severity: WARN

  Message Text: Smart Licensing disabled

  Message Description: Smart Licensing disabled

  Local Target Message Format: <timestamp> <seq_num> 35001 WARN Licensing: Smart Licensing disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35001 WARN Licensing: Smart Licensing disabled, <log details>

- **Message Code:** 35002

  Severity: INFO

  Message Text: Smart Licensing communication failure

  Message Description: Smart Licensing communication failure

  Local Target Message Format: <timestamp> <seq_num> 35002 INFO Licensing: Smart Licensing communication failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35002 INFO Licensing: Smart Licensing communication failure, <log details>

- **Message Code:** 35003

  Severity: INFO

  Message Text: Smart Licensing communication restored

  Message Description: Smart Licensing communication restored

  Local Target Message Format: <timestamp> <seq_num> 35003 INFO Licensing: Smart Licensing communication restored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35003 INFO Licensing: Smart Licensing communication restored, <log details>

- **Message Code:** 35004

  Severity: INFO

  Message Text: Smart Licensing Id Certificate renew failure

  Message Description: Smart Licensing Id Certificate renew failure

Local Target Message Format: <timestamp> <seq_num> 35004 INFO Licensing: Smart Licensing Id Certificate renew failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35004 INFO Licensing: Smart Licensing Id Certificate renew failure, <log details>

- **Message Code:** 35005

  Severity: INFO

  Message Text: Smart Licensing Id Certificate renew success

  Message Description: Smart Licensing Id Certificate renew success

  Local Target Message Format: <timestamp> <seq_num> 35005 INFO Licensing: Smart Licensing Id Certificate renew success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35005 INFO Licensing: Smart Licensing Id Certificate renew success, <log details>

- **Message Code:** 35006

  Severity: WARN

  Message Text: Smart Licensing Agent is Out Of Compliance

  Message Description: Smart Licensing Agent is Out Of Compliance

  Local Target Message Format: <timestamp> <seq_num> 35006 WARN Licensing: Smart Licensing Agent is Out Of Compliance, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35006 WARN Licensing: Smart Licensing Agent is Out Of Compliance, <log details>

- **Message Code:** 35007

  Severity: WARN

  Message Text: Smart Licensing evaluation period expired

  Message Description: Smart Licensing evaluation period expired

  Local Target Message Format: <timestamp> <seq_num> 35007 WARN Licensing: Smart Licensing evaluation period expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35007 WARN Licensing: Smart Licensing evaluation period expired, <log details>

- **Message Code:** 35008

  Severity: WARN

  Message Text: Smart Licensing authorization expired

  Message Description: Smart Licensing authorization expired

Local Target Message Format: <timestamp> <seq_num> 35008 WARN Licensing: Smart Licensing authorization expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35008 WARN Licensing: Smart Licensing authorization expired, <log details>

- **Message Code:** 35009

  Severity: WARN

  Message Text: Invalid Smart Licensing request issued

  Message Description: Invalid Smart Licensing request issued

  Local Target Message Format: <timestamp> <seq_num> 35009 WARN Licensing: Invalid Smart Licensing request issued, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35009 WARN Licensing: Invalid Smart Licensing request issued, <log details>

- **Message Code:** 35010

  Severity: WARN

  Message Text: License is set to expire soon

  Message Description: A License that is currently installed in the ISE Deployment is set to expire soon.

  Local Target Message Format: <timestamp> <seq_num> 35010 WARN Licensing: License is set to expire soon, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35010 WARN Licensing: License is set to expire soon, <log details>

- **Message Code:** 35011

  Severity: ERROR

  Message Text: License expired

  Message Description: A License in the ISE Deployment has expired.

  Local Target Message Format: <timestamp> <seq_num> 35011 ERROR Licensing: License expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35011 ERROR Licensing: License expired, <log details>

- **Message Code:** 35012

  Severity: WARN

  Message Text: Device count exceeded for base license

  Message Description: Device count exceeded for base license. Upgrade to large deployment required.

Local Target Message Format: <timestamp> <seq_num> 35012 WARN Licensing: Device count exceeded for base license, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35012 WARN Licensing: Device count exceeded for base license, <log details>

- **Message Code:** 35013

  Severity: ERROR

  Message Text: License deletion failed

  Message Description: License deletion failed

  Local Target Message Format: <timestamp> <seq_num> 35013 ERROR Licensing: License deletion failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35013 ERROR Licensing: License deletion failed, <log details>

- **Message Code:** 35014

  Severity: ERROR

  Message Text: License create failed

  Message Description: License create failed

  Local Target Message Format: <timestamp> <seq_num> 35014 ERROR Licensing: License create failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35014 ERROR Licensing: License create failed, <log details>

- **Message Code:** 35015

  Severity: ERROR

  Message Text: License update failed

  Message Description: License update failed

  Local Target Message Format: <timestamp> <seq_num> 35015 ERROR Licensing: License update failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35015 ERROR Licensing: License update failed, <log details>

- **Message Code:** 35016

  Severity: INFO

  Message Text: Smart Licensing registration success

  Message Description: Smart Licensing registration success

Local Target Message Format: <timestamp> <seq_num> 35016 INFO Licensing: Smart Licensing registration success, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35016 INFO Licensing: Smart Licensing registration success, <log details>

- **Message Code:** 35017

  Severity: INFO

  Message Text: Smart Licensing authorization renewal success

  Message Description: Smart Licensing authorization renewal success

  Local Target Message Format: <timestamp> <seq_num> 35017 INFO Licensing: Smart Licensing authorization renewal success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35017 INFO Licensing: Smart Licensing authorization renewal success, <log details>

- **Message Code:** 35018

  Severity: WARN

  Message Text: Smart Licensing authorization renewal failure

  Message Description: Smart Licensing authorization renewal failure

  Local Target Message Format: <timestamp> <seq_num> 35018 WARN Licensing: Smart Licensing authorization renewal failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35018 WARN Licensing: Smart Licensing authorization renewal failure, <log details>

- **Message Code:** 35019

  Severity: INFO

  Message Text: Smart Licensing de-registration success

  Message Description: Smart Licensing de-registration success

  Local Target Message Format: <timestamp> <seq_num> 35019 INFO Licensing: Smart Licensing de-registration success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35019 INFO Licensing: Smart Licensing de-registration success, <log details>

- **Message Code:** 35020

  Severity: WARN

  Message Text: Smart Licensing de-registration failure

  Message Description: Smart Licensing de-registration failure

Local Target Message Format: <timestamp> <seq_num> 35020 WARN Licensing: Smart Licensing de-registration failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35020 WARN Licensing: Smart Licensing de-registration failure, <log details>

- **Message Code:** 35021

  Severity: WARN

  Message Text: Smart Licensing id certificate expired

  Message Description: Smart Licensing id certificate expired

  Local Target Message Format: <timestamp> <seq_num> 35021 WARN Licensing: Smart Licensing id certificate expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35021 WARN Licensing: Smart Licensing id certificate expired, <log details>

- **Message Code:** 35022

  Severity: INFO

  Message Text: Smart Licensing HA Role changed

  Message Description: Smart Licensing HA Role changed

  Local Target Message Format: <timestamp> <seq_num> 35022 INFO Licensing: Smart Licensing HA Role changed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35022 INFO Licensing: Smart Licensing HA Role changed, <log details>

- **Message Code:** 35023

  Severity: INFO

  Message Text: License expiring within 90 Days

  Message Description: License expiring within 90 Days

  Local Target Message Format: <timestamp> <seq_num> 35023 INFO Licensing: License expiring within 90 Days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35023 INFO Licensing: License expiring within 90 Days, <log details>

- **Message Code:** 35024

  Severity: WARN

  Message Text: License expiring within 60 Days

  Message Description: License expiring within 60 Days

Local Target Message Format: <timestamp> <seq_num> 35024 WARN Licensing: License expiring within 60 Days, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35024 WARN Licensing: License expiring within 60 Days, <log details>

- **Message Code:** 35025

  Severity: ERROR

  Message Text: License expiring within 30 Days

  Message Description: License expiring within 30 Days

  Local Target Message Format: <timestamp> <seq_num> 35025 ERROR Licensing: License expiring within 30 Days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35025 ERROR Licensing: License expiring within 30 Days, <log details>

- **Message Code:** 35026

  Severity: ERROR

  Message Text: License Out of Compliance for 5 or more days

  Message Description: License Out of Compliance for 5 or more days

  Local Target Message Format: <timestamp> <seq_num> 35026 ERROR Licensing: License Out of Compliance for 5 or more days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35026 ERROR Licensing: License Out of Compliance for 5 or more days, <log details>

- **Message Code:** 35027

  Severity: ERROR

  Message Text: License Out of Compliance for 15 or more days

  Message Description: License Out of Compliance for 15 or more days

  Local Target Message Format: <timestamp> <seq_num> 35027 ERROR Licensing: License Out of Compliance for 15 or more days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35027 ERROR Licensing: License Out of Compliance for 15 or more days, <log details>

- **Message Code:** 35028

  Severity: ERROR

  Message Text: License Out of Compliance for 30 or more days

  Message Description: License Out of Compliance for 30 or more days

Local Target Message Format: <timestamp> <seq_num> 35028 ERROR Licensing: License Out of Compliance for 30 or more days, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35028 ERROR Licensing: License Out of Compliance for 30 or more days, <log details>

- **Message Code:** 35029

  Severity: ERROR

  Message Text: License Out of Compliance for more than 45 Days Services Configuration Disabled

  Message Description: License Out of Compliance for more than 45 Days Services Configuration Disabled

  Local Target Message Format: <timestamp> <seq_num> 35029 ERROR Licensing: License Out of Compliance for more than 45 Days Services Configuration Disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35029 ERROR Licensing: License Out of Compliance for more than 45 Days Services Configuration Disabled, <log details>

- **Message Code:** 35030

  Severity: WARN

  Message Text: License exceeded 100% session usage

  Message Description: License exceeded 100% session usage

  Local Target Message Format: <timestamp> <seq_num> 35030 WARN Licensing: License exceeded 100% session usage, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35030 WARN Licensing: License exceeded 100% session usage, <log details>

- **Message Code:** 35031

  Severity: ERROR

  Message Text: License exceeded 125% session usage

  Message Description: License exceeded 125% session usage

  Local Target Message Format: <timestamp> <seq_num> 35031 ERROR Licensing: License exceeded 125% session usage, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35031 ERROR Licensing: License exceeded 125% session usage, <log details>

- **Message Code:** 35032

  Severity: INFO

  Message Text: License expiring Within 90 Days

  Message Description: License expiring Within 90 Days

Local Target Message Format: <timestamp> <seq_num> 35032 INFO Licensing: License expiring Within 90 Days, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35032 INFO Licensing: License expiring Within 90 Days, <log details>

- **Message Code:** 35033

  Severity: WARN

  Message Text: License expiring Within 60 Days

  Message Description: License expiring Within 60 Days

  Local Target Message Format: <timestamp> <seq_num> 35033 WARN Licensing: License expiring Within 60 Days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35033 WARN Licensing: License expiring Within 60 Days, <log details>

- **Message Code:** 35034

  Severity: ERROR

  Message Text: License expiring Within 30 Days

  Message Description: License expiring Within 30 Days

  Local Target Message Format: <timestamp> <seq_num> 35034 ERROR Licensing: License expiring Within 30 Days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35034 ERROR Licensing: License expiring Within 30 Days, <log details>

- **Message Code:** 35035

  Severity: ERROR

  Message Text: License expired

  Message Description: License expired

  Local Target Message Format: <timestamp> <seq_num> 35035 ERROR Licensing: License expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35035 ERROR Licensing: License expired, <log details>

- **Message Code:** 35036

  Severity: INFO

  Message Text: License expiring Within 90 Days

  Message Description: License expiring Within 90 Days

Local Target Message Format: <timestamp> <seq_num> 35036 INFO Licensing: License expiring Within 90 Days, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35036 INFO Licensing: License expiring Within 90 Days, <log details>

- **Message Code:** 35037

  Severity: WARN

  Message Text: License expiring Within 60 Days

  Message Description: License expiring Within 60 Days

  Local Target Message Format: <timestamp> <seq_num> 35037 WARN Licensing: License expiring Within 60 Days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35037 WARN Licensing: License expiring Within 60 Days, <log details>

- **Message Code:** 35038

  Severity: ERROR

  Message Text: License expiring Within 30 Days

  Message Description: License expiring Within 30 Days

  Local Target Message Format: <timestamp> <seq_num> 35038 ERROR Licensing: License expiring Within 30 Days, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35038 ERROR Licensing: License expiring Within 30 Days, <log details>

- **Message Code:** 35039

  Severity: ERROR

  Message Text: License expired

  Message Description: License expired

  Local Target Message Format: <timestamp> <seq_num> 35039 ERROR Licensing: License expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 35039 ERROR Licensing: License expired, <log details>

- **Message Code:** 35040

  Severity: WARN

  Message Text: Fewer VM licenses installed than VM nodes deployed

  Message Description: The number of VM licenses installed is fewer than the number of VM nodes deployed

Local Target Message Format: <timestamp> <seq_num>35040 WARN Licensing Fewer VM licenses installed than VM nodes deployed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35040 WARN Licensing Fewer VM licenses installed than VM nodes deployed, <log details>

- **Message Code:** 35041

  Severity: WARN

  Message Text: Fewer Device Admin licenses installed than Device Admin nodes deployed

  Message Description: The number of Device Admin licenses installed is fewer than the number of Device Admin nodes deployed

  Local Target Message Format: <timestamp> <seq_num>35041 WARN Licensing Fewer Device Admin licenses installed than Device Admin nodes deployed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35041 WARN Licensing Fewer Device Admin licenses installed than Device Admin nodes deployed, <log details>

- **Message Code:** 35042

  Severity: ERROR

  Message Text: Communication to Satellite server failed

  Message Description: Communication to Satellite server failed

  Local Target Message Format: <timestamp> <seq_num>35042 ERROR Licensing Communication to Satellite server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35042 ERROR Licensing Communication to Satellite server failed, <log details>

- **Message Code:** 35043

  Severity: INFO

  Message Text: Communication to Satellite server is restored

  Message Description: Communication to Satellite server is restored

  Local Target Message Format: <timestamp> <seq_num>35043 INFO Licensing Communication to Satellite server is restored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35043 INFO Licensing Communication to Satellite server is restored, <log details>

- **Message Code:** 35044

  Severity: INFO

  Message Text: Authorization Renewal to satellite server is successful

  Message Description: Authorization Renewal to satellite server is successful

Local Target Message Format: <timestamp> <seq_num>35044 INFO Licensing Authorization Renewal to satellite server is successful, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35044 INFO Licensing Authorization Renewal to satellite server is successful, <log details>

- **Message Code:** 35045

  Severity: ERROR

  Message Text: Authorization Renewal to satellite server failed

  Message Description: Authorization Renewal to satellite server failed

  Local Target Message Format: <timestamp> <seq_num>35045 ERROR Licensing Authorization Renewal to satellite server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35045 ERROR Licensing Authorization Renewal to satellite server failed, <log details>

- **Message Code:** 35046

  Severity: INFO

  Message Text: Permanent license Reservation , Generate Reservation Code Success

  Message Description: Permanent license Reservation , Generate Reservation Code Success

  Local Target Message Format: <timestamp> <seq_num>35046 INFO Licensing Permanent license Reservation , Generate Reservation Code Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35046 INFO Licensing Permanent license Reservation , Generate Reservation Code Success, <log details>

- **Message Code:** 35047

  Severity: INFO

  Message Text: Permanent license Reservation , Authorization Code Installation Success

  Message Description: Permanent license Reservation , Authorization Code Installation Success

  Local Target Message Format: <timestamp> <seq_num>35047 INFO Licensing Permanent license Reservation , Authorization Code Installation Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35047 INFO Licensing Permanent license Reservation , Authorization Code Installation Success, <log details>

- **Message Code:** 35048

  Severity: INFO

  Message Text: Permanent license Reservation , Reservation Failed

  Message Description: Permanent license Reservation , Reservation Failed

Local Target Message Format: <timestamp> <seq_num>35048 INFO Licensing Permanent license Reservation , Reservation Failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35048 INFO Licensing Permanent license Reservation , Reservation Failed, <log details>

- **Message Code:** 35049

  Severity: INFO

  Message Text: Permanent license Reservation , Return Reservation Success

  Message Description: Permanent license Reservation , Return Reservation Success

  Local Target Message Format: <timestamp> <seq_num>35049 INFO Licensing Permanent license Reservation , Return Reservation Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35049 INFO Licensing Permanent license Reservation , Return Reservation Success, <log details>

- **Message Code:** 35050

  Severity: INFO

  Message Text: Permanent license Reservation , Disabled Successfully.

  Message Description: Permanent license Reservation , Disabled Successfully

  Local Target Message Format: <timestamp> <seq_num>35050 INFO Licensing Permanent license Reservation , Disabled Successfully., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35050 INFO Licensing Permanent license Reservation , Disabled Successfully., <log details>

- **Message Code:** 35051

  Severity: INFO

  Message Text: Specific license Reservation , Generate Reservation Code Success

  Message Description: Specific license Reservation , Generate Reservation Code Success

  Local Target Message Format: <timestamp> <seq_num>35051 INFO Licensing Specific license Reservation , Generate Reservation Code Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35051 INFO Licensing Specific license Reservation , Generate Reservation Code Success, <log details>

- **Message Code:** 35052

  Severity: INFO

  Message Text: Specific license Reservation , Upload SLR Key Success

  Message Description: Specific license Reservation , Upload SLR Key Success

Local Target Message Format: <timestamp> <seq_num>35052 INFO Licensing Specific license Reservation , Upload SLR Key Success, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35052 INFO Licensing Specific license Reservation , Upload SLR Key Success, <log details>

- **Message Code:** 35053

  Severity: INFO

  Message Text: Specific license Reservation , Reservation Failed

  Message Description: Specific license Reservation , Reservation Failed

  Local Target Message Format: <timestamp> <seq_num>35053 INFO Licensing Specific license Reservation , Reservation Failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35053 INFO Licensing Specific license Reservation , Reservation Failed, <log details>

- **Message Code:** 35054

  Severity: INFO

  Message Text: Specific license Reservation , Return Reservation Success

  Message Description: Specific license Reservation , Return Reservation Success

  Local Target Message Format: <timestamp> <seq_num>35054 INFO Licensing Specific license Reservation , Return Reservation Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35054 INFO Licensing Specific license Reservation , Return Reservation Success, <log details>

- **Message Code:** 35055

  Severity: INFO

  Message Text: Specific license Reservation , Disabled Successfully.

  Message Description: Specific license Reservation , Disabled Successfully

  Local Target Message Format: <timestamp> <seq_num>35055 INFO Licensing Specific license Reservation , Disabled Successfully., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>35055 INFO Licensing Specific license Reservation , Disabled Successfully., <log details>

MDM Diagnostics

- **Message Code:** 89200

  Severity: ERROR

Message Text: Invalid payload encountered in inmobile device enrollment request.

Message Description: Indicates that the enrollment request contains an invalid payload.

Local Target Message Format: <timestamp> <seq_num> 89200 ERROR MDM: Invalid payload encountered in inmobile device enrollment request., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89200 ERROR MDM: Invalid payload encountered in inmobile device enrollment request., <log details>

- **Message Code:** 89201

  Severity: ERROR

  Message Text: Invalid session encountered in mobile device enrollment request.

  Message Description: Indicates that the enrollment request contains invalid session information.

  Local Target Message Format: <timestamp> <seq_num> 89201 ERROR MDM: Invalid session encountered in mobile device enrollment request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89201 ERROR MDM: Invalid session encountered in mobile device enrollment request., <log details>

- **Message Code:** 89202

  Severity: ERROR

  Message Text: Authentication failure encountered while handling mobile device enrollment request.

  Message Description: Indicates that the enrollment request has failed due to authentication failure.

  Local Target Message Format: <timestamp> <seq_num> 89202 ERROR MDM: Authentication failure encountered while handling mobile device enrollment request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89202 ERROR MDM: Authentication failure encountered while handling mobile device enrollment request., <log details>

- **Message Code:** 89203

  Severity: ERROR

  Message Text: Authorization failure encountered while handling mobile device enrollment request.

  Message Description: Indicates that the enrollment request contains invalid authorization information.

  Local Target Message Format: <timestamp> <seq_num> 89203 ERROR MDM: Authorization failure encountered while handling mobile device enrollment request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89203 ERROR MDM: Authorization failure encountered while handling mobile device enrollment request., <log details>

- **Message Code:** 89204

  Severity: ERROR

Message Text: Authorization failure encountered while handling mobile device enrollment request. The user must uninstall the iOS MDM profile before retrying the enrollment.

Message Description: Indicates that the enrollment request contains invalid authorization information. The user must uninstall the iOS MDM profile before retrying the enrollment.

Local Target Message Format: <timestamp> <seq_num> 89204 ERROR MDM: Authorization failure encountered while handling mobile device enrollment request. The user must uninstall the iOS MDM profile before retrying the enrollment., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89204 ERROR MDM: Authorization failure encountered while handling mobile device enrollment request. The user must uninstall the iOS MDM profile before retrying the enrollment., <log details>

- **Message Code:** 89205

  Severity: ERROR

  Message Text: Internal error encountered while handling mobile device enrollment request.

  Message Description: Indicates that the enrollment request has failed due to an ISE internal error.

  Local Target Message Format: <timestamp> <seq_num> 89205 ERROR MDM: Internal error encountered while handling mobile device enrollment request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89205 ERROR MDM: Internal error encountered while handling mobile device enrollment request., <log details>

- **Message Code:** 89206

  Severity: ERROR

  Message Text: Mobile device enrollment attempt has expired.

  Message Description: Indicates that the enrollment attempt did not complete within an acceptable time frame.

  Local Target Message Format: <timestamp> <seq_num> 89206 ERROR MDM: Mobile device enrollment attempt has expired., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89206 ERROR MDM: Mobile device enrollment attempt has expired., <log details>

- **Message Code:** 89207

  Severity: ERROR

  Message Text: Unsupported mobile device platform encountered while handling enrollment request.

  Message Description: Indicates that the mobile device does not meet the minimum platform version requirements. The platform version is included in the event details.

  Local Target Message Format: <timestamp> <seq_num> 89207 ERROR MDM: Unsupported mobile device platform encountered while handling enrollment request., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89207 ERROR MDM: Unsupported mobile device platform encountered while handling enrollment request., <log details>

- **Message Code:** 89208

  Severity: ERROR

  Message Text: Maximum number of authentication attempts has been exceeded.

  Message Description: Indicates that the maximum number of authentication attempts has been exceeded during enrollment.

  Local Target Message Format: <timestamp> <seq_num> 89208 ERROR MDM: Maximum number of authentication attempts has been exceeded., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89208 ERROR MDM: Maximum number of authentication attempts has been exceeded., <log details>

- **Message Code:** 89209

  Severity: ERROR

  Message Text: Mobile device enrollment request failed due to no matching MDM profile.

  Message Description: Indicates that no MDM profile is configured for this mobile device.

  Local Target Message Format: <timestamp> <seq_num> 89209 ERROR MDM: Mobile device enrollment request failed due to no matching MDM profile., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89209 ERROR MDM: Mobile device enrollment request failed due to no matching MDM profile., <log details>

- **Message Code:** 89210

  Severity: ERROR

  Message Text: Mobile device enrollment request failed due to unconfigured MDM trust anchor

  Message Description: Indicates that the MDM trust anchor has not been configured. The device cannot be enrolled.

  Local Target Message Format: <timestamp> <seq_num> 89210 ERROR MDM: Mobile device enrollment request failed due to unconfigured MDM trust anchor, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89210 ERROR MDM: Mobile device enrollment request failed due to unconfigured MDM trust anchor, <log details>

- **Message Code:** 89211

  Severity: ERROR

  Message Text: Invalid payload encountered in inmobile device check-in request.

  Message Description: Indicates that the check-in request contains an invalid payload.

  Local Target Message Format: <timestamp> <seq_num> 89211 ERROR MDM: Invalid payload encountered in inmobile device check-in request., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89211 ERROR MDM: Invalid payload encountered in inmobile device check-in request., <log details>

- **Message Code:** 89212

  Severity: ERROR

  Message Text: Unsupported mobile device platform encountered while handling check-in request.

  Message Description: Indicates that the mobile device does not meet the minimum platform version requirements. The platform version is included in the event details.

  Local Target Message Format: <timestamp> <seq_num> 89212 ERROR MDM: Unsupported mobile device platform encountered while handling check-in request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89212 ERROR MDM: Unsupported mobile device platform encountered while handling check-in request., <log details>

- **Message Code:** 89213

  Severity: ERROR

  Message Text: Profile signing failed.

  Message Description: Indicates that the cryptographic signing of the profile via the configured profile signing certificate has failed.

  Local Target Message Format: <timestamp> <seq_num> 89213 ERROR MDM: Profile signing failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89213 ERROR MDM: Profile signing failed., <log details>

- **Message Code:** 89214

  Severity: ERROR

  Message Text: Profile encryption failed.

  Message Description: Indicates that the cryptographic encryption of the profile has failed.

  Local Target Message Format: <timestamp> <seq_num> 89214 ERROR MDM: Profile encryption failed., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89214 ERROR MDM: Profile encryption failed., <log details>

- **Message Code:** 89215

  Severity: ERROR

  Message Text: Invalid payload encountered while handling profile provisioning request.

  Message Description: Indicates that the profile provisioning request has failed due to an invalid payload being encountered.

Local Target Message Format: <timestamp> <seq_num> 89215 ERROR MDM: Invalid payload encountered while handling profile provisioning request., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89215 ERROR MDM: Invalid payload encountered while handling profile provisioning request., <log details>

- **Message Code:** 89216

  Severity: ERROR

  Message Text: Authorization failure encountered while handling profile provisioning request.

  Message Description: Indicates that the profile provisioning request has failed due to an authorization failure.

  Local Target Message Format: <timestamp> <seq_num> 89216 ERROR MDM: Authorization failure encountered while handling profile provisioning request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89216 ERROR MDM: Authorization failure encountered while handling profile provisioning request., <log details>

- **Message Code:** 89217

  Severity: ERROR

  Message Text: Internal error encountered while handling profile provisioning request.

  Message Description: Indicates that the profile provisioning request has failed due to an ISE internal error.

  Local Target Message Format: <timestamp> <seq_num> 89217 ERROR MDM: Internal error encountered while handling profile provisioning request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89217 ERROR MDM: Internal error encountered while handling profile provisioning request., <log details>

- **Message Code:** 89218

  Severity: ERROR

  Message Text: Profile signing failed due to misconfiguration of the MDM certificate.

  Message Description: Indicates that the cryptographic signing of the profile has failed due to misconfiguration of the MDM certificate chain.

  Local Target Message Format: <timestamp> <seq_num> 89218 ERROR MDM: Profile signing failed due to misconfiguration of the MDM certificate., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89218 ERROR MDM: Profile signing failed due to misconfiguration of the MDM certificate., <log details>

- **Message Code:** 89219

  Severity: ERROR

  Message Text: The application request timed out.

Message Description: Indicates that the application request has timed out.

Local Target Message Format: <timestamp> <seq_num> 89219 ERROR MDM: The application request timed out., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89219 ERROR MDM: The application request timed out., <log details>

- **Message Code:** 89220

  Severity: ERROR

  Message Text: Internal error encountered while handling application request.

  Message Description: Indicates that the application request has failed due to an ISE internal error.

  Local Target Message Format: <timestamp> <seq_num> 89220 ERROR MDM: Internal error encountered while handling application request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89220 ERROR MDM: Internal error encountered while handling application request., <log details>

- **Message Code:** 89221

  Severity: ERROR

  Message Text: The profile request timed out

  Message Description: Indicates that the profile request has timed out

  Local Target Message Format: <timestamp> <seq_num> 89221 ERROR MDM: The profile request timed out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89221 ERROR MDM: The profile request timed out, <log details>

- **Message Code:** 89222

  Severity: ERROR

  Message Text: Maximum number of token resets exceeded

  Message Description: Indicates the user has exceeded the maximum number of token reset attempts and needs to wait until they can reset their token again

  Local Target Message Format: <timestamp> <seq_num> 89222 ERROR MDM: Maximum number of token resets exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89222 ERROR MDM: Maximum number of token resets exceeded, <log details>

- **Message Code:** 89223

  Severity: ERROR

  Message Text: Failed to send token

Message Description: Indicates a token could not be sent to the user using the configured SMS or email information

Local Target Message Format: <timestamp> <seq_num> 89223 ERROR MDM: Failed to send token, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89223 ERROR MDM: Failed to send token, <log details>

- **Message Code:** 89224

  Severity: ERROR

  Message Text: Token configurations are incomplete

  Message Description: Indicates token configurations are incomplete. Please ensure SMS or email information has been configured for the user

  Local Target Message Format: <timestamp> <seq_num> 89224 ERROR MDM: Token configurations are incomplete, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 89224 ERROR MDM: Token configurations are incomplete, <log details>

My Devices

- **Message Code:** 88000

  Severity: INFO

  Message Text: Successfully added a device (endpoint)

  Message Description: Successfully added a device (endpoint)

  Local Target Message Format: <timestamp> <seq_num> 88000 INFO MyDevices: Successfully added a device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88000 INFO MyDevices: Successfully added a device (endpoint), <log details>

- **Message Code:** 88001

  Severity: ERROR

  Message Text: Failed to added a device (endpoint)

  Message Description: Please verify that the MAC Address format is valid and that the MAC Address is not already registered

  Local Target Message Format: <timestamp> <seq_num> 88001 ERROR MyDevices: Failed to added a device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88001 ERROR MyDevices: Failed to added a device (endpoint), <log details>

- **Message Code:** 88002

  Severity: INFO

  Message Text: Successfully modified the device (endpoint)

  Message Description: Successfully modified the device (endpoint)

  Local Target Message Format: <timestamp> <seq_num> 88002 INFO MyDevices: Successfully modified the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88002 INFO MyDevices: Successfully modified the device (endpoint), <log details>

- **Message Code:** 88003

  Severity: ERROR

  Message Text: Failed to modify the device (endpoint)

  Message Description: Endpoint may not exist or there is a communication error with server/db. Please contact your Administrator

  Local Target Message Format: <timestamp> <seq_num> 88003 ERROR MyDevices: Failed to modify the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88003 ERROR MyDevices: Failed to modify the device (endpoint), <log details>

- **Message Code:** 88004

  Severity: INFO

  Message Text: Successfully deleted the device (endpoint)

  Message Description: Successfully deleted the device (endpoint)

  Local Target Message Format: <timestamp> <seq_num> 88004 INFO MyDevices: Successfully deleted the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88004 INFO MyDevices: Successfully deleted the device (endpoint), <log details>

- **Message Code:** 88005

  Severity: ERROR

  Message Text: Failed to delete the device (endpoint)

  Message Description: Endpoint may not exist or there is a communication error with server/db. Please contact your Administrator

  Local Target Message Format: <timestamp> <seq_num> 88005 ERROR MyDevices: Failed to delete the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88005 ERROR MyDevices: Failed to delete the device (endpoint), <log details>

- **Message Code:** 88006

  Severity: INFO

  Message Text: Successfully blacklisted the device (endpoint)

  Message Description: Successfully blacklisted the device (endpoint)

  Local Target Message Format: <timestamp> <seq_num> 88006 INFO MyDevices: Successfully blacklisted the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88006 INFO MyDevices: Successfully blacklisted the device (endpoint), <log details>

- **Message Code:** 88007

  Severity: ERROR

  Message Text: Failed to blacklist the device (endpoint)

  Message Description: Endpoint may not exist or there is a communication error with server/db. Please contact your Administrator

  Local Target Message Format: <timestamp> <seq_num> 88007 ERROR MyDevices: Failed to blacklist the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88007 ERROR MyDevices: Failed to blacklist the device (endpoint), <log details>

- **Message Code:** 88008

  Severity: INFO

  Message Text: Successfully reinstated the device (endpoint)

  Message Description: Successfully reinstated the device (endpoint)

  Local Target Message Format: <timestamp> <seq_num> 88008 INFO MyDevices: Successfully reinstated the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88008 INFO MyDevices: Successfully reinstated the device (endpoint), <log details>

- **Message Code:** 88009

  Severity: ERROR

  Message Text: Failed to reinstate the device (endpoint)

  Message Description: Endpoint may not exist or there is a communication error with server/db. Please contact your Administrator

  Local Target Message Format: <timestamp> <seq_num> 88009 ERROR MyDevices: Failed to reinstate the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88009 ERROR MyDevices: Failed to reinstate the device (endpoint), <log details>

- **Message Code:** 88010

  Severity: INFO

  Message Text: Successfully registered/provisioned the device (endpoint)

  Message Description: Successfully registered/provisioned the device (endpoint)

  Local Target Message Format: <timestamp> <seq_num> 88010 INFO MyDevices: Successfully registered/provisioned the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88010 INFO MyDevices: Successfully registered/provisioned the device (endpoint), <log details>

- **Message Code:** 88011

  Severity: ERROR

  Message Text: Failed to register/provision the device (endpoint)

  Message Description: Please contact your Administrator

  Local Target Message Format: <timestamp> <seq_num> 88011 ERROR MyDevices: Failed to register/provision the device (endpoint), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88011 ERROR MyDevices: Failed to register/provision the device (endpoint), <log details>

- **Message Code:** 88012

  Severity: INFO

  Message Text: Successfully performed a CoA termination

  Message Description: Successfully performed a CoA termination

  Local Target Message Format: <timestamp> <seq_num> 88012 INFO MyDevices: Successfully performed a CoA termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88012 INFO MyDevices: Successfully performed a CoA termination, <log details>

- **Message Code:** 88013

  Severity: ERROR

  Message Text: Failed to perform a CoA termination

  Message Description: Please make sure that the NAD is configured to send the client MAC Address when making RADIUS access-requests to ISE.

  Local Target Message Format: <timestamp> <seq_num> 88013 ERROR MyDevices: Failed to perform a CoA termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88013 ERROR MyDevices: Failed to perform a CoA termination, <log details>

- **Message Code:** 88014

  Severity: INFO

  Message Text: Successfully performed a CoA re-authentication

  Message Description: Successfully performed a CoA re-authentication

  Local Target Message Format: <timestamp> <seq_num> 88014 INFO MyDevices: Successfully performed a CoA re-authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88014 INFO MyDevices: Successfully performed a CoA re-authentication, <log details>

- **Message Code:** 88015

  Severity: ERROR

  Message Text: Failed to perform a CoA re-authentication

  Message Description: Please contact your administrator

  Local Target Message Format: <timestamp> <seq_num> 88015 ERROR MyDevices: Failed to perform a CoA re-authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 88015 ERROR MyDevices: Failed to perform a CoA re-authentication, <log details>

Passed Authentications

- **Message Code:** 5200

  Severity: NOTICE

  Message Text: Authentication succeeded

  Message Description: User authentication ended successfully (RADIUS)

  Local Target Message Format: <timestamp> <seq_num> 5200 NOTICE Passed-Authentication: Authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5200 NOTICE Passed-Authentication: Authentication succeeded, <log details>

- **Message Code:** 5201

  Severity: NOTICE

  Message Text: Authentication succeeded

  Message Description: User authentication ended successfully (TACACS)

  Local Target Message Format: <timestamp> <seq_num> 5201 NOTICE Passed-Authentication: Authentication succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5201 NOTICE Passed-Authentication: Authentication succeeded, <log details>

- **Message Code:** 5202

  Severity: NOTICE

  Message Text: Command Authorization succeeded

  Message Description: The requested Command Authorization passed

  Local Target Message Format: <timestamp> <seq_num> 5202 NOTICE Device-Administration: Command Authorization succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5202 NOTICE Device-Administration: Command Authorization succeeded, <log details>

- **Message Code:** 5203

  Severity: NOTICE

  Message Text: Session Authorization succeeded

  Message Description: The requested Session Authorization passed

  Local Target Message Format: <timestamp> <seq_num> 5203 NOTICE Device-Administration: Session Authorization succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5203 NOTICE Device-Administration: Session Authorization succeeded, <log details>

- **Message Code:** 5204

  Severity: NOTICE

  Message Text: Change password succeeded

  Message Description: User change password ended successfully

  Local Target Message Format: <timestamp> <seq_num> 5204 NOTICE Passed-Authentication: Change password succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5204 NOTICE Passed-Authentication: Change password succeeded, <log details>

- **Message Code:** 5205

  Severity: NOTICE

  Message Text: Dynamic Authorization succeeded

  Message Description: Dynamic Authorization succeeded

  Local Target Message Format: <timestamp> <seq_num> 5205 NOTICE Dynamic-Authorization: Dynamic Authorization succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5205 NOTICE Dynamic-Authorization: Dynamic Authorization succeeded, <log details>

- **Message Code:** 5206

  Severity: NOTICE

  Message Text: PAC provisioned

  Message Description: Access rejected after successful in-band PAC provisioning

  Local Target Message Format: <timestamp> <seq_num> 5206 NOTICE Passed-Authentication: PAC provisioned, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5206 NOTICE Passed-Authentication: PAC provisioned, <log details>

- **Message Code:** 5207

  Severity: NOTICE

  Message Text: PAC-less Authenticated

  Message Description: Access rejected after successful PAC-less authentication

  Local Target Message Format: <timestamp> <seq_num>Passed-Authentication PAC-less Authenticated NOTICE Access rejected after successful PAC-less authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Passed-Authentication PAC-less Authenticated NOTICE Access rejected after successful PAC-less authentication, <log details>

- **Message Code:** 5208

  Severity: NOTICE

  Message Text: PAC provisioned

  Message Description: PAC-less failed

  Local Target Message Format: <timestamp> <seq_num>Failed-Attempt PAC provisioned NOTICE PAC-less failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Failed-Attempt PAC provisioned NOTICE PAC-less failed, <log details>

- **Message Code:** 5231

  Severity: NOTICE

  Message Text: Guest Authentication Passed

  Message Description: Guest Authentication Passed

  Local Target Message Format: <timestamp> <seq_num> 5231 NOTICE Guest: Guest Authentication Passed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5231 NOTICE Guest: Guest Authentication Passed, <log details>

- **Message Code:** 5232

  Severity: NOTICE

  Message Text: DACL Download Succeeded

  Message Description: DACL Download Succeeded

  Local Target Message Format: <timestamp> <seq_num> 5232 NOTICE Passed-Authentication: DACL Download Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5232 NOTICE Passed-Authentication: DACL Download Succeeded, <log details>

- **Message Code:** 5233

  Severity: NOTICE

  Message Text: TrustSec Data Download Succeeded

  Message Description: TrustSec Data Download Succeeded

  Local Target Message Format: <timestamp> <seq_num> 5233 NOTICE Passed-Authentication: TrustSec Data Download Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5233 NOTICE Passed-Authentication: TrustSec Data Download Succeeded, <log details>

- **Message Code:** 5234

  Severity: NOTICE

  Message Text: TrustSec Peer Policy Download Succeeded

  Message Description: TrustSec Peer Policy Download Succeeded

  Local Target Message Format: <timestamp> <seq_num> 5234 NOTICE Passed-Authentication: TrustSec Peer Policy Download Succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5234 NOTICE Passed-Authentication: TrustSec Peer Policy Download Succeeded, <log details>

- **Message Code:** 5236

  Severity: NOTICE

  Message Text: Authorize-Only succeeded

  Message Description: Authorize-Only ended successfully

  Local Target Message Format: <timestamp> <seq_num> 5236 NOTICE Passed-Authentication: Authorize-Only succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5236 NOTICE Passed-Authentication: Authorize-Only succeeded, <log details>

- **Message Code:** 5237

  Severity: NOTICE

  Message Text: Device Registration Web Authentication Passed

  Message Description: Device Registration Web Authentication passed

  Local Target Message Format: <timestamp> <seq_num> 5237 NOTICE Guest: Device Registration Web Authentication Passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5237 NOTICE Guest: Device Registration Web Authentication Passed, <log details>

- **Message Code:** 5238

  Severity: WARN

  Message Text: Endpoint authentication problem was fixed

  Message Description: Endpoint authentication problem was fixed

  Local Target Message Format: <timestamp> <seq_num> 5238 WARN RADIUS: Endpoint authentication problem was fixed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5238 WARN RADIUS: Endpoint authentication problem was fixed, <log details>

- **Message Code:** 5239

  Severity: WARN

  Message Text: NAS problem was fixed

  Message Description: NAS problem was fixed

  Local Target Message Format: <timestamp> <seq_num> 5239 WARN RADIUS: NAS problem was fixed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5239 WARN RADIUS: NAS problem was fixed, <log details>

- **Message Code:** 5240

  Severity: INFO

  Message Text: Previously rejected endpoint was released to continue authentications

  Message Description: Previously rejected endpoint was released to continue authentications

  Local Target Message Format: <timestamp> <seq_num> 5240 INFO RADIUS: Previously rejected endpoint was released to continue authentications, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5240 INFO RADIUS: Previously rejected endpoint was released to continue authentications, <log details>

- **Message Code:** 5241

  Severity: NOTICE

  Message Text: RADIUS DTLS handshake succeeded

  Message Description: RADIUS DTLS handshake succeeded

  Local Target Message Format: <timestamp> <seq_num> 5241 NOTICE Passed-Authentication: RADIUS DTLS handshake succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 5241 NOTICE Passed-Authentication: RADIUS DTLS handshake succeeded, <log details>

Passive ID

- **Message Code:** 90046

  Severity: ERROR

  Message Text: Internal error

  Message Description: Internal error

  Local Target Message Format: <timestamp> <seq_num> 90046 ERROR PassiveID: Internal error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90046 ERROR PassiveID: Internal error, <log details>

- **Message Code:** 90047

  Severity: INFO

  Message Text: PassiveID is now the primary node

  Message Description: PassiveID is now the primary node

  Local Target Message Format: <timestamp> <seq_num> 90047 INFO PassiveID: PassiveID is now the primary node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90047 INFO PassiveID: PassiveID is now the primary node, <log details>

- **Message Code:** 90048

  Severity: INFO

  Message Text: PassiveID is no longer the primary node

  Message Description: PassiveID is no longer the primary node

Local Target Message Format: <timestamp> <seq_num> 90048 INFO PassiveID: PassiveID is no longer the primary node, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90048 INFO PassiveID: PassiveID is no longer the primary node, <log details>

- **Message Code:** 90049

  Severity: INFO

  Message Text: PassiveID primary node was elected

  Message Description: PassiveID primary node was elected

  Local Target Message Format: <timestamp> <seq_num> 90049 INFO PassiveID: PassiveID primary node was elected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90049 INFO PassiveID: PassiveID primary node was elected, <log details>

- **Message Code:** 90050

  Severity: ERROR

  Message Text: PassiveID primary node is not responsive

  Message Description: PassiveID primary node is not responsive

  Local Target Message Format: <timestamp> <seq_num> 90050 ERROR PassiveID: PassiveID primary node is not responsive, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90050 ERROR PassiveID: PassiveID primary node is not responsive, <log details>

- **Message Code:** 90051

  Severity: INFO

  Message Text: Service started

  Message Description: Service started

  Local Target Message Format: <timestamp> <seq_num> 90051 INFO PassiveID: Service started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90051 INFO PassiveID: Service started, <log details>

- **Message Code:** 90052

  Severity: ERROR

  Message Text: Keep alive between PassiveID services is unavailable

  Message Description: Keep alive between PassiveID services is unavailable

Local Target Message Format: <timestamp> <seq_num> 90052 ERROR PassiveID: Keep alive between PassiveID services is unavailable, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90052 ERROR PassiveID: Keep alive between PassiveID services is unavailable, <log details>

- **Message Code:** 90053

  Severity: ERROR

  Message Text: Cannot resolve PassiveID service name

  Message Description: Cannot resolve PassiveID service name

  Local Target Message Format: <timestamp> <seq_num> 90053 ERROR PassiveID: Cannot resolve PassiveID service name, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90053 ERROR PassiveID: Cannot resolve PassiveID service name, <log details>

- **Message Code:** 90054

  Severity: INFO

  Message Text: Active PassiveID service is set

  Message Description: Active PassiveID service is set

  Local Target Message Format: <timestamp> <seq_num> 90054 INFO PassiveID: Active PassiveID service is set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90054 INFO PassiveID: Active PassiveID service is set, <log details>

- **Message Code:** 90055

  Severity: INFO

  Message Text: Standby PassiveID service is set

  Message Description: Standby PassiveID service is set

  Local Target Message Format: <timestamp> <seq_num> 90055 INFO PassiveID: Standby PassiveID service is set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90055 INFO PassiveID: Standby PassiveID service is set, <log details>

- **Message Code:** 90056

  Severity: ERROR

  Message Text: Service cannot apply configuration, service is unavailable

  Message Description: Service cannot apply configuration, service is unavailable

Local Target Message Format: <timestamp> <seq_num> 90056 ERROR PassiveID: Service cannot apply configuration, service is unavailable, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90056 ERROR PassiveID: Service cannot apply configuration, service is unavailable, <log details>

- **Message Code:** 90057

  Severity: INFO

  Message Text: Service applied configuration

  Message Description: Service applied configuration

  Local Target Message Format: <timestamp> <seq_num> 90057 INFO PassiveID: Service applied configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90057 INFO PassiveID: Service applied configuration, <log details>

- **Message Code:** 90058

  Severity: ERROR

  Message Text: Cannot resolve hostname

  Message Description: Cannot resolve hostname

  Local Target Message Format: <timestamp> <seq_num> 90058 ERROR PassiveID: Cannot resolve hostname, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90058 ERROR PassiveID: Cannot resolve hostname, <log details>

- **Message Code:** 90059

  Severity: ERROR

  Message Text: Cannot get Domain Controller Windows version

  Message Description: Cannot get Domain Controller Windows version

  Local Target Message Format: <timestamp> <seq_num> 90059 ERROR PassiveID: Cannot get Domain Controller Windows version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90059 ERROR PassiveID: Cannot get Domain Controller Windows version, <log details>

- **Message Code:** 90060

  Severity: ERROR

  Message Text: Domain Controller Windows version is unsupported

  Message Description: Domain Controller Windows version is unsupported

Local Target Message Format: <timestamp> <seq_num> 90060 ERROR PassiveID: Domain Controller Windows version is unsupported, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90060 ERROR PassiveID: Domain Controller Windows version is unsupported, <log details>

- **Message Code:** 90061

  Severity: ERROR

  Message Text: Cannot get Domain Controller NetBIOS

  Message Description: Cannot get Domain Controller NetBIOS

  Local Target Message Format: <timestamp> <seq_num> 90061 ERROR PassiveID: Cannot get Domain Controller NetBIOS, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90061 ERROR PassiveID: Cannot get Domain Controller NetBIOS, <log details>

- **Message Code:** 90062

  Severity: ERROR

  Message Text: Cannot connect to Domain Controller

  Message Description: Cannot connect to Domain Controller

  Local Target Message Format: <timestamp> <seq_num> 90062 ERROR PassiveID: Cannot connect to Domain Controller, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90062 ERROR PassiveID: Cannot connect to Domain Controller, <log details>

- **Message Code:** 90063

  Severity: INFO

  Message Text: Successfully establish connection to Domain Controller

  Message Description: Successfully establish connection to Domain Controller

  Local Target Message Format: <timestamp> <seq_num> 90063 INFO PassiveID: Successfully establish connection to Domain Controller, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90063 INFO PassiveID: Successfully establish connection to Domain Controller, <log details>

- **Message Code:** 90064

  Severity: ERROR

  Message Text: Cannot get history login events

  Message Description: Cannot get history login events

Local Target Message Format: <timestamp> <seq_num> 90064 ERROR PassiveID: Cannot get history login events, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90064 ERROR PassiveID: Cannot get history login events, <log details>

- **Message Code:** 90065

  Severity: DEBUG

  Message Text: Received history login events

  Message Description: Received history login events

  Local Target Message Format: <timestamp> <seq_num> 90065 DEBUG PassiveID: Received history login events, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90065 DEBUG PassiveID: Received history login events, <log details>

- **Message Code:** 90066

  Severity: ERROR

  Message Text: Lost connection with Domain Controller

  Message Description: Lost connection with Domain Controller

  Local Target Message Format: <timestamp> <seq_num> 90066 ERROR PassiveID: Lost connection with Domain Controller, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90066 ERROR PassiveID: Lost connection with Domain Controller, <log details>

- **Message Code:** 90067

  Severity: DEBUG

  Message Text: Received login event

  Message Description: Received login event

  Local Target Message Format: <timestamp> <seq_num> 90067 DEBUG PassiveID: Received login event, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90067 DEBUG PassiveID: Received login event, <log details>

- **Message Code:** 90068

  Severity: DEBUG

  Message Text: Received machine login event

  Message Description: Received machine login event

Local Target Message Format: <timestamp> <seq_num> 90068 DEBUG PassiveID: Received machine login event, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90068 DEBUG PassiveID: Received machine login event, <log details>

- **Message Code:** 90069

  Severity: DEBUG

  Message Text: Replaced local IP

  Message Description: Replaced local IP

  Local Target Message Format: <timestamp> <seq_num> 90069 DEBUG PassiveID: Replaced local IP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90069 DEBUG PassiveID: Replaced local IP, <log details>

- **Message Code:** 90070

  Severity: WARN

  Message Text: Received incorrect login event

  Message Description: Received incorrect login event

  Local Target Message Format: <timestamp> <seq_num> 90070 WARN PassiveID: Received incorrect login event, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90070 WARN PassiveID: Received incorrect login event, <log details>

- **Message Code:** 90071

  Severity: WARN

  Message Text: Received unsupported login event

  Message Description: Received unsupported login event

  Local Target Message Format: <timestamp> <seq_num> 90071 WARN PassiveID: Received unsupported login event, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90071 WARN PassiveID: Received unsupported login event, <log details>

- **Message Code:** 90072

  Severity: DEBUG

  Message Text: Filtered login event

  Message Description: Filtered login event

Local Target Message Format: <timestamp> <seq_num> 90072 DEBUG PassiveID: Filtered login event, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90072 DEBUG PassiveID: Filtered login event, <log details>

- **Message Code:** 90073

  Severity: ERROR

  Message Text: Login events are being dropped as storage size has been exceeded

  Message Description: Login events are being dropped as storage size has been exceeded

  Local Target Message Format: <timestamp> <seq_num> 90073 ERROR PassiveID: Login events are being dropped as storage size has been exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90073 ERROR PassiveID: Login events are being dropped as storage size has been exceeded, <log details>

- **Message Code:** 90074

  Severity: DEBUG

  Message Text: Forwarded login event to session directory

  Message Description: Forwarded login event to session directory

  Local Target Message Format: <timestamp> <seq_num> 90074 DEBUG PassiveID: Forwarded login event to session directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90074 DEBUG PassiveID: Forwarded login event to session directory, <log details>

- **Message Code:** 90075

  Severity: ERROR

  Message Text: Cannot forward login event to session directory

  Message Description: Cannot forward login event to session directory

  Local Target Message Format: <timestamp> <seq_num> 90075 ERROR PassiveID: Cannot forward login event to session directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90075 ERROR PassiveID: Cannot forward login event to session directory, <log details>

- **Message Code:** 90076

  Severity: INFO

  Message Text: The number of events handled in the last 24 hours

  Message Description: The number of events handled in the last 24 hours

Local Target Message Format: <timestamp> <seq_num> 90076 INFO PassiveID: The number of events handled in the last 24 hours, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90076 INFO PassiveID: The number of events handled in the last 24 hours, <log details>

- **Message Code:** 90077

  Severity: DEBUG

  Message Text: The number of events handled in the last hour

  Message Description: The number of events handled in the last hour

  Local Target Message Format: <timestamp> <seq_num> 90077 DEBUG PassiveID: The number of events handled in the last hour, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90077 DEBUG PassiveID: The number of events handled in the last hour, <log details>

- **Message Code:** 90078

  Severity: INFO

  Message Text: Closed connection to Domain Controller

  Message Description: Closed connection to Domain Controller

  Local Target Message Format: <timestamp> <seq_num> 90078 INFO PassiveID: Closed connection to Domain Controller, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90078 INFO PassiveID: Closed connection to Domain Controller, <log details>

- **Message Code:** 90079

  Severity: INFO

  Message Text: Service shutdown

  Message Description: Service shutdown

  Local Target Message Format: <timestamp> <seq_num> 90079 INFO PassiveID: Service shutdown, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90079 INFO PassiveID: Service shutdown, <log details>

- **Message Code:** 90080

  Severity: NOTICE

  Message Text: PassiveID service collected details

  Message Description: PassiveID service collected details

Local Target Message Format: <timestamp> <seq_num> 90080 NOTICE PassiveID: PassiveID service collected details, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90080 NOTICE PassiveID: PassiveID service collected details, <log details>

- **Message Code:** 90081

  Severity: ERROR

  Message Text: Failed to start REST server

  Message Description: Failed to start REST server

  Local Target Message Format: <timestamp> <seq_num> 90081 ERROR PassiveID: Failed to start REST server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90081 ERROR PassiveID: Failed to start REST server, <log details>

- **Message Code:** 90082

  Severity: ERROR

  Message Text: Failed to open syslog port

  Message Description: Failed to open syslog port

  Local Target Message Format: <timestamp> <seq_num> 90082 ERROR PassiveID: Failed to open syslog port, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90082 ERROR PassiveID: Failed to open syslog port, <log details>

- **Message Code:** 90083

  Severity: NOTICE

  Message Text: Forwarded logout event to session directory

  Message Description: Forwarded logout event to session directory

  Local Target Message Format: <timestamp> <seq_num> 90083 NOTICE PassiveID: Forwarded logout event to session directory, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90083 NOTICE PassiveID: Forwarded logout event to session directory, <log details>

- **Message Code:** 90084

  Severity: INFO

  Message Text: Endpoint Probe Service is Starting

  Message Description: Endpoint Probe Service is Starting

Local Target Message Format: <timestamp> <seq_num> 90084 INFO PassiveID: Endpoint Probe Service is Starting, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90084 INFO PassiveID: Endpoint Probe Service is Starting, <log details>

- **Message Code:** 90085

  Severity: INFO

  Message Text: Endpoint Probe Service Stoped

  Message Description: Endpoint Probe Service stop

  Local Target Message Format: <timestamp> <seq_num> 90085 INFO PassiveID: Endpoint Probe Service Stoped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90085 INFO PassiveID: Endpoint Probe Service Stoped, <log details>

- **Message Code:** 90086

  Severity: FATAL

  Message Text: Endpoint Probe unexpected service termination

  Message Description: Endpoint Probe Service stop

  Local Target Message Format: <timestamp> <seq_num> 90086 FATAL PassiveID: Endpoint Probe unexpected service termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90086 FATAL PassiveID: Endpoint Probe unexpected service termination, <log details>

- **Message Code:** 90088

  Severity: INFO

  Message Text: Endpoint Probe configuration update domain admin list

  Message Description: Endpoint probe can only monitor known domain admins , list been updated

  Local Target Message Format: <timestamp> <seq_num> 90088 INFO PassiveID: Endpoint Probe configuration update domain admin list, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90088 INFO PassiveID: Endpoint Probe configuration update domain admin list, <log details>

- **Message Code:** 90089

  Severity: DEBUG

  Message Text: Endpoint Probe configuration update domain information

  Message Description: Endpoint probe can only monitor known domain admins , list been updated

Local Target Message Format: <timestamp> <seq_num> 90089 DEBUG PassiveID: Endpoint Probe configuration update domain information, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90089 DEBUG PassiveID: Endpoint Probe configuration update domain information, <log details>

- **Message Code:** 90090

  Severity: INFO

  Message Text: Endpoint Probe configuration deleted a domain admin

  Message Description: Endpoint probe can only monitor known domain admins , list been updated

  Local Target Message Format: <timestamp> <seq_num> 90090 INFO PassiveID: Endpoint Probe configuration deleted a domain admin, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90090 INFO PassiveID: Endpoint Probe configuration deleted a domain admin, <log details>

- **Message Code:** 90091

  Severity: INFO

  Message Text: Endpoint Probe service status changed to disabled

  Message Description: Endpoint Probe service status changed to disabled

  Local Target Message Format: <timestamp> <seq_num> 90091 INFO PassiveID: Endpoint Probe service status changed to disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90091 INFO PassiveID: Endpoint Probe service status changed to disabled, <log details>

- **Message Code:** 90092

  Severity: INFO

  Message Text: Endpoint Probe service status changed to enabled

  Message Description: Endpoint Probe service status changed to enabled

  Local Target Message Format: <timestamp> <seq_num> 90092 INFO PassiveID: Endpoint Probe service status changed to enabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90092 INFO PassiveID: Endpoint Probe service status changed to enabled, <log details>

- **Message Code:** 90093

  Severity: INFO

  Message Text: Endpoint Probe service status changed result with ERROR !

  Message Description: Failed to change current probe status , please check debug logs for detailed information

Local Target Message Format: <timestamp> <seq_num> 90093 INFO PassiveID: Endpoint Probe service status changed result with ERROR !, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90093 INFO PassiveID: Endpoint Probe service status changed result with ERROR !, <log details>

- **Message Code:** 90094

  Severity: INFO

  Message Text: Endpoint Probe service status changed result with ERROR !

  Message Description: Failed to change current probe status , please check debug logs for detailed information

  Local Target Message Format: <timestamp> <seq_num> 90094 INFO PassiveID: Endpoint Probe service status changed result with ERROR !, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90094 INFO PassiveID: Endpoint Probe service status changed result with ERROR !, <log details>

- **Message Code:** 90095

  Severity: INFO

  Message Text: Endpoint Probe service status changed to enabled !

  Message Description: PIC mode only , Endpoint Probe Setting set to Enabled

  Local Target Message Format: <timestamp> <seq_num> 90095 INFO PassiveID: Endpoint Probe service status changed to enabled !, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90095 INFO PassiveID: Endpoint Probe service status changed to enabled !, <log details>

- **Message Code:** 90096

  Severity: INFO

  Message Text: Endpoint Probe service status changed to disabled !

  Message Description: PIC mode only , Endpoint Probe Setting set to disabled

  Local Target Message Format: <timestamp> <seq_num> 90096 INFO PassiveID: Endpoint Probe service status changed to disabled !, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90096 INFO PassiveID: Endpoint Probe service status changed to disabled !, <log details>

- **Message Code:** 90097

  Severity: ERROR

  Message Text: Endpoint Probe configuration apply new configuration result with error

  Message Description: Create Endpoint Probe configuration was not successful. Please try service restated in order to fix the issue

Local Target Message Format: <timestamp> <seq_num> 90097 ERROR PassiveID: Endpoint Probe configuration apply new configuration result with error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90097 ERROR PassiveID: Endpoint Probe configuration apply new configuration result with error, <log details>

- **Message Code:** 90098

  Severity: ERROR

  Message Text: Endpoint Probe delete configuration result with error

  Message Description: Delete Endpoint Probe configuration was not successful. Please try service restated in order to fix the issue

  Local Target Message Format: <timestamp> <seq_num> 90098 ERROR PassiveID: Endpoint Probe delete configuration result with error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90098 ERROR PassiveID: Endpoint Probe delete configuration result with error, <log details>

- **Message Code:** 90099

  Severity: ERROR

  Message Text: Endpoint Probe update configuration result with error

  Message Description: Update Endpoint Probe configuration was not successful. Please try service restated in order to fix the issue

  Local Target Message Format: <timestamp> <seq_num> 90099 ERROR PassiveID: Endpoint Probe update configuration result with error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90099 ERROR PassiveID: Endpoint Probe update configuration result with error, <log details>

- **Message Code:** 90100

  Severity: ERROR

  Message Text: Endpoint Probe Manual Check completed with error

  Message Description: Unexpected error occur during endpoint manual check request

  Local Target Message Format: <timestamp> <seq_num> 90100 ERROR PassiveID: Endpoint Probe Manual Check completed with error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90100 ERROR PassiveID: Endpoint Probe Manual Check completed with error, <log details>

- **Message Code:** 90101

  Severity: INFO

  Message Text: Endpoint Probe Manual Check starting

  Message Description: Starting manual endpoint check

Local Target Message Format: <timestamp> <seq_num> 90101 INFO PassiveID: Endpoint Probe Manual Check starting, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90101 INFO PassiveID: Endpoint Probe Manual Check starting, <log details>

- **Message Code:** 90102

  Severity: INFO

  Message Text: Endpoint Probe Scheduler starting

  Message Description: Starting to check endpoints. Retrieving list of session to query

  Local Target Message Format: <timestamp> <seq_num> 90102 INFO PassiveID: Endpoint Probe Scheduler starting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90102 INFO PassiveID: Endpoint Probe Scheduler starting, <log details>

- **Message Code:** 90103

  Severity: DEBUG

  Message Text: Endpoint Probe complete fetching endpoint list to verify current login identity

  Message Description: Retrieved list of endpoints to query

  Local Target Message Format: <timestamp> <seq_num> 90103 DEBUG PassiveID: Endpoint Probe complete fetching endpoint list to verify current login identity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90103 DEBUG PassiveID: Endpoint Probe complete fetching endpoint list to verify current login identity, <log details>

- **Message Code:** 90104

  Severity: INFO

  Message Text: Endpoint Probe monitor check completed successfully.

  Message Description: Done querying all endpoints

  Local Target Message Format: <timestamp> <seq_num> 90104 INFO PassiveID: Endpoint Probe monitor check completed successfully., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90104 INFO PassiveID: Endpoint Probe monitor check completed successfully., <log details>

- **Message Code:** 90105

  Severity: ERROR

  Message Text: Endpoint Probe monitor check completed with ERROR

  Message Description: Endpoint check completed unsuccessfully

Local Target Message Format: <timestamp> <seq_num> 90105 ERROR PassiveID: Endpoint Probe monitor check completed with ERROR, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90105 ERROR PassiveID: Endpoint Probe monitor check completed with ERROR, <log details>

- **Message Code:** 90106

  Severity: DEBUG

  Message Text: Endpoint Probe Scheduler Manager Starting

  Message Description: Setting probe to check endpoints periodically

  Local Target Message Format: <timestamp> <seq_num> 90106 DEBUG PassiveID: Endpoint Probe Scheduler Manager Starting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90106 DEBUG PassiveID: Endpoint Probe Scheduler Manager Starting, <log details>

- **Message Code:** 90107

  Severity: DEBUG

  Message Text: Endpoint Probe Scheduler Manager canceled

  Message Description: Stopped querying new endpoints

  Local Target Message Format: <timestamp> <seq_num> 90107 DEBUG PassiveID: Endpoint Probe Scheduler Manager canceled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90107 DEBUG PassiveID: Endpoint Probe Scheduler Manager canceled, <log details>

- **Message Code:** 90108

  Severity: DEBUG

  Message Text: Endpoint Probe enabling WMI on Endpoint

  Message Description: WMI Services were not enabled on the endpoint and were enabled for further checks

  Local Target Message Format: <timestamp> <seq_num> 90108 DEBUG PassiveID: Endpoint Probe enabling WMI on Endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90108 DEBUG PassiveID: Endpoint Probe enabling WMI on Endpoint, <log details>

- **Message Code:** 90109

  Severity: DEBUG

  Message Text: Endpoint Probe failed to enable WMI on Endpoint

  Message Description: Failed to enable WMI on endpoint. Please verify Active Directory configuration credentials

Local Target Message Format: <timestamp> <seq_num> 90109 DEBUG PassiveID: Endpoint Probe failed to enable WMI on Endpoint, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90109 DEBUG PassiveID: Endpoint Probe failed to enable WMI on Endpoint, <log details>

- **Message Code:** 90110

  Severity: DEBUG

  Message Text: Endpoint Probe enabling WMI on Endpoint

  Message Description: WMI Services are not enable on endpoint will be set for further checks .

  Local Target Message Format: <timestamp> <seq_num> 90110 DEBUG PassiveID: Endpoint Probe enabling WMI on Endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90110 DEBUG PassiveID: Endpoint Probe enabling WMI on Endpoint, <log details>

- **Message Code:** 90111

  Severity: DEBUG

  Message Text: Endpoint domain admin credentials are not known for provided DOMAIN

  Message Description: chekc your PassiveID Active Directory configuration , is that a known DOMAIN ?

  Local Target Message Format: <timestamp> <seq_num> 90111 DEBUG PassiveID: Endpoint domain admin credentials are not known for provided DOMAIN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90111 DEBUG PassiveID: Endpoint domain admin credentials are not known for provided DOMAIN, <log details>

- **Message Code:** 90112

  Severity: DEBUG

  Message Text: Endpoint probe check result with user is still active

  Message Description: The current known user is still logged on

  Local Target Message Format: <timestamp> <seq_num> 90112 DEBUG PassiveID: Endpoint probe check result with user is still active, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90112 DEBUG PassiveID: Endpoint probe check result with user is still active, <log details>

- **Message Code:** 90113

  Severity: DEBUG

  Message Text: Endpoint probe check result with user is still active

  Message Description: The current known user is no longer logged on. Removing the session

Local Target Message Format: <timestamp> <seq_num> 90113 DEBUG PassiveID: Endpoint probe check result with user is still active, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90113 DEBUG PassiveID: Endpoint probe check result with user is still active, <log details>

- **Message Code:** 90114

  Severity: DEBUG

  Message Text: Endpoint probe check result with unreachable endpoint

  Message Description: Endpoint is unreachable. Please verify connectivity to endpoint

  Local Target Message Format: <timestamp> <seq_num> 90114 DEBUG PassiveID: Endpoint probe check result with unreachable endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90114 DEBUG PassiveID: Endpoint probe check result with unreachable endpoint, <log details>

- **Message Code:** 90115

  Severity: WARN

  Message Text: Endpoint Probe : DNS reverse lookup failed .

  Message Description: DNS reverse lookup is mandatory for successful monitoring of endpoints

  Local Target Message Format: <timestamp> <seq_num> 90115 WARN PassiveID: Endpoint Probe : DNS reverse lookup failed ., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90115 WARN PassiveID: Endpoint Probe : DNS reverse lookup failed ., <log details>

- **Message Code:** 90116

  Severity: INFO

  Message Text: Endpoint Probe configuration list of endpoint network subnet to monitor

  Message Description: Only endpoints that match one of the configured subnets will be monitor by this node

  Local Target Message Format: <timestamp> <seq_num> 90116 INFO PassiveID: Endpoint Probe configuration list of endpoint network subnet to monitor, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90116 INFO PassiveID: Endpoint Probe configuration list of endpoint network subnet to monitor, <log details>

- **Message Code:** 90117

  Severity: DEBUG

  Message Text: Endpoint Probe Total number of session need valid login user

  Message Description: DNS reverse lookup is mandatory in order to successful monitor endpoint login users .

Local Target Message Format: <timestamp> <seq_num> 90117 DEBUG PassiveID: Endpoint Probe Total number of session need valid login user, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90117 DEBUG PassiveID: Endpoint Probe Total number of session need valid login user, <log details>

- **Message Code:** 90118

  Severity: FATAL

  Message Text: Fatal error occourd during SYSLOG probe startup

  Message Description: Fatal error occourd during SYSLOG probe startup

  Local Target Message Format: <timestamp> <seq_num> 90118 FATAL PassiveID: Fatal error occourd during SYSLOG probe startup, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90118 FATAL PassiveID: Fatal error occourd during SYSLOG probe startup, <log details>

- **Message Code:** 90119

  Severity: INFO

  Message Text: Start listening to tcp port

  Message Description: Start listening to tcp port

  Local Target Message Format: <timestamp> <seq_num> 90119 INFO PassiveID: Start listening to tcp port, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90119 INFO PassiveID: Start listening to tcp port, <log details>

- **Message Code:** 90120

  Severity: INFO

  Message Text: Start listening to udp port

  Message Description: Start listening to udp port

  Local Target Message Format: <timestamp> <seq_num> 90120 INFO PassiveID: Start listening to udp port, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90120 INFO PassiveID: Start listening to udp port, <log details>

- **Message Code:** 90121

  Severity: INFO

  Message Text: Applied template for hostname

  Message Description: Applied template for hostname

Local Target Message Format: <timestamp> <seq_num> 90121 INFO PassiveID: Applied template for hostname, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90121 INFO PassiveID: Applied template for hostname, <log details>

- **Message Code:** 90122

  Severity: ERROR

  Message Text: DNS resoultion failed for syslog client, Will not parse messages from this client

  Message Description: DNS resoultion failed for syslog client, Will not parse messages from this client, Please check DNS can resolve ip to hostname

  Local Target Message Format: <timestamp> <seq_num> 90122 ERROR PassiveID: DNS resoultion failed for syslog client, Will not parse messages from this client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90122 ERROR PassiveID: DNS resoultion failed for syslog client, Will not parse messages from this client, <log details>

- **Message Code:** 90123

  Severity: DEBUG

  Message Text: Receive message from unkown client, Droping message

  Message Description: Receive message from unkown client, Droping message

  Local Target Message Format: <timestamp> <seq_num> 90123 DEBUG PassiveID: Receive message from unkown client, Droping message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90123 DEBUG PassiveID: Receive message from unkown client, Droping message, <log details>

- **Message Code:** 90124

  Severity: DEBUG

  Message Text: Receive unkown syslog format message

  Message Description: Receive unkown syslog format message

  Local Target Message Format: <timestamp> <seq_num> 90124 DEBUG PassiveID: Receive unkown syslog format message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90124 DEBUG PassiveID: Receive unkown syslog format message, <log details>

- **Message Code:** 90125

  Severity: WARN

  Message Text: Couldn't find session ID in ISE/ACS syslog message

  Message Description: Couldn't find session ID in ISE/ACS syslog message

Local Target Message Format: <timestamp> <seq_num> 90125 WARN PassiveID: Couldn't find session ID in ISE/ACS syslog message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90125 WARN PassiveID: Couldn't find session ID in ISE/ACS syslog message, <log details>

- **Message Code:** 90126

  Severity: WARN

  Message Text: Couldn't find IP address in ISE/ACS syslog message

  Message Description: Couldn't find address in ISE/ACS syslog message

  Local Target Message Format: <timestamp> <seq_num> 90126 WARN PassiveID: Couldn't find IP address in ISE/ACS syslog message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90126 WARN PassiveID: Couldn't find IP address in ISE/ACS syslog message, <log details>

- **Message Code:** 90127

  Severity: WARN

  Message Text: Receive ISE/ACS start/update radius message without pass authentication, Can't create PassiveID session

  Message Description: Receive ISE/ACS start/update radius message without pass authentication, Can't create PassiveID session

  Local Target Message Format: <timestamp> <seq_num> 90127 WARN PassiveID: Receive ISE/ACS start/update radius message without pass authentication, Can't create PassiveID session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90127 WARN PassiveID: Receive ISE/ACS start/update radius message without pass authentication, Can't create PassiveID session, <log details>

- **Message Code:** 90128

  Severity: ERROR

  Message Text: Failed to apply configuration

  Message Description: Failed to apply configuration

  Local Target Message Format: <timestamp> <seq_num> 90128 ERROR PassiveID: Failed to apply configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90128 ERROR PassiveID: Failed to apply configuration, <log details>

- **Message Code:** 90129

  Severity: ERROR

  Message Text: Error

Message Description: Failed to publish DHCP event to MNT

Local Target Message Format: <timestamp> <seq_num> 90129 ERROR PassiveID: Error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90129 ERROR PassiveID: Error, <log details>

- **Message Code:** 90130

  Severity: ERROR

  Message Text: Error

  Message Description: Failed to retrieve ad user's info from active directory

  Local Target Message Format: <timestamp> <seq_num> 90130 ERROR PassiveID: Error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90130 ERROR PassiveID: Error, <log details>

- **Message Code:** 90131

  Severity: ERROR

  Message Text: Error

  Message Description: Can not resolve syslog provider hostname to ip address

  Local Target Message Format: <timestamp> <seq_num> 90131 ERROR PassiveID: Error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90131 ERROR PassiveID: Error, <log details>

- **Message Code:** 90132

  Severity: DEBUG

  Message Text: Could not parse Syslog message

  Message Description: Could not parse Syslog message

  Local Target Message Format: <timestamp> <seq_num> 90132 DEBUG PassiveID: Could not parse Syslog message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90132 DEBUG PassiveID: Could not parse Syslog message, <log details>

- **Message Code:** 90133

  Severity: ERROR

  Message Text: Invalid Syslog message format

  Message Description: Invalid Syslog message format

  Local Target Message Format: <timestamp> <seq_num> 90133 ERROR PassiveID: Invalid Syslog message format, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90133 ERROR PassiveID: Invalid Syslog message format, <log details>

- **Message Code:** 90134

  Severity: ERROR

  Message Text: Could not parse Syslog hostname from message

  Message Description: Could not parse Syslog hostname from message

  Local Target Message Format: <timestamp> <seq_num> 90134 ERROR PassiveID: Could not parse Syslog hostname from message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90134 ERROR PassiveID: Could not parse Syslog hostname from message, <log details>

- **Message Code:** 90135

  Severity: DEBUG

  Message Text: Message received

  Message Description: Message received

  Local Target Message Format: <timestamp> <seq_num> 90135 DEBUG PassiveID: Message received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90135 DEBUG PassiveID: Message received, <log details>

- **Message Code:** 90136

  Severity: WARN

  Message Text: Syslog protocol server error

  Message Description: Received message in wrong format, dropped

  Local Target Message Format: <timestamp> <seq_num> 90136 WARN PassiveID: Syslog protocol server error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90136 WARN PassiveID: Syslog protocol server error, <log details>

- **Message Code:** 90137

  Severity: NOTICE

  Message Text: Syslog listener is up

  Message Description: Syslog listener is up

  Local Target Message Format: <timestamp> <seq_num> 90137 NOTICE PassiveID: Syslog listener is up, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90137 NOTICE PassiveID: Syslog listener is up, <log details>

- **Message Code:** 90138

  Severity: NOTICE

  Message Text: Syslog listener is down

  Message Description: Syslog listener is down

  Local Target Message Format: <timestamp> <seq_num> 90138 NOTICE PassiveID: Syslog listener is down, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90138 NOTICE PassiveID: Syslog listener is down, <log details>

- **Message Code:** 90139

  Severity: DEBUG

  Message Text: Identity Mapping message received, dropped

  Message Description: Identity Mapping message received, dropped

  Local Target Message Format: <timestamp> <seq_num> 90139 DEBUG PassiveID: Identity Mapping message received, dropped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90139 DEBUG PassiveID: Identity Mapping message received, dropped, <log details>

- **Message Code:** 90140

  Severity: INFO

  Message Text: Message parsed

  Message Description: Message parsed

  Local Target Message Format: <timestamp> <seq_num> 90140 INFO PassiveID: Message parsed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90140 INFO PassiveID: Message parsed, <log details>

- **Message Code:** 90141

  Severity: DEBUG

  Message Text: Incomplete message received, dropped

  Message Description: Incomplete message received, dropped

  Local Target Message Format: <timestamp> <seq_num> 90141 DEBUG PassiveID: Incomplete message received, dropped, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90141 DEBUG PassiveID: Incomplete message received, dropped, <log details>

- **Message Code:** 90142

  Severity: INFO

  Message Text: No Active Directory with credentials were found. Endpoint check will not run

  Message Description: No Active Directory with credentials were found. Endpoint probing will not run

  Local Target Message Format: <timestamp> <seq_num> 90142 INFO PassiveID: No Active Directory with credentials were found. Endpoint check will not run, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90142 INFO PassiveID: No Active Directory with credentials were found. Endpoint check will not run, <log details>

- **Message Code:** 90143

  Severity: INFO

  Message Text: This IP is not part of any configured subnet. Endpoint check will not run

  Message Description: This IP is not part of any configured subnet. Endpoint check will not run

  Local Target Message Format: <timestamp> <seq_num> 90143 INFO PassiveID: This IP is not part of any configured subnet. Endpoint check will not run, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90143 INFO PassiveID: This IP is not part of any configured subnet. Endpoint check will not run, <log details>

- **Message Code:** 90200

  Severity: INFO

  Message Text: REST server started succesfully.

  Message Description: Waiting for inconming requests

  Local Target Message Format: <timestamp> <seq_num> 90200 INFO PassiveID: REST server started succesfully., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90200 INFO PassiveID: REST server started succesfully., <log details>

- **Message Code:** 90201

  Severity: INFO

  Message Text: New authentication token was issued for client.

  Message Description: Token will be used on further requests.

  Local Target Message Format: <timestamp> <seq_num> 90201 INFO PassiveID: New authentication token was issued for client., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90201 INFO PassiveID: New authentication token was issued for client., <log details>

- **Message Code:** 90202

  Severity: ERROR

  Message Text: Authentication request failed

  Message Description: Check credentials used for initial basic authentication

  Local Target Message Format: <timestamp> <seq_num> 90202 ERROR PassiveID: Authentication request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90202 ERROR PassiveID: Authentication request failed, <log details>

- **Message Code:** 90203

  Severity: INFO

  Message Text: Token was revoked according to client request.

  Message Description: Further requests with a revoked token will be denied.

  Local Target Message Format: <timestamp> <seq_num> 90203 INFO PassiveID: Token was revoked according to client request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90203 INFO PassiveID: Token was revoked according to client request., <log details>

- **Message Code:** 90204

  Severity: ERROR

  Message Text: Failed to reverse resolve ip to hostname

  Message Description: Failed to reverse resolve ip to hostname, configure reverse DNS for the REST client host.

  Local Target Message Format: <timestamp> <seq_num> 90204 ERROR PassiveID: Failed to reverse resolve ip to hostname, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90204 ERROR PassiveID: Failed to reverse resolve ip to hostname, <log details>

- **Message Code:** 90205

  Severity: DEBUG

  Message Text: Request from unknown clinet was dropped.

  Message Description: Request from unknown clinet was dropped. Try to configure client in ISE.

  Local Target Message Format: <timestamp> <seq_num> 90205 DEBUG PassiveID: Request from unknown clinet was dropped., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90205 DEBUG PassiveID: Request from unknown clinet was dropped., <log details>

- **Message Code:** 90206

  Severity: ERROR

  Message Text: Request dropped due to invalid or missing token.

  Message Description: Request dropped due to invalid or missing token. Make sure the client is sending valid token.

  Local Target Message Format: <timestamp> <seq_num> 90206 ERROR PassiveID: Request dropped due to invalid or missing token., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90206 ERROR PassiveID: Request dropped due to invalid or missing token., <log details>

- **Message Code:** 90300

  Severity: ERROR

  Message Text: Probe didn't receive keep-alive signal from agent.

  Message Description: Make sure agent is up and running.

  Local Target Message Format: <timestamp> <seq_num> 90300 ERROR PassiveID: Probe didn't receive keep-alive signal from agent., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90300 ERROR PassiveID: Probe didn't receive keep-alive signal from agent., <log details>

- **Message Code:** 90301

  Severity: ERROR

  Message Text: Probe received incorrect number of client status.

  Message Description: Check debug logs for further infomation.

  Local Target Message Format: <timestamp> <seq_num> 90301 ERROR PassiveID: Probe received incorrect number of client status., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90301 ERROR PassiveID: Probe received incorrect number of client status., <log details>

- **Message Code:** 90500

  Severity: NOTICE

  Message Text: New Identity Mapping

  Message Description: PassiveID new mapping event received

  Local Target Message Format: <timestamp> <seq_num> 90500 NOTICE PassiveID: New Identity Mapping, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90500 NOTICE PassiveID: New Identity Mapping, <log details>

- **Message Code:** 90501

  Severity: NOTICE

  Message Text: Update Identity Mapping

  Message Description: PassiveID updated mapping event received

  Local Target Message Format: <timestamp> <seq_num> 90501 NOTICE PassiveID: Update Identity Mapping, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90501 NOTICE PassiveID: Update Identity Mapping, <log details>

- **Message Code:** 90502

  Severity: NOTICE

  Message Text: Remove Identity Mapping

  Message Description: PassiveID delete mapping event received

  Local Target Message Format: <timestamp> <seq_num> 90502 NOTICE PassiveID: Remove Identity Mapping, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 90502 NOTICE PassiveID: Remove Identity Mapping, <log details>

- **Message Code:** 90504

  Severity: ERROR

  Message Text: NO Identity Mapping

  Message Description: PassiveID no mapping event received

  Local Target Message Format: <timestamp> <seq_num>90504 ERROR PassiveID NO Identity Mapping, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>90504 ERROR PassiveID NO Identity Mapping, <log details>

- **Message Code:** 90505

  Severity: NOTICE

  Message Text: Latency detected in mappings

  Message Description: Latency detected in receiving mappings

  Local Target Message Format: <timestamp> <seq_num>90505 NOTICE PassiveID Latency detected in mappings, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>90505 NOTICE PassiveID Latency detected in mappings, <log details>

- **Message Code:** 90503

  Severity: ERROR

  Message Text: Request from registered client was dropped due to unsupported protocol.

  Message Description: Request from registered client was dropped due to unsupported protocol. Try to configure client in ISE with supported protocol.

  Local Target Message Format: <timestamp> <seq_num>90503 ERROR PassiveID Request from registered client was dropped due to unsupported protocol., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>90503 ERROR PassiveID Request from registered client was dropped due to unsupported protocol., <log details>

- **Message Code:** 90506

  Severity: NOTICE

  Message Text: Running Authorize Only Flow for Passive ID

  Message Description: Running Authorize Only Flow for Passive ID

  Local Target Message Format: <timestamp> <seq_num>90506 NOTICE PassiveID Running Authorize Only Flow for Passive ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>90506 NOTICE PassiveID Running Authorize Only Flow for Passive ID, <log details>

Policy Diagnostics

- **Message Code:** 15001

  Severity: ERROR

  Message Text: Adapter must contain at least one value

  Message Description: This is a database configuration problem

  Local Target Message Format: <timestamp> <seq_num> 15001 ERROR Policy: Adapter must contain at least one value, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15001 ERROR Policy: Adapter must contain at least one value, <log details>

- **Message Code:** 15002

  Severity: ERROR

  Message Text: Configured operator failed to match the value type

Message Description: This is a database configuration problem, the operator and value type mismatch

Local Target Message Format: <timestamp> <seq_num> 15002 ERROR Policy: Configured operator failed to match the value type, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15002 ERROR Policy: Configured operator failed to match the value type, <log details>

- **Message Code:** 15003

  Severity: ERROR

  Message Text: Incorrect database configuration

  Message Description: Incorrect database configuration

  Local Target Message Format: <timestamp> <seq_num> 15003 ERROR Policy: Incorrect database configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15003 ERROR Policy: Incorrect database configuration, <log details>

- **Message Code:** 15004

  Severity: DEBUG

  Message Text: Matched rule

  Message Description: Matched rule

  Local Target Message Format: <timestamp> <seq_num> 15004 DEBUG Policy: Matched rule, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15004 DEBUG Policy: Matched rule, <log details>

- **Message Code:** 15005

  Severity: DEBUG

  Message Text: Matched monitored rule

  Message Description: Matched monitored rule

  Local Target Message Format: <timestamp> <seq_num> 15005 DEBUG Policy: Matched monitored rule, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15005 DEBUG Policy: Matched monitored rule, <log details>

- **Message Code:** 15006

  Severity: DEBUG

  Message Text: Matched Default Rule

  Message Description: The policy default rule matched

Local Target Message Format: <timestamp> <seq_num> 15006 DEBUG Policy: Matched Default Rule, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15006 DEBUG Policy: Matched Default Rule, <log details>

- **Message Code:** 15007

  Severity: ERROR

  Message Text: Policy result type did not match expected result

  Message Description: Policy result type did not match expected result

  Local Target Message Format: <timestamp> <seq_num> 15007 ERROR Policy: Policy result type did not match expected result, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15007 ERROR Policy: Policy result type did not match expected result, <log details>

- **Message Code:** 15008

  Severity: DEBUG

  Message Text: Evaluating Service Selection Policy

  Message Description: Evaluating Service Selection Policy

  Local Target Message Format: <timestamp> <seq_num> 15008 DEBUG Policy: Evaluating Service Selection Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15008 DEBUG Policy: Evaluating Service Selection Policy, <log details>

- **Message Code:** 15009

  Severity: DEBUG

  Message Text: Exception Authorization Policy not configured

  Message Description: Exception Authorization Policy not configured

  Local Target Message Format: <timestamp> <seq_num> 15009 DEBUG Policy: Exception Authorization Policy not configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15009 DEBUG Policy: Exception Authorization Policy not configured, <log details>

- **Message Code:** 15010

  Severity: ERROR

  Message Text: Identity policy is not configured

  Message Description: Identity policy is not configured.

Local Target Message Format: <timestamp> <seq_num> 15010 ERROR Policy: Identity policy is not configured, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15010 ERROR Policy: Identity policy is not configured, <log details>

- **Message Code:** 15011

  Severity: INFO

  Message Text: Authorization Policy not configured

  Message Description: Authorization Policy not configured

  Local Target Message Format: <timestamp> <seq_num> 15011 INFO Policy: Authorization Policy not configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15011 INFO Policy: Authorization Policy not configured, <log details>

- **Message Code:** 15012

  Severity: DEBUG

  Message Text: Selected Access Service

  Message Description: Selected Access Service

  Local Target Message Format: <timestamp> <seq_num> 15012 DEBUG Policy: Selected Access Service, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15012 DEBUG Policy: Selected Access Service, <log details>

- **Message Code:** 15013

  Severity: DEBUG

  Message Text: Selected Identity Source

  Message Description: Selected Identity Source

  Local Target Message Format: <timestamp> <seq_num> 15013 DEBUG Policy: Selected Identity Source, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15013 DEBUG Policy: Selected Identity Source, <log details>

- **Message Code:** 15015

  Severity: ERROR

  Message Text: Could not find ID Store

  Message Description: Could not find ID Store in the database

Local Target Message Format: <timestamp> <seq_num> 15015 ERROR Policy: Could not find ID Store, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15015 ERROR Policy: Could not find ID Store, <log details>

- **Message Code:** 15016

  Severity: DEBUG

  Message Text: Selected Authorization Profile

  Message Description: Selected Authorization Profile

  Local Target Message Format: <timestamp> <seq_num> 15016 DEBUG Policy: Selected Authorization Profile, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15016 DEBUG Policy: Selected Authorization Profile, <log details>

- **Message Code:** 15017

  Severity: DEBUG

  Message Text: Selected Shell Profile

  Message Description: Selected Shell Profile

  Local Target Message Format: <timestamp> <seq_num> 15017 DEBUG Policy: Selected Shell Profile, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15017 DEBUG Policy: Selected Shell Profile, <log details>

- **Message Code:** 15018

  Severity: DEBUG

  Message Text: Selected Command Set

  Message Description: Selected Command Set

  Local Target Message Format: <timestamp> <seq_num> 15018 DEBUG Policy: Selected Command Set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15018 DEBUG Policy: Selected Command Set, <log details>

- **Message Code:** 15019

  Severity: DEBUG

  Message Text: Could not find selected Authorization Profiles

  Message Description: Could not find selected Authorization Profiles

Local Target Message Format: <timestamp> <seq_num> 15019 DEBUG Policy: Could not find selected Authorization Profiles, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15019 DEBUG Policy: Could not find selected Authorization Profiles, <log details>

- **Message Code:** 15020

  Severity: WARN

  Message Text: Could not find selected Shell Profiles

  Message Description: Could not find selected Shell Profiles

  Local Target Message Format: <timestamp> <seq_num> 15020 WARN Policy: Could not find selected Shell Profiles, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15020 WARN Policy: Could not find selected Shell Profiles, <log details>

- **Message Code:** 15021

  Severity: ERROR

  Message Text: Could not find selected Command Set

  Message Description: Could not find selected Command Set

  Local Target Message Format: <timestamp> <seq_num> 15021 ERROR Policy: Could not find selected Command Set, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15021 ERROR Policy: Could not find selected Command Set, <log details>

- **Message Code:** 15022

  Severity: ERROR

  Message Text: Could not find selected Access Service

  Message Description: Could not find selected Access Service

  Local Target Message Format: <timestamp> <seq_num> 15022 ERROR Policy: Could not find selected Access Service, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15022 ERROR Policy: Could not find selected Access Service, <log details>

- **Message Code:** 15023

  Severity: DEBUG

  Message Text: Could not match rule

  Message Description: Could not match rule

Local Target Message Format: <timestamp> <seq_num> 15023 DEBUG Policy: Could not match rule, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15023 DEBUG Policy: Could not match rule, <log details>

- **Message Code:** 15024

  Severity: INFO

  Message Text: PAP is not allowed

  Message Description: PAP is not allowed

  Local Target Message Format: <timestamp> <seq_num> 15024 INFO Policy: PAP is not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15024 INFO Policy: PAP is not allowed, <log details>

- **Message Code:** 15025

  Severity: DEBUG

  Message Text: External Policy Check Policy not configured

  Message Description: External Policy Check Policy not configured

  Local Target Message Format: <timestamp> <seq_num> 15025 DEBUG Posture: External Policy Check Policy not configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15025 DEBUG Posture: External Policy Check Policy not configured, <log details>

- **Message Code:** 15026

  Severity: DEBUG

  Message Text: External Policy Server not found

  Message Description: External Policy Server not found

  Local Target Message Format: <timestamp> <seq_num> 15026 DEBUG Posture: External Policy Server not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15026 DEBUG Posture: External Policy Server not found, <log details>

- **Message Code:** 15027

  Severity: DEBUG

  Message Text: External Policy Server selected

  Message Description: External Policy Server selected

Local Target Message Format: <timestamp> <seq_num> 15027 DEBUG Posture: External Policy Server selected, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15027 DEBUG Posture: External Policy Server selected, <log details>

- **Message Code:** 15028

  Severity: DEBUG

  Message Text: Sending request to External Policy Server

  Message Description: Sending request to External Policy Server

  Local Target Message Format: <timestamp> <seq_num> 15028 DEBUG Posture: Sending request to External Policy Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15028 DEBUG Posture: Sending request to External Policy Server, <log details>

- **Message Code:** 15029

  Severity: DEBUG

  Message Text: Could not retrieve attributes from External Policy Server

  Message Description: Could not retrieve attributes from External Policy Server

  Local Target Message Format: <timestamp> <seq_num> 15029 DEBUG Posture: Could not retrieve attributes from External Policy Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15029 DEBUG Posture: Could not retrieve attributes from External Policy Server, <log details>

- **Message Code:** 15030

  Severity: DEBUG

  Message Text: Apparent misconfiguration of External Policy Server

  Message Description: Apparent misconfiguration of External Policy Server

  Local Target Message Format: <timestamp> <seq_num> 15030 DEBUG Posture: Apparent misconfiguration of External Policy Server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15030 DEBUG Posture: Apparent misconfiguration of External Policy Server, <log details>

- **Message Code:** 15031

  Severity: DEBUG

  Message Text: External Policy attributes retrieved

  Message Description: External Policy attributes retrieved

Local Target Message Format: <timestamp> <seq_num> 15031 DEBUG Posture: External Policy attributes retrieved, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15031 DEBUG Posture: External Policy attributes retrieved, <log details>

- **Message Code:** 15032

  Severity: DEBUG

  Message Text: Evaluating External Policy Check Policy

  Message Description: Evaluating External Policy Check Policy

  Local Target Message Format: <timestamp> <seq_num> 15032 DEBUG Policy: Evaluating External Policy Check Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15032 DEBUG Policy: Evaluating External Policy Check Policy, <log details>

- **Message Code:** 15033

  Severity: INFO

  Message Text: Group Mapping Policy not configured

  Message Description: Group Mapping Policy not configured

  Local Target Message Format: <timestamp> <seq_num> 15033 INFO Policy: Group Mapping Policy not configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15033 INFO Policy: Group Mapping Policy not configured, <log details>

- **Message Code:** 15034

  Severity: DEBUG

  Message Text: Skip External Policy Check

  Message Description: Skip External Policy Check

  Local Target Message Format: <timestamp> <seq_num> 15034 DEBUG Posture: Skip External Policy Check, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15034 DEBUG Posture: Skip External Policy Check, <log details>

- **Message Code:** 15035

  Severity: DEBUG

  Message Text: Evaluating Exception Authorization Policy

  Message Description: Evaluating Exception Authorization Policy

Local Target Message Format: <timestamp> <seq_num> 15035 DEBUG Policy: Evaluating Exception Authorization Policy, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15035 DEBUG Policy: Evaluating Exception Authorization Policy, <log details>

- **Message Code:** 15036

  Severity: DEBUG

  Message Text: Evaluating Authorization Policy

  Message Description: Evaluating Authorization Policy

  Local Target Message Format: <timestamp> <seq_num> 15036 DEBUG Policy: Evaluating Authorization Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15036 DEBUG Policy: Evaluating Authorization Policy, <log details>

- **Message Code:** 15037

  Severity: DEBUG

  Message Text: Using previously selected Access Service

  Message Description: Using previously selected Access Service

  Local Target Message Format: <timestamp> <seq_num> 15037 DEBUG Policy: Using previously selected Access Service, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15037 DEBUG Policy: Using previously selected Access Service, <log details>

- **Message Code:** 15038

  Severity: DEBUG

  Message Text: Skipping External Policy because of missing or malformed required attributes

  Message Description: Skipping External Policy because of missing or malformed required attributes

  Local Target Message Format: <timestamp> <seq_num> 15038 DEBUG Posture: Skipping External Policy because of missing or malformed required attributes, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15038 DEBUG Posture: Skipping External Policy because of missing or malformed required attributes, <log details>

- **Message Code:** 15039

  Severity: INFO

  Message Text: Rejected per authorization profile

  Message Description: Selected Authorization Profile contains ACCESS_REJECT attribute

Local Target Message Format: <timestamp> <seq_num> 15039 INFO RADIUS: Rejected per authorization profile, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15039 INFO RADIUS: Rejected per authorization profile, <log details>

- **Message Code:** 15040

  Severity: INFO

  Message Text: User name attribute not defined in certificate profile

  Message Description: User name attribute not defined in certificate profile

  Local Target Message Format: <timestamp> <seq_num> 15040 INFO Policy: User name attribute not defined in certificate profile, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15040 INFO Policy: User name attribute not defined in certificate profile, <log details>

- **Message Code:** 15041

  Severity: DEBUG

  Message Text: Evaluating Identity Policy

  Message Description: Evaluating Identity Policy

  Local Target Message Format: <timestamp> <seq_num> 15041 DEBUG Policy: Evaluating Identity Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15041 DEBUG Policy: Evaluating Identity Policy, <log details>

- **Message Code:** 15042

  Severity: INFO

  Message Text: No rule was matched

  Message Description: The evaluated policy did not match any rule

  Local Target Message Format: <timestamp> <seq_num> 15042 INFO Policy: No rule was matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15042 INFO Policy: No rule was matched, <log details>

- **Message Code:** 15043

  Severity: INFO

  Message Text: Dynamic attribute value is unavailable

  Message Description: Dynamic attribute value is unavailable, Referenced attribute that contains the value does not exist

Local Target Message Format: <timestamp> <seq_num> 15043 INFO Policy: Dynamic attribute value is unavailable, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15043 INFO Policy: Dynamic attribute value is unavailable, <log details>

- **Message Code:** 15044

  Severity: DEBUG

  Message Text: Evaluating Group Mapping Policy

  Message Description: Evaluating Group Mapping Policy

  Local Target Message Format: <timestamp> <seq_num> 15044 DEBUG Policy: Evaluating Group Mapping Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15044 DEBUG Policy: Evaluating Group Mapping Policy, <log details>

- **Message Code:** 15045

  Severity: ERROR

  Message Text: CHAP is not allowed

  Message Description: CHAP is not allowed.

  Local Target Message Format: <timestamp> <seq_num> 15045 ERROR Policy: CHAP is not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15045 ERROR Policy: CHAP is not allowed, <log details>

- **Message Code:** 15046

  Severity: ERROR

  Message Text: MS-CHAP v1 is disabled under allowed protocols.

  Message Description: MS-CHAP v1 is disabled under allowed protocols.

  Local Target Message Format: <timestamp> <seq_num> 15046 ERROR Policy: MS-CHAP v1 is disabled under allowed protocols., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15046 ERROR Policy: MS-CHAP v1 is disabled under allowed protocols., <log details>

- **Message Code:** 15047

  Severity: ERROR

  Message Text: MS-CHAP v2 is disabled under allowed protocols.

  Message Description: MS-CHAP v2 is disabled under allowed protocols.

Local Target Message Format: <timestamp> <seq_num> 15047 ERROR Policy: MS-CHAP v2 is disabled under allowed protocols., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15047 ERROR Policy: MS-CHAP v2 is disabled under allowed protocols., <log details>

- **Message Code:** 15048

  Severity: DEBUG

  Message Text: Queried PIP

  Message Description: The Policy Engine queried a PIP for attributes that were referenced by the policy

  Local Target Message Format: <timestamp> <seq_num> 15048 DEBUG Policy: Queried PIP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15048 DEBUG Policy: Queried PIP, <log details>

- **Message Code:** 15049

  Severity: DEBUG

  Message Text: Evaluating Policy Group

  Message Description: Evaluating Policy Group

  Local Target Message Format: <timestamp> <seq_num> 15049 DEBUG Policy: Evaluating Policy Group, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15049 DEBUG Policy: Evaluating Policy Group, <log details>

- **Message Code:** 15050

  Severity: DEBUG

  Message Text: Network Access Device does not support configuration of VLAN

  Message Description: Network Access Device does not support configuration of VLAN

  Local Target Message Format: <timestamp> <seq_num> 15050 DEBUG Policy: Network Access Device does not support configuration of VLAN, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15050 DEBUG Policy: Network Access Device does not support configuration of VLAN, <log details>

- **Message Code:** 15051

  Severity: DEBUG

  Message Text: Network Access Device does not support configuration of ACL

  Message Description: Network Access Device does not support configuration of ACL

Local Target Message Format: <timestamp> <seq_num> 15051 DEBUG Policy: Network Access Device does not support configuration of ACL, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15051 DEBUG Policy: Network Access Device does not support configuration of ACL, <log details>

- **Message Code:** 15052

  Severity: DEBUG

  Message Text: Authorization profile/s specified are not suited for this Network Access Device

  Message Description: Authorization profile/s specified are not suited for this Network Access Device

  Local Target Message Format: <timestamp> <seq_num> 15052 DEBUG Policy: Authorization profile/s specified are not suited for this Network Access Device, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15052 DEBUG Policy: Authorization profile/s specified are not suited for this Network Access Device, <log details>

- **Message Code:** 15053

  Severity: DEBUG

  Message Text: Network Access Device does not support CoA

  Message Description: Network Access Device does not support CoA

  Local Target Message Format: <timestamp> <seq_num> 15053 DEBUG Policy: Network Access Device does not support CoA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15053 DEBUG Policy: Network Access Device does not support CoA, <log details>

- **Message Code:** 15054

  Severity: DEBUG

  Message Text: Sending SNMP set :

  Message Description: Sending SNMP set :

  Local Target Message Format: <timestamp> <seq_num> 15054 DEBUG Policy: Sending SNMP set :, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15054 DEBUG Policy: Sending SNMP set :, <log details>

- **Message Code:** 15055

  Severity: DEBUG

  Message Text: SNMP CoA failed

  Message Description: SNMP CoA failed

Local Target Message Format: <timestamp> <seq_num> 15055 DEBUG Policy: SNMP CoA failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15055 DEBUG Policy: SNMP CoA failed, <log details>

- **Message Code:** 15056

  Severity: ERROR

  Message Text: IP Address for interface selected in portal settings is undefined

  Message Description: IP Address for interface selected in portal settings is undefined. Please use CLI to configure IP address for selected interface

  Local Target Message Format: <timestamp> <seq_num> 15056 ERROR Policy: IP Address for interface selected in portal settings is undefined, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 15056 ERROR Policy: IP Address for interface selected in portal settings is undefined, <log details>

- **Message Code:** 15057

  Severity: INFO

  Message Text: Evaluating Multi-Factor Authentication Policy

  Message Description: Evaluating Multi-Factor Authentication Policy

  Local Target Message Format: <timestamp> <seq_num>Policy Evaluating Multi-Factor Authentication Policy INFO Evaluating Multi-Factor Authentication Policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Policy Evaluating Multi-Factor Authentication Policy INFO Evaluating Multi-Factor Authentication Policy, <log details>

- **Message Code:** 15503

  Severity: ERROR

  Message Text: Policy Engine request queue is full

  Message Description: Policy Engine request queue is full.

  Local Target Message Format: <timestamp> <seq_num>Policy Policy Engine request queue is full ERROR Policy Engine request queue is full., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Policy Policy Engine request queue is full ERROR Policy Engine request queue is full., <log details>

- **Message Code:** 15504

  Severity: ERROR

  Message Text: No Policy Engine request consumer threads are running

  Message Description: No Policy Engine request consumer threads are running.

Local Target Message Format: <timestamp> <seq_num>Policy No Policy Engine request consumer threads are running ERROR No Policy Engine request consumer threads are running., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Policy No Policy Engine request consumer threads are running ERROR No Policy Engine request consumer threads are running., <log details>

- **Message Code:** 15505

  Severity: ERROR

  Message Text: Internal Policy Engine error

  Message Description: Some unexpected exception has occurred while adding request to Policy Engine request queue.

  Local Target Message Format: <timestamp> <seq_num>Policy Internal Policy Engine error ERROR Some unexpected exception has occurred while adding request to Policy Engine request queue., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Policy Internal Policy Engine error ERROR Some unexpected exception has occurred while adding request to Policy Engine request queue., <log details>

- **Message Code:** 15506

  Severity: ERROR

  Message Text: Response queue provided for policy-engine is full

  Message Description: Response queue provided for policy-engine is full.

  Local Target Message Format: <timestamp> <seq_num>Policy Response queue provided for policy-engine is full ERROR Response queue provided for policy-engine is full., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Policy Response queue provided for policy-engine is full ERROR Response queue provided for policy-engine is full., <log details>

- **Message Code:** 15509

  Severity: INFO

  Message Text: Skipping Service Selection for accounting

  Message Description: Skipping Service Selection for accounting

  Local Target Message Format: <timestamp> <seq_num>Policy Skipping Service Selection for accounting INFO Skipping Service Selection for accounting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Policy Skipping Service Selection for accounting INFO Skipping Service Selection for accounting, <log details>

- **Message Code:** 15508

  Severity: WARN

  Message Text: Setting default value of 1800 seconds for session timeout

Message Description: Setting default value of 1800 seconds for session timeout.

Local Target Message Format: <timestamp> <seq_num>15508 WARN Policy Setting default value of 1800 seconds for session timeout, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>15508 WARN Policy Setting default value of 1800 seconds for session timeout, <log details>

- **Message Code:** 15507

  Severity: ERROR

  Message Text: Dynamic attribute value for Session Timeout is in wrong format

  Message Description: Dynamic attribute value for Session Timeout is in wrong format.

  Local Target Message Format: <timestamp> <seq_num>15507 ERROR Policy Dynamic attribute value for Session Timeout is in wrong format, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>15507 ERROR Policy Dynamic attribute value for Session Timeout is in wrong format, <log details>

Posture And Client Provisioning Audit

- **Message Code:** 87000

  Severity: NOTICE

  Message Text: Received a posture report from an endpoint

  Message Description: Received a posture report from an endpoint

  Local Target Message Format: <timestamp> <seq_num> 87000 NOTICE Posture: Received a posture report from an endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87000 NOTICE Posture: Received a posture report from an endpoint, <log details>

- **Message Code:** 87001

  Severity: NOTICE

  Message Text: Posture service received a reassessment report from an endpoint

  Message Description: Received a PRA report request from an endpoint

  Local Target Message Format: <timestamp> <seq_num> 87001 NOTICE Posture: Posture service received a reassessment report from an endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87001 NOTICE Posture: Posture service received a reassessment report from an endpoint, <log details>

- **Message Code:** 87002

Severity: NOTICE

Message Text: Terminating endpoint session: reassessment timeout

Message Description: A change of authorization request is sent to the device for terminating the current endpoint session per reassessment timeout

Local Target Message Format: <timestamp> <seq_num> 87002 NOTICE Posture: Terminating endpoint session: reassessment timeout, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87002 NOTICE Posture: Terminating endpoint session: reassessment timeout, <log details>

- **Message Code:** 87004

  Severity: NOTICE

  Message Text: Posture service received a USB-check report from an endpoint

  Message Description: Received a USB-check report message from an endpoint

  Local Target Message Format: <timestamp> <seq_num> 87004 NOTICE Posture: Posture service received a USB-check report from an endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87004 NOTICE Posture: Posture service received a USB-check report from an endpoint, <log details>

- **Message Code:** 87500

  Severity: NOTICE

  Message Text: Client provisioning succeeded

  Message Description: Client provisioning succeeded

  Local Target Message Format: <timestamp> <seq_num> 87500 NOTICE Client Provisioning: Client provisioning succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87500 NOTICE Client Provisioning: Client provisioning succeeded, <log details>

- **Message Code:** 87501

  Severity: NOTICE

  Message Text: Client provisioning failed

  Message Description: Client provisioning failed

  Local Target Message Format: <timestamp> <seq_num> 87501 NOTICE Client Provisioning: Client provisioning failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87501 NOTICE Client Provisioning: Client provisioning failed, <log details>

- **Message Code:** 87600

Severity: NOTICE

Message Text: Supplicant provisioning succeeded

Message Description: Supplicant provisioning for client succeeded

Local Target Message Format: <timestamp> <seq_num> 87600 NOTICE Supplicant Provisioning: Supplicant provisioning succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87600 NOTICE Supplicant Provisioning: Supplicant provisioning succeeded, <log details>

- **Message Code:** 87601

  Severity: NOTICE

  Message Text: Supplicant provisioning failed

  Message Description: Supplicant provisioning failed

  Local Target Message Format: <timestamp> <seq_num> 87601 NOTICE Supplicant Provisioning: Supplicant provisioning failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87601 NOTICE Supplicant Provisioning: Supplicant provisioning failed, <log details>

- **Message Code:** 87602

  Severity: NOTICE

  Message Text: Supplicant provisioning is in progress

  Message Description: Supplicant provisioning is in progress

  Local Target Message Format: <timestamp> <seq_num> 87602 NOTICE Supplicant Provisioning: Supplicant provisioning is in progress, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87602 NOTICE Supplicant Provisioning: Supplicant provisioning is in progress, <log details>

- **Message Code:** 87603

  Severity: NOTICE

  Message Text: Supplicant provisioning disabled

  Message Description: Supplicant provisioning for client is disabled

  Local Target Message Format: <timestamp> <seq_num> 87603 NOTICE Supplicant Provisioning: Supplicant provisioning disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87603 NOTICE Supplicant Provisioning: Supplicant provisioning disabled, <log details>

- **Message Code:** 87604

  Severity: WARN

Message Text: CA Server is down

Message Description: CA Server is down

Local Target Message Format: <timestamp> <seq_num> 87604 WARN Supplicant Provisioning: CA Server is down, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87604 WARN Supplicant Provisioning: CA Server is down, <log details>

- **Message Code:** 87605

  Severity: INFO

  Message Text: CA Server is up

  Message Description: CA Server is up

  Local Target Message Format: <timestamp> <seq_num> 87605 INFO Supplicant Provisioning: CA Server is up, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87605 INFO Supplicant Provisioning: CA Server is up, <log details>

- **Message Code:** 87606

  Severity: ERROR

  Message Text: Certificate request forwarding failed

  Message Description: Certificate request forwarding failed

  Local Target Message Format: <timestamp> <seq_num> 87606 ERROR Supplicant Provisioning: Certificate request forwarding failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87606 ERROR Supplicant Provisioning: Certificate request forwarding failed, <log details>

- **Message Code:** 87607

  Severity: WARN

  Message Text: High volume of OCSP transactions

  Message Description: High volume of OCSP transactions

  Local Target Message Format: <timestamp> <seq_num> 87607 WARN Supplicant Provisioning: High volume of OCSP transactions, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87607 WARN Supplicant Provisioning: High volume of OCSP transactions, <log details>

- **Message Code:** 87608

  Severity: WARN

  Message Text: EST Service is down

Message Description: EST Service is down

Local Target Message Format: <timestamp> <seq_num> 87608 WARN Supplicant Provisioning: EST Service is down, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87608 WARN Supplicant Provisioning: EST Service is down, <log details>

- **Message Code:** 87609

  Severity: INFO

  Message Text: EST Service is up

  Message Description: EST Service is up

  Local Target Message Format: <timestamp> <seq_num> 87609 INFO Supplicant Provisioning: EST Service is up, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87609 INFO Supplicant Provisioning: EST Service is up, <log details>

- **Message Code:** 87750

  Severity: NOTICE

  Message Text: Endpoint Protection Service has received a request to perform an operation

  Message Description: Endpoint Protection Service performs the requested operation on an endpoint

  Local Target Message Format: <timestamp> <seq_num> 87750 NOTICE EPS: Endpoint Protection Service has received a request to perform an operation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87750 NOTICE EPS: Endpoint Protection Service has received a request to perform an operation, <log details>

- **Message Code:** 87751

  Severity: NOTICE

  Message Text: Endpoint Protection Service has obtained the result of an operation

  Message Description: Endpoint Protection Service stores the result of an operation in the Operation Status

  Local Target Message Format: <timestamp> <seq_num> 87751 NOTICE EPS: Endpoint Protection Service has obtained the result of an operation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87751 NOTICE EPS: Endpoint Protection Service has obtained the result of an operation, <log details>

- **Message Code:** 87752

  Severity: NOTICE

  Message Text: Manual Certificate Provisioning Portal - Request submitted

Message Description: A certificate request is initiated from the Manual Certificate Provisioning Portal

Local Target Message Format: <timestamp> <seq_num> 87752 NOTICE Internal CA: Manual Certificate Provisioning Portal - Request submitted, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87752 NOTICE Internal CA: Manual Certificate Provisioning Portal - Request submitted, <log details>

- **Message Code:** 87753

  Severity: NOTICE

  Message Text: Manual Certificate Provisioning Portal - Status Update

  Message Description: Status update to a certificate request

  Local Target Message Format: <timestamp> <seq_num> 87753 NOTICE Internal CA: Manual Certificate Provisioning Portal - Status Update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87753 NOTICE Internal CA: Manual Certificate Provisioning Portal - Status Update, <log details>

- **Message Code:** 87754

  Severity: NOTICE

  Message Text: Manual Certificate Provisioning Portal - User login occurred

  Message Description: The new sessions is created for a user logging into the Manual Certificate Provisioning Portal

  Local Target Message Format: <timestamp> <seq_num> 87754 NOTICE Internal CA: Manual Certificate Provisioning Portal - User login occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 87754 NOTICE Internal CA: Manual Certificate Provisioning Portal - User login occurred, <log details>

- **Message Code:** 87901

  Severity: NOTICE

  Message Text: EndPoint Scripts Provisioned a new job for script execution

  Message Description: A new job has been successfully created to execute admin scripts on the selected end-points

  Local Target Message Format: <timestamp> <seq_num>87901 NOTICE EndPoint Scripts Provisioning EndPoint Scripts Provisioned a new job for script execution, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>87901 NOTICE EndPoint Scripts Provisioning EndPoint Scripts Provisioned a new job for script execution, <log details>

- **Message Code:** 87921

  Severity: NOTICE

  Message Text: Result of EndPoint Scripts execution from an endpoint obtained

Message Description: Endpoint scripts execution report of an endpoint from the given list is received

Local Target Message Format: <timestamp> <seq_num>87921 NOTICE EndPoint Scripts Provisioning Result of EndPoint Scripts execution from an endpoint obtained, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>87921 NOTICE EndPoint Scripts Provisioning Result of EndPoint Scripts execution from an endpoint obtained, <log details>

- **Message Code:** 87005

  Severity: NOTICE

  Message Text: Anyconnect probes to PSN during posture compliant state

  Message Description: Anyconnect probes to PSN during posture compliant state

  Local Target Message Format: <timestamp> <seq_num>87005 NOTICE Posture Anyconnect probes to PSN during posture compliant state, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>87005 NOTICE Posture Anyconnect probes to PSN during posture compliant state, <log details>

- **Message Code:** 87006

  Severity: NOTICE

  Message Text: Posture Queries per hour for MNT session lookup is high

  Message Description: Posture Queries per hour for MNT session lookup is high

  Local Target Message Format: <timestamp> <seq_num>87006 NOTICE Posture Posture Queries per hour for MNT session lookup is high, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>87006 NOTICE Posture Posture Queries per hour for MNT session lookup is high, <log details>

- **Message Code:** 87007

  Severity: WARN

  Message Text: Request rate limit exceeded

  Message Description: The system has detected an unusually high number of requests in a short period. Please reduce the request rate or try again later.

  Local Target Message Format: <timestamp> <seq_num>87007 WARN Posture Request rate limit exceeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>87007 WARN Posture Request rate limit exceeded, <log details>

- **Message Code:** 87008

  Severity: WARN

  Message Text: Thread limit exceeded

Message Description: The system has detected that the maximum allowed number of concurrent threads has been reached. This may occur due to excessive parallel processing or simultaneous sessions.

Local Target Message Format: <timestamp> <seq_num>87008 WARN Posture Thread limit exceeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>87008 WARN Posture Thread limit exceeded, <log details>

Posture And Client Provisioning Diagnostics

- **Message Code:** 83001

  Severity: DEBUG

  Message Text: Posture request from endpoint matched the policy

  Message Description: Posture request from endpoint matched the policy

  Local Target Message Format: <timestamp> <seq_num> 83001 DEBUG Posture: Posture request from endpoint matched the policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 83001 DEBUG Posture: Posture request from endpoint matched the policy, <log details>

- **Message Code:** 83003

  Severity: DEBUG

  Message Text: Received a reassessment request from an endpoint

  Message Description: A reassessment request is received from an endpoint

  Local Target Message Format: <timestamp> <seq_num> 83003 DEBUG Posture: Received a reassessment request from an endpoint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 83003 DEBUG Posture: Received a reassessment request from an endpoint, <log details>

- **Message Code:** 83007

  Severity: WARN

  Message Text: Terminating the non-compliant endpoint session

  Message Description: A change of authorization request is sent to the device for terminating the current non-compliant endpoint session

  Local Target Message Format: <timestamp> <seq_num> 83007 WARN Posture: Terminating the non-compliant endpoint session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 83007 WARN Posture: Terminating the non-compliant endpoint session, <log details>

- **Message Code:** 83009

  Severity: INFO

  Message Text: NAC agent on client is terminated

  Message Description: NAC agent on client is closed by the end user

  Local Target Message Format: <timestamp> <seq_num> 83009 INFO Posture: NAC agent on client is terminated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 83009 INFO Posture: NAC agent on client is terminated, <log details>

- **Message Code:** 83015

  Severity: INFO

  Message Text: Posture service is triggering a Change Of Authorization request

  Message Description: Posture service is triggering a new Change Of Authorization request due to changes in the session posture status

  Local Target Message Format: <timestamp> <seq_num> 83015 INFO Posture: Posture service is triggering a Change Of Authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 83015 INFO Posture: Posture service is triggering a Change Of Authorization request, <log details>

- **Message Code:** 84002

  Severity: WARN

  Message Text: Provisioning is disabled. You are not allowed to perform any provisioning related operations at this time

  Message Description: Provisioning is disabled. You are not allowed to perform any provisioning related operations at this time

  Local Target Message Format: <timestamp> <seq_num> 84002 WARN Client Provisioning: Provisioning is disabled. You are not allowed to perform any provisioning related operations at this time, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 84002 WARN Client Provisioning: Provisioning is disabled. You are not allowed to perform any provisioning related operations at this time, <log details>

- **Message Code:** 84003

  Severity: WARN

  Message Text: Posture component not provisioned due to version incompatibility with agent version

  Message Description: Posture component on server is not compatible with agent version, hence it is not provisioned

  Local Target Message Format: <timestamp> <seq_num> 84003 WARN Client Provisioning: Posture component not provisioned due to version incompatibility with agent version, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 84003 WARN Client Provisioning: Posture component not provisioned due to version incompatibility with agent version, <log details>

- **Message Code:** 85000

  Severity: INFO

  Message Text: Endpoint Protection Service is triggering a Change Of Authorization request

  Message Description: Endpoint Protection Service is triggering a new Change Of Authorization request

  Local Target Message Format: <timestamp> <seq_num> 85000 INFO EPS: Endpoint Protection Service is triggering a Change Of Authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 85000 INFO EPS: Endpoint Protection Service is triggering a Change Of Authorization request, <log details>

Profiler

- **Message Code:** 80001

  Severity: INFO

  Message Text: Profiler EndPoint collection event occurred

  Message Description: This message is generated when a profiler end point is collected

  Local Target Message Format: <timestamp> <seq_num> 80001 INFO Profiler: Profiler EndPoint collection event occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80001 INFO Profiler: Profiler EndPoint collection event occurred, <log details>

- **Message Code:** 80002

  Severity: INFO

  Message Text: Profiler EndPoint profiling event occurred

  Message Description: This message is generated when a profiler end point is profiled

  Local Target Message Format: <timestamp> <seq_num> 80002 INFO Profiler: Profiler EndPoint profiling event occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80002 INFO Profiler: Profiler EndPoint profiling event occurred, <log details>

- **Message Code:** 80003

  Severity: ERROR

  Message Text: Profiler Probe failed to load

  Message Description: This message is generated when a probe fails to start

Local Target Message Format: <timestamp> <seq_num> 80003 ERROR Profiler: Profiler Probe failed to load, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80003 ERROR Profiler: Profiler Probe failed to load, <log details>

- **Message Code:** 80004

  Severity: INFO

  Message Text: Profiler Performance Counters Snapshot update event occurred

  Message Description: This message is generated when a new Profiler performance-counters snapshot is reported

  Local Target Message Format: <timestamp> <seq_num> 80004 INFO Profiler: Profiler Performance Counters Snapshot update event occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80004 INFO Profiler: Profiler Performance Counters Snapshot update event occurred, <log details>

- **Message Code:** 80005

  Severity: INFO

  Message Text: Profiler Exception Action execution occurred

  Message Description: This message is generated when a profiler end point is profiled and matched an exception rule

  Local Target Message Format: <timestamp> <seq_num> 80005 INFO Profiler: Profiler Exception Action execution occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80005 INFO Profiler: Profiler Exception Action execution occurred, <log details>

- **Message Code:** 80006

  Severity: INFO

  Message Text: Profiler is triggering Change Of Authorization Request

  Message Description: Profiler is triggering Change Of Authorization Request

  Local Target Message Format: <timestamp> <seq_num> 80006 INFO Profiler: Profiler is triggering Change Of Authorization Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80006 INFO Profiler: Profiler is triggering Change Of Authorization Request, <log details>

- **Message Code:** 80007

  Severity: DEBUG

  Message Text: Profiler SNMP request sent

  Message Description: This message is generated when profiler sends the SNMP request.

Local Target Message Format: <timestamp> <seq_num> 80007 DEBUG Profiler: Profiler SNMP request sent, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80007 DEBUG Profiler: Profiler SNMP request sent, <log details>

- **Message Code:** 80008

  Severity: DEBUG

  Message Text: Profiler SNMP response received

  Message Description: This message is generated when profiler receives the SNMP response.

  Local Target Message Format: <timestamp> <seq_num> 80008 DEBUG Profiler: Profiler SNMP response received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80008 DEBUG Profiler: Profiler SNMP response received, <log details>

- **Message Code:** 80009

  Severity: ERROR

  Message Text: Profiler SNMP request failure

  Message Description: This message is generated when profiler SNMP request fails.

  Local Target Message Format: <timestamp> <seq_num> 80009 ERROR Profiler: Profiler SNMP request failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80009 ERROR Profiler: Profiler SNMP request failure, <log details>

- **Message Code:** 80010

  Severity: INFO

  Message Text: Profiler DNS request sent

  Message Description: This message is generated when profiler sends the DNS request.

  Local Target Message Format: <timestamp> <seq_num> 80010 INFO Profiler: Profiler DNS request sent, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80010 INFO Profiler: Profiler DNS request sent, <log details>

- **Message Code:** 80013

  Severity: INFO

  Message Text: Profiler EndPoint feed profiling event occurred

  Message Description: Profiler re-profiles the endpoint due to Feed Service policy

Local Target Message Format: <timestamp> <seq_num> 80013 INFO Profiler: Profiler EndPoint feed profiling event occurred, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80013 INFO Profiler: Profiler EndPoint feed profiling event occurred, <log details>

- **Message Code:** 80014

  Severity: INFO

  Message Text: Profiler EndPoint purge event occurred

  Message Description: This message is generated when a profiler end point purge policy is evaluated and matched

  Local Target Message Format: <timestamp> <seq_num> 80014 INFO Profiler: Profiler EndPoint purge event occurred, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80014 INFO Profiler: Profiler EndPoint purge event occurred, <log details>

- **Message Code:** 80015

  Severity: WARN

  Message Text: Profiler queue size limit has been reached.

  Message Description: Profiler queue size limit has been reached. Events received after the queue size limit has been reached will be dropped.

  Local Target Message Format: <timestamp> <seq_num> 80015 WARN Profiler: Profiler queue size limit has been reached., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80015 WARN Profiler: Profiler queue size limit has been reached., <log details>

- **Message Code:** 80016

  Severity: WARN

  Message Text: Anomalous behavior detected

  Message Description: MAC spoofing detection is enabled and endpoints exhibit anomalous behavior

  Local Target Message Format: <timestamp> <seq_num> 80016 WARN Profiler: Anomalous behavior detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 80016 WARN Profiler: Anomalous behavior detected, <log details>

- **Message Code:** 80017

  Severity: INFO

  Message Text: Edda schedular job started

  Message Description: Edda schedular job started

Local Target Message Format: <timestamp> <seq_num>80017 INFO Edda-Connector Edda schedular job started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>80017 INFO Edda-Connector Edda schedular job started, <log details>

- **Message Code:** 80018

  Severity: INFO

  Message Text: Edda new connector has been added or modified

  Message Description: Edda new connector has been added or modified

  Local Target Message Format: <timestamp> <seq_num>80018 INFO Edda-Connector Edda new connector has been added or modified, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>80018 INFO Edda-Connector Edda new connector has been added or modified, <log details>

- **Message Code:** 80019

  Severity: INFO

  Message Text: Edda connector has been deleted

  Message Description: Edda connector has been deleted

  Local Target Message Format: <timestamp> <seq_num>80019 INFO Edda-Connector Edda connector has been deleted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>80019 INFO Edda-Connector Edda connector has been deleted, <log details>

- **Message Code:** 80020

  Severity: INFO

  Message Text: Chatty Endpoint detected

  Message Description: Profiler Chatty Endpoints detected

  Local Target Message Format: <timestamp> <seq_num>80020 INFO Profiler Chatty Endpoint detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>80020 INFO Profiler Chatty Endpoint detected, <log details>

RADIUS Accounting

- **Message Code:** 3000

  Severity: NOTICE

Message Text: RADIUS Accounting start request

Message Description: RADIUS Accounting start request

Local Target Message Format: <timestamp> <seq_num> 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, <log details>

- **Message Code:** 3001

  Severity: NOTICE

  Message Text: RADIUS Accounting stop request

  Message Description: RADIUS Accounting stop request

  Local Target Message Format: <timestamp> <seq_num> 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, <log details>

- **Message Code:** 3002

  Severity: NOTICE

  Message Text: RADIUS Accounting watchdog update

  Message Description: RADIUS Accounting watchdog update

  Local Target Message Format: <timestamp> <seq_num> 3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog update, <log details>

- **Message Code:** 3003

  Severity: NOTICE

  Message Text: RADIUS Accounting is on

  Message Description: RADIUS Accounting is on

  Local Target Message Format: <timestamp> <seq_num> 3003 NOTICE Radius-Accounting: RADIUS Accounting is on, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3003 NOTICE Radius-Accounting: RADIUS Accounting is on, <log details>

- **Message Code:** 3004

  Severity: NOTICE

  Message Text: RADIUS Accounting is off

Message Description: RADIUS Accounting is off

Local Target Message Format: <timestamp> <seq_num> 3004 NOTICE Radius-Accounting: RADIUS Accounting is off, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3004 NOTICE Radius-Accounting: RADIUS Accounting is off, <log details>

- **Message Code:** 3005

  Severity: NOTICE

  Message Text: RADIUS Accounting tunnel start request

  Message Description: RADIUS Accounting tunnel start request

  Local Target Message Format: <timestamp> <seq_num> 3005 NOTICE Radius-Accounting: RADIUS Accounting tunnel start request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3005 NOTICE Radius-Accounting: RADIUS Accounting tunnel start request, <log details>

- **Message Code:** 3006

  Severity: NOTICE

  Message Text: RADIUS Accounting tunnel stop request

  Message Description: RADIUS Accounting tunnel stop request

  Local Target Message Format: <timestamp> <seq_num> 3006 NOTICE Radius-Accounting: RADIUS Accounting tunnel stop request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3006 NOTICE Radius-Accounting: RADIUS Accounting tunnel stop request, <log details>

- **Message Code:** 3007

  Severity: NOTICE

  Message Text: RADIUS Accounting tunnel rejected

  Message Description: RADIUS Accounting tunnel rejected

  Local Target Message Format: <timestamp> <seq_num> 3007 NOTICE Radius-Accounting: RADIUS Accounting tunnel rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3007 NOTICE Radius-Accounting: RADIUS Accounting tunnel rejected, <log details>

- **Message Code:** 3008

  Severity: NOTICE

  Message Text: RADIUS Accounting tunnel link start

  Message Description: RADIUS Accounting tunnel link start

Local Target Message Format: <timestamp> <seq_num> 3008 NOTICE Radius-Accounting: RADIUS Accounting tunnel link start, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3008 NOTICE Radius-Accounting: RADIUS Accounting tunnel link start, <log details>

- **Message Code:** 3009

  Severity: NOTICE

  Message Text: RADIUS Accounting tunnel link stop

  Message Description: RADIUS Accounting tunnel link stop

  Local Target Message Format: <timestamp> <seq_num> 3009 NOTICE Radius-Accounting: RADIUS Accounting tunnel link stop, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3009 NOTICE Radius-Accounting: RADIUS Accounting tunnel link stop, <log details>

- **Message Code:** 3010

  Severity: NOTICE

  Message Text: RADIUS Accounting tunnel link rejected

  Message Description: RADIUS Accounting tunnel link rejected

  Local Target Message Format: <timestamp> <seq_num> 3010 NOTICE Radius-Accounting: RADIUS Accounting tunnel link rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3010 NOTICE Radius-Accounting: RADIUS Accounting tunnel link rejected, <log details>

RADIUS Diagnostics

- **Message Code:** 11001

  Severity: DEBUG

  Message Text: Received RADIUS Access-Request

  Message Description: Received RADIUS Access-Request

  Local Target Message Format: <timestamp> <seq_num> 11001 DEBUG RADIUS: Received RADIUS Access-Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11001 DEBUG RADIUS: Received RADIUS Access-Request, <log details>

- **Message Code:** 11002

  Severity: DEBUG

Message Text: Returned RADIUS Access-Accept

Message Description: Returned RADIUS Access-Accept - authentication succeeded

Local Target Message Format: <timestamp> <seq_num> 11002 DEBUG RADIUS: Returned RADIUS Access-Accept, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11002 DEBUG RADIUS: Returned RADIUS Access-Accept, <log details>

- **Message Code:** 11003

  Severity: DEBUG

  Message Text: Returned RADIUS Access-Reject

  Message Description: Returned RADIUS Access-Reject - authentication failed

  Local Target Message Format: <timestamp> <seq_num> 11003 DEBUG RADIUS: Returned RADIUS Access-Reject, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11003 DEBUG RADIUS: Returned RADIUS Access-Reject, <log details>

- **Message Code:** 11004

  Severity: DEBUG

  Message Text: Received RADIUS Accounting-Request

  Message Description: Received RADIUS Accounting-Request

  Local Target Message Format: <timestamp> <seq_num> 11004 DEBUG RADIUS: Received RADIUS Accounting-Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11004 DEBUG RADIUS: Received RADIUS Accounting-Request, <log details>

- **Message Code:** 11005

  Severity: DEBUG

  Message Text: Returned RADIUS Accounting-Response

  Message Description: Returned RADIUS Accounting-Response - acknowledging receipt of Accounting-Request

  Local Target Message Format: <timestamp> <seq_num> 11005 DEBUG RADIUS: Returned RADIUS Accounting-Response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11005 DEBUG RADIUS: Returned RADIUS Accounting-Response, <log details>

- **Message Code:** 11006

  Severity: DEBUG

Message Text: Returned RADIUS Access-Challenge

Message Description: Returned RADIUS Access-Challenge asking for additional information

Local Target Message Format: <timestamp> <seq_num> 11006 DEBUG RADIUS: Returned RADIUS Access-Challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11006 DEBUG RADIUS: Returned RADIUS Access-Challenge, <log details>

- **Message Code:** 11007

  Severity: DEBUG

  Message Text: Could not locate Network Device or AAA Client

  Message Description: Could not find the network device or the AAA Client while accessing NAS by IP during authentication.

  Local Target Message Format: <timestamp> <seq_num> 11007 DEBUG RADIUS: Could not locate Network Device or AAA Client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11007 DEBUG RADIUS: Could not locate Network Device or AAA Client, <log details>

- **Message Code:** 11008

  Severity: DEBUG

  Message Text: Received Service-Type = Call Check (but there is no Calling-Station-ID)

  Message Description: Although the request contained a Service-Type attribute with the value, Call Check (10), the Host Lookup UseCase was not detected. This is because the Calling-Station-ID attribute was not present in the request

  Local Target Message Format: <timestamp> <seq_num> 11008 DEBUG RADIUS: Received Service-Type = Call Check (but there is no Calling-Station-ID), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11008 DEBUG RADIUS: Received Service-Type = Call Check (but there is no Calling-Station-ID), <log details>

- **Message Code:** 11009

  Severity: INFO

  Message Text: RADIUS listener started

  Message Description: Started listening for incoming RADIUS requests on submitted ports

  Local Target Message Format: <timestamp> <seq_num> 11009 INFO RADIUS: RADIUS listener started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11009 INFO RADIUS: RADIUS listener started, <log details>

- **Message Code:** 11010

Severity: INFO

Message Text: RADIUS listener stopped

Message Description: Stopped listening for RADIUS requests

Local Target Message Format: <timestamp> <seq_num> 11010 INFO RADIUS: RADIUS listener stopped, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11010 INFO RADIUS: RADIUS listener stopped, <log details>

- **Message Code:** 11011

  Severity: ERROR

  Message Text: RADIUS listener failed to open

  Message Description: Could not open one or more of the ports used to receive RADIUS requests

  Local Target Message Format: <timestamp> <seq_num> 11011 ERROR RADIUS: RADIUS listener failed to open, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11011 ERROR RADIUS: RADIUS listener failed to open, <log details>

- **Message Code:** 11012

  Severity: ERROR

  Message Text: RADIUS packet contains invalid header

  Message Description: The header of the RADIUS packet did not parse correctly

  Local Target Message Format: <timestamp> <seq_num> 11012 ERROR RADIUS: RADIUS packet contains invalid header, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11012 ERROR RADIUS: RADIUS packet contains invalid header, <log details>

- **Message Code:** 11014

  Severity: ERROR

  Message Text: RADIUS packet contains invalid attribute(s)

  Message Description: One of the attributes in the RADIUS packet did not parse correctly

  Local Target Message Format: <timestamp> <seq_num> 11014 ERROR RADIUS: RADIUS packet contains invalid attribute(s), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11014 ERROR RADIUS: RADIUS packet contains invalid attribute(s), <log details>

- **Message Code:** 11015

  Severity: WARN

Message Text: An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing

Message Description: According to the RADIUS standard, an Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address or a NAS-Identifier. This condition is ignored and processing continues.

Local Target Message Format: <timestamp> <seq_num> 11015 WARN RADIUS: An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11015 WARN RADIUS: An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing, <log details>

- **Message Code:** 11016

  Severity: DEBUG

  Message Text: Translating EAP protocol result into RADIUS result

  Message Description: Translating EAP protocol result into RADIUS result

  Local Target Message Format: <timestamp> <seq_num> 11016 DEBUG RADIUS: Translating EAP protocol result into RADIUS result, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11016 DEBUG RADIUS: Translating EAP protocol result into RADIUS result, <log details>

- **Message Code:** 11017

  Severity: DEBUG

  Message Text: RADIUS created a new session

  Message Description: RADIUS created a new session for the request

  Local Target Message Format: <timestamp> <seq_num> 11017 DEBUG RADIUS: RADIUS created a new session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11017 DEBUG RADIUS: RADIUS created a new session, <log details>

- **Message Code:** 11018

  Severity: DEBUG

  Message Text: RADIUS is re-using an existing session

  Message Description: RADIUS is re-using an existing session while processing this request

  Local Target Message Format: <timestamp> <seq_num> 11018 DEBUG RADIUS: RADIUS is re-using an existing session, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11018 DEBUG RADIUS: RADIUS is re-using an existing session, <log details>

- **Message Code:** 11019

  Severity: INFO

  Message Text: Selected DenyAccess Service

  Message Description: The Service Selection policy selected the DenyAccess Service

  Local Target Message Format: <timestamp> <seq_num> 11019 INFO RADIUS: Selected DenyAccess Service, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11019 INFO RADIUS: Selected DenyAccess Service, <log details>

- **Message Code:** 11020

  Severity: ERROR

  Message Text: RADIUS session authorization did not return a valid result

  Message Description: An unexpected error occurred. The RADIUS session authorization should return a valid result.

  Local Target Message Format: <timestamp> <seq_num> 11020 ERROR RADIUS: RADIUS session authorization did not return a valid result, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11020 ERROR RADIUS: RADIUS session authorization did not return a valid result, <log details>

- **Message Code:** 11021

  Severity: ERROR

  Message Text: RADIUS could not decipher password. packet missing necessary attributes

  Message Description: RADIUS could not decipher password because the packet does not have the necessary attributes

  Local Target Message Format: <timestamp> <seq_num> 11021 ERROR RADIUS: RADIUS could not decipher password. packet missing necessary attributes, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11021 ERROR RADIUS: RADIUS could not decipher password. packet missing necessary attributes, <log details>

- **Message Code:** 11022

  Severity: DEBUG

  Message Text: Added the dACL specified in the Authorization Profile

  Message Description: The Downloadable ACL (dACL) specified in the Authorization Profile, was added to the set of attributes that should be returned in the response

  Local Target Message Format: <timestamp> <seq_num> 11022 DEBUG DACL: Added the dACL specified in the Authorization Profile, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11022 DEBUG DACL: Added the dACL specified in the Authorization Profile, <log details>

- **Message Code:** 11023

  Severity: WARN

  Message Text: The requested dACL is not found. This is an unknown dACL name

  Message Description: Could not find the Downloadable ACL (dACL) specified in the Authorization Profile

  Local Target Message Format: <timestamp> <seq_num> 11023 WARN DACL: The requested dACL is not found. This is an unknown dACL name, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11023 WARN DACL: The requested dACL is not found. This is an unknown dACL name, <log details>

- **Message Code:** 11024

  Severity: ERROR

  Message Text: The Access-Request for the requested dACL is missing a Message-Authenticator attribute. The request is rejected

  Message Description: The Access-Request does not have a Message-Authenticator attribute that is required for Downloadable ACL requests. The request is rejected because of this

  Local Target Message Format: <timestamp> <seq_num> 11024 ERROR DACL: The Access-Request for the requested dACL is missing a Message-Authenticator attribute. The request is rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11024 ERROR DACL: The Access-Request for the requested dACL is missing a Message-Authenticator attribute. The request is rejected, <log details>

- **Message Code:** 11025

  Severity: ERROR

  Message Text: The Access-Request for the requested dACL is missing a cisco-av-pair attribute with the value aaa:event=acl-download. The request is rejected

  Message Description: The Access-Request is missing a cisco-av-pair attribute with the value aaa:event=acl-download that is required for Downloadable ACL requests. The request is rejected because of this.

  Local Target Message Format: <timestamp> <seq_num> 11025 ERROR DACL: The Access-Request for the requested dACL is missing a cisco-av-pair attribute with the value aaa:event=acl-download. The request is rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11025 ERROR DACL: The Access-Request for the requested dACL is missing a cisco-av-pair attribute with the value aaa:event=acl-download. The request is rejected, <log details>

- **Message Code:** 11026

  Severity: ERROR

  Message Text: The requested dACL is not found

  Message Description: The version of the Downloadable ACL requested in the Access-Request is not found. The request is rejected because of this.

  Local Target Message Format: <timestamp> <seq_num> 11026 ERROR DACL: The requested dACL is not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11026 ERROR DACL: The requested dACL is not found, <log details>

- **Message Code:** 11027

  Severity: DEBUG

  Message Text: Detected Host Lookup UseCase (Service-Type = Call Check (10))

  Message Description: Detected Host Lookup UseCase (Service-Type = Call Check (10))

  Local Target Message Format: <timestamp> <seq_num> 11027 DEBUG RADIUS: Detected Host Lookup UseCase (Service-Type = Call Check (10)), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11027 DEBUG RADIUS: Detected Host Lookup UseCase (Service-Type = Call Check (10)), <log details>

- **Message Code:** 11028

  Severity: DEBUG

  Message Text: Detected Host Lookup UseCase (UserName = Calling-Station-ID)

  Message Description: Detected Host Lookup UseCase (UserName = Calling-Station-ID)

  Local Target Message Format: <timestamp> <seq_num> 11028 DEBUG RADIUS: Detected Host Lookup UseCase (UserName = Calling-Station-ID), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11028 DEBUG RADIUS: Detected Host Lookup UseCase (UserName = Calling-Station-ID), <log details>

- **Message Code:** 11029

  Severity: WARN

  Message Text: Unsupported RADIUS packet type

  Message Description: The RADIUS packet type is not supported by ISE

  Local Target Message Format: <timestamp> <seq_num> 11029 WARN RADIUS: Unsupported RADIUS packet type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11029 WARN RADIUS: Unsupported RADIUS packet type, <log details>

- **Message Code:** 11030

  Severity: WARN

  Message Text: Pre-parsing of the RADIUS packet failed

  Message Description: Pre-parsing of the RADIUS packet failed. This packet does not appear to be a valid RADIUS packet

  Local Target Message Format: <timestamp> <seq_num> 11030 WARN RADIUS: Pre-parsing of the RADIUS packet failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11030 WARN RADIUS: Pre-parsing of the RADIUS packet failed, <log details>

- **Message Code:** 11031

  Severity: WARN

  Message Text: RADIUS packet type is not a valid Request

  Message Description: RADIUS packet type is not a valid Request.

  Local Target Message Format: <timestamp> <seq_num> 11031 WARN RADIUS: RADIUS packet type is not a valid Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11031 WARN RADIUS: RADIUS packet type is not a valid Request, <log details>

- **Message Code:** 11032

  Severity: INFO

  Message Text: Selected Access Service type is not Device Administration

  Message Description: TACACS+ requests can only be processed by Access Services that are of type Device Administration

  Local Target Message Format: <timestamp> <seq_num> 11032 INFO RADIUS: Selected Access Service type is not Device Administration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11032 INFO RADIUS: Selected Access Service type is not Device Administration, <log details>

- **Message Code:** 11033

  Severity: INFO

  Message Text: Selected Service type is not Network Access

  Message Description: RADIUS requests can only be processed by Access Services that are of type Network Access

  Local Target Message Format: <timestamp> <seq_num> 11033 INFO RADIUS: Selected Service type is not Network Access, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11033 INFO RADIUS: Selected Service type is not Network Access, <log details>

- **Message Code:** 11034

  Severity: DEBUG

  Message Text: Process Host Lookup is disabled. (Service-Type = Call Check (10) cannot be applied)

  Message Description: Process Host Lookup option was not enabled in the Allowed Protocols; so the earlier detection of Service-Type = Call Check (10) is ignored

  Local Target Message Format: <timestamp> <seq_num> 11034 DEBUG RADIUS: Process Host Lookup is disabled. (Service-Type = Call Check (10) cannot be applied), <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11034 DEBUG RADIUS: Process Host Lookup is disabled. (Service-Type = Call Check (10) cannot be applied), <log details>

- **Message Code:** 11035

  Severity: WARN

  Message Text: The session associated with the requested dACL has timed out

  Message Description: The session associated with the requested Downloadable ACL (dACL) has timed out. The request is rejected

  Local Target Message Format: <timestamp> <seq_num> 11035 WARN DACL: The session associated with the requested dACL has timed out, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11035 WARN DACL: The session associated with the requested dACL has timed out, <log details>

- **Message Code:** 11036

  Severity: WARN

  Message Text: The Message-Authenticator RADIUS attribute is invalid

  Message Description: The Message-Authenticator RADIUS attribute is invalid. This maybe because of mismatched Shared Secrets.

  Local Target Message Format: <timestamp> <seq_num> 11036 WARN RADIUS: The Message-Authenticator RADIUS attribute is invalid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11036 WARN RADIUS: The Message-Authenticator RADIUS attribute is invalid, <log details>

- **Message Code:** 11037

  Severity: ERROR

  Message Text: Dropped accounting request received via unsupported port

  Message Description: Accounting request was dropped because it was received via an unsupported UDP port number.

Local Target Message Format: <timestamp> <seq_num> 11037 ERROR RADIUS: Dropped accounting request received via unsupported port, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11037 ERROR RADIUS: Dropped accounting request received via unsupported port, <log details>

- **Message Code:** 11038

  Severity: WARN

  Message Text: RADIUS Accounting-Request header contains invalid Authenticator field

  Message Description: ISE cannot validate the Authenticator field in the header of the RADIUS Accounting-Request packet. Note that the Authenticator field should not be confused with the Message-Authenticator RADIUS attribute.

  Local Target Message Format: <timestamp> <seq_num> 11038 WARN RADIUS: RADIUS Accounting-Request header contains invalid Authenticator field, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11038 WARN RADIUS: RADIUS Accounting-Request header contains invalid Authenticator field, <log details>

- **Message Code:** 11039

  Severity: INFO

  Message Text: RADIUS authentication request rejected due to critical logging error

  Message Description: A RADIUS authentication request was rejected due to a critical logging error.

  Local Target Message Format: <timestamp> <seq_num> 11039 INFO RADIUS: RADIUS authentication request rejected due to critical logging error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11039 INFO RADIUS: RADIUS authentication request rejected due to critical logging error, <log details>

- **Message Code:** 11040

  Severity: INFO

  Message Text: RADIUS accounting request dropped due to critical logging error

  Message Description: The RADIUS accounting request was dropped due to a critical logging error.

  Local Target Message Format: <timestamp> <seq_num> 11040 INFO RADIUS: RADIUS accounting request dropped due to critical logging error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11040 INFO RADIUS: RADIUS accounting request dropped due to critical logging error, <log details>

- **Message Code:** 11041

  Severity: WARN

  Message Text: RADIUS PAP session timed out

  Message Description: A RADIUS PAP session timed out.

Local Target Message Format: <timestamp> <seq_num> 11041 WARN RADIUS: RADIUS PAP session timed out, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11041 WARN RADIUS: RADIUS PAP session timed out, <log details>

- **Message Code:** 11042

  Severity: DEBUG

  Message Text: Received duplicate RADIUS request; retransmitting previous response

  Message Description: Received a duplicate RADIUS request. Retransmitting the previously transmitted corresponding RADIUS response.

  Local Target Message Format: <timestamp> <seq_num> 11042 DEBUG RADIUS: Received duplicate RADIUS request; retransmitting previous response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11042 DEBUG RADIUS: Received duplicate RADIUS request; retransmitting previous response, <log details>

- **Message Code:** 11043

  Severity: DEBUG

  Message Text: Received RADIUS CoA request

  Message Description: Received RADIUS CoA request

  Local Target Message Format: <timestamp> <seq_num> 11043 DEBUG RADIUS: Received RADIUS CoA request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11043 DEBUG RADIUS: Received RADIUS CoA request, <log details>

- **Message Code:** 11044

  Severity: DEBUG

  Message Text: Received RADIUS disconnect request

  Message Description: Received RADIUS disconnect request

  Local Target Message Format: <timestamp> <seq_num> 11044 DEBUG RADIUS: Received RADIUS disconnect request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11044 DEBUG RADIUS: Received RADIUS disconnect request, <log details>

- **Message Code:** 11045

  Severity: DEBUG

  Message Text: Returned RADIUS CoA ACK

  Message Description: Returned RADIUS CoA ACK

Local Target Message Format: <timestamp> <seq_num> 11045 DEBUG RADIUS: Returned RADIUS CoA ACK, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11045 DEBUG RADIUS: Returned RADIUS CoA ACK, <log details>

- **Message Code:** 11046

  Severity: DEBUG

  Message Text: Returned RADIUS CoA NAK

  Message Description: Returned RADIUS CoA NAK

  Local Target Message Format: <timestamp> <seq_num> 11046 DEBUG RADIUS: Returned RADIUS CoA NAK, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11046 DEBUG RADIUS: Returned RADIUS CoA NAK, <log details>

- **Message Code:** 11047

  Severity: DEBUG

  Message Text: Returned RADIUS disconnect ACK

  Message Description: Returned RADIUS disconnect ACK

  Local Target Message Format: <timestamp> <seq_num> 11047 DEBUG RADIUS: Returned RADIUS disconnect ACK, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11047 DEBUG RADIUS: Returned RADIUS disconnect ACK, <log details>

- **Message Code:** 11048

  Severity: DEBUG

  Message Text: Returned RADIUS disconnect NAK

  Message Description: Returned RADIUS disconnect NAK

  Local Target Message Format: <timestamp> <seq_num> 11048 DEBUG RADIUS: Returned RADIUS disconnect NAK, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11048 DEBUG RADIUS: Returned RADIUS disconnect NAK, <log details>

- **Message Code:** 11049

  Severity: INFO

  Message Text: Settings of RADIUS default network device will be used

  Message Description: Settings of RADIUS default network device will be used

Local Target Message Format: <timestamp> <seq_num> 11049 INFO RADIUS: Settings of RADIUS default network device will be used, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11049 INFO RADIUS: Settings of RADIUS default network device will be used, <log details>

- **Message Code:** 11051

  Severity: WARN

  Message Text: RADIUS packet contains invalid state attribute

  Message Description: The state attribute in the RADIUS packet did not match any active session.

  Local Target Message Format: <timestamp> <seq_num> 11051 WARN RADIUS: RADIUS packet contains invalid state attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11051 WARN RADIUS: RADIUS packet contains invalid state attribute, <log details>

- **Message Code:** 11052

  Severity: ERROR

  Message Text: Authentication request dropped due to unsupported port number

  Message Description: An authentication request was dropped because it was received through an unsupported port number.

  Local Target Message Format: <timestamp> <seq_num> 11052 ERROR RADIUS: Authentication request dropped due to unsupported port number, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11052 ERROR RADIUS: Authentication request dropped due to unsupported port number, <log details>

- **Message Code:** 11053

  Severity: WARN

  Message Text: Invalid attributes in outgoing radius packet - possibly some attributes exceeded their size limit

  Message Description: The RADIUS response packet is invalid. A likely reason is that at least one of the attributes has exceeded its allowed length or that the total size of the attributes attached to this response packet exceeded 4k (max radius packet size)

  Local Target Message Format: <timestamp> <seq_num> 11053 WARN RADIUS: Invalid attributes in outgoing radius packet - possibly some attributes exceeded their size limit, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11053 WARN RADIUS: Invalid attributes in outgoing radius packet - possibly some attributes exceeded their size limit, <log details>

- **Message Code:** 11054

  Severity: WARN

Message Text: Request from a non-wireless device was dropped due to installed Wireless license

Message Description: The RADIUS request from a non-wireless device was dropped because the installed license is for wireless devices only

Local Target Message Format: <timestamp> <seq_num> 11054 WARN RADIUS: Request from a non-wireless device was dropped due to installed Wireless license, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11054 WARN RADIUS: Request from a non-wireless device was dropped due to installed Wireless license, <log details>

- **Message Code:** 11055

  Severity: INFO

  Message Text: User name change detected for the session. Attributes for the session will be removed from the cache

  Message Description: User name change detected for the session. Attributes for the session will be removed from the cache

  Local Target Message Format: <timestamp> <seq_num> 11055 INFO RADIUS: User name change detected for the session. Attributes for the session will be removed from the cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11055 INFO RADIUS: User name change detected for the session. Attributes for the session will be removed from the cache, <log details>

- **Message Code:** 11056

  Severity: INFO

  Message Text: Duplicate of previously processed (but not the last) RADIUS Request packet received

  Message Description: Duplicate of previously processed (but not the last) RADIUS Request packet received

  Local Target Message Format: <timestamp> <seq_num> 11056 INFO RADIUS: Duplicate of previously processed (but not the last) RADIUS Request packet received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11056 INFO RADIUS: Duplicate of previously processed (but not the last) RADIUS Request packet received, <log details>

- **Message Code:** 11057

  Severity: WARN

  Message Text: The Access-Request for the requested RADIUS is missing

  Message Description: Please mention that Message-Authenticator RADIUS attribute is configured as mandatory in Allowed Protocols

  Local Target Message Format: <timestamp> <seq_num> 11057 WARN RADIUS: The Access-Request for the requested RADIUS is missing, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11057 WARN RADIUS: The Access-Request for the requested RADIUS is missing, <log details>

- **Message Code:** 11058

  Severity: DEBUG

  Message Text: An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing

  Message Description: According to the RADIUS standard, an Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address or a NAS-Identifier. This condition is ignored and processing continues. This message reports on every Access-Request.

  Local Target Message Format: <timestamp> <seq_num>RADIUS An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing DEBUG According to the RADIUS standard, an Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address or a NAS-Identifier. This condition is ignored and processing continues. This message reports on every Access-Request., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing DEBUG According to the RADIUS standard, an Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address or a NAS-Identifier. This condition is ignored and processing continues. This message reports on every Access-Request., <log details>

- **Message Code:** 11059

  Severity: WARN

  Message Text: DACL attribute is not found due to bad configuration

  Message Description: DACL attribute is not found due to bad configuration

  Local Target Message Format: <timestamp> <seq_num>DACL DACL attribute is not found due to bad configuration WARN DACL attribute is not found due to bad configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>DACL DACL attribute is not found due to bad configuration WARN DACL attribute is not found due to bad configuration, <log details>

- **Message Code:** 11100

  Severity: DEBUG

  Message Text: RADIUS-Client about to send request

  Message Description: RADIUS-Client about to send request

  Local Target Message Format: <timestamp> <seq_num> 11100 DEBUG RADIUS-Client: RADIUS-Client about to send request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11100 DEBUG RADIUS-Client: RADIUS-Client about to send request, <log details>

- **Message Code:** 11101

  Severity: DEBUG

  Message Text: RADIUS-Client received response

Message Description: RADIUS-Client received a response

Local Target Message Format: <timestamp> <seq_num> 11101 DEBUG RADIUS-Client: RADIUS-Client received response, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11101 DEBUG RADIUS-Client: RADIUS-Client received response, <log details>

- **Message Code:** 11102

  Severity: DEBUG

  Message Text: RADIUS-Client silently discarded invalid response

  Message Description: RADIUS-Client silently discarded an invalid response

  Local Target Message Format: <timestamp> <seq_num> 11102 DEBUG RADIUS-Client: RADIUS-Client silently discarded invalid response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11102 DEBUG RADIUS-Client: RADIUS-Client silently discarded invalid response, <log details>

- **Message Code:** 11103

  Severity: ERROR

  Message Text: RADIUS-Client encountered error during processing flow

  Message Description: RADIUS-Client encountered an error during processing flow

  Local Target Message Format: <timestamp> <seq_num> 11103 ERROR RADIUS-Client: RADIUS-Client encountered error during processing flow, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11103 ERROR RADIUS-Client: RADIUS-Client encountered error during processing flow, <log details>

- **Message Code:** 11104

  Severity: DEBUG

  Message Text: RADIUS-Client request timeout expired

  Message Description: RADIUS-Client request timeout expired

  Local Target Message Format: <timestamp> <seq_num> 11104 DEBUG RADIUS-Client: RADIUS-Client request timeout expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11104 DEBUG RADIUS-Client: RADIUS-Client request timeout expired, <log details>

- **Message Code:** 11105

  Severity: DEBUG

  Message Text: Request received from a device that is configured with KeyWrap in ISE.

  Message Description: Request received from a device that is configured with KeyWrap in ISE.

Local Target Message Format: <timestamp> <seq_num> 11105 DEBUG RADIUS-Client: Request received from a device that is configured with KeyWrap in ISE., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11105 DEBUG RADIUS-Client: Request received from a device that is configured with KeyWrap in ISE., <log details>

- **Message Code:** 11106

  Severity: DEBUG

  Message Text: Error in KeyWrap configuration

  Message Description: Error in KeyWrap configuration

  Local Target Message Format: <timestamp> <seq_num> 11106 DEBUG RADIUS-Client: Error in KeyWrap configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11106 DEBUG RADIUS-Client: Error in KeyWrap configuration, <log details>

- **Message Code:** 11107

  Severity: DEBUG

  Message Text: Required attributes for KeyWrap are missing

  Message Description: Required attributes for KeyWrap are missing

  Local Target Message Format: <timestamp> <seq_num> 11107 DEBUG RADIUS-Client: Required attributes for KeyWrap are missing, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11107 DEBUG RADIUS-Client: Required attributes for KeyWrap are missing, <log details>

- **Message Code:** 11108

  Severity: DEBUG

  Message Text: Missing required EapMessage attribute for KeyWrap

  Message Description: The RADIUS request from a KeyWrap enabled device is missing the required EapMessage attribute

  Local Target Message Format: <timestamp> <seq_num> 11108 DEBUG RADIUS-Client: Missing required EapMessage attribute for KeyWrap, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11108 DEBUG RADIUS-Client: Missing required EapMessage attribute for KeyWrap, <log details>

- **Message Code:** 11109

  Severity: DEBUG

  Message Text: RADIUS request improperly contains both KeyWrap and MessageAuthenticator attributes

  Message Description: RADIUS request improperly contains both KeyWrap and MessageAuthenticator attributes

Local Target Message Format: <timestamp> <seq_num> 11109 DEBUG RADIUS-Client: RADIUS request improperly contains both KeyWrap and MessageAuthenticator attributes, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11109 DEBUG RADIUS-Client: RADIUS request improperly contains both KeyWrap and MessageAuthenticator attributes, <log details>

- **Message Code:** 11110

  Severity: DEBUG

  Message Text: Request received from a KeyWrap enabled device. The TunnelPassword attribute is present in KeyWrap.

  Message Description: Request received from a KeyWrap enabled device. The TunnelPassword attribute is present in KeyWrap.

  Local Target Message Format: <timestamp> <seq_num> 11110 DEBUG RADIUS-Client: Request received from a KeyWrap enabled device. The TunnelPassword attribute is present in KeyWrap., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11110 DEBUG RADIUS-Client: Request received from a KeyWrap enabled device. The TunnelPassword attribute is present in KeyWrap., <log details>

- **Message Code:** 11111

  Severity: DEBUG

  Message Text: RADIUS request has been received with KeyWrap attributes. However, KeyWrap is not configured for the requesting device in ISE.

  Message Description: RADIUS request has been received with KeyWrap attributes. However, KeyWrap is not configured for the requesting device in ISE.

  Local Target Message Format: <timestamp> <seq_num> 11111 DEBUG RADIUS-Client: RADIUS request has been received with KeyWrap attributes. However, KeyWrap is not configured for the requesting device in ISE., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11111 DEBUG RADIUS-Client: RADIUS request has been received with KeyWrap attributes. However, KeyWrap is not configured for the requesting device in ISE., <log details>

- **Message Code:** 11112

  Severity: DEBUG

  Message Text: KeyWrap keys accepted from PAC_OPAQUE.

  Message Description: KeyWrap keys accepted from PAC_OPAQUE.

  Local Target Message Format: <timestamp> <seq_num> 11112 DEBUG RADIUS-Client: KeyWrap keys accepted from PAC_OPAQUE., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11112 DEBUG RADIUS-Client: KeyWrap keys accepted from PAC_OPAQUE., <log details>

- **Message Code:** 11113

  Severity: DEBUG

  Message Text: KeyWrap is not supported in Proxy.

  Message Description: KeyWrap is not supported in Proxy.

  Local Target Message Format: <timestamp> <seq_num> 11113 DEBUG RADIUS-Client: KeyWrap is not supported in Proxy., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11113 DEBUG RADIUS-Client: KeyWrap is not supported in Proxy., <log details>

- **Message Code:** 11114

  Severity: DEBUG

  Message Text: KeyWrap parameters on RADIUS request packet are not compatible with the earlier KeyWrap request in this session.

  Message Description: KeyWrap parameters on RADIUS request packet are not compatible with the earlier KeyWrap request in this session.

  Local Target Message Format: <timestamp> <seq_num> 11114 DEBUG RADIUS-Client: KeyWrap parameters on RADIUS request packet are not compatible with the earlier KeyWrap request in this session., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11114 DEBUG RADIUS-Client: KeyWrap parameters on RADIUS request packet are not compatible with the earlier KeyWrap request in this session., <log details>

- **Message Code:** 11115

  Severity: ERROR

  Message Text: The AAA Client Message Authenticator Code Key does not match the configured ISE Server Message Authenticator Code Key.

  Message Description: The AAA Client Message Authenticator Code Key does not match the configured ISE Server Message Authenticator Code Key.

  Local Target Message Format: <timestamp> <seq_num> 11115 ERROR RADIUS: The AAA Client Message Authenticator Code Key does not match the configured ISE Server Message Authenticator Code Key., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11115 ERROR RADIUS: The AAA Client Message Authenticator Code Key does not match the configured ISE Server Message Authenticator Code Key., <log details>

- **Message Code:** 11116

  Severity: DEBUG

  Message Text: Stitched existing session from Session Cache

  Message Description: Stitched existing session from Session Cache. Session ID is reused.

Local Target Message Format: <timestamp> <seq_num> 11116 DEBUG RADIUS: Stitched existing session from Session Cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11116 DEBUG RADIUS: Stitched existing session from Session Cache, <log details>

- **Message Code:** 11117

  Severity: DEBUG

  Message Text: Generated a new session ID

  Message Description: Generated a new session ID based on the Radius attributes

  Local Target Message Format: <timestamp> <seq_num> 11117 DEBUG RADIUS: Generated a new session ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11117 DEBUG RADIUS: Generated a new session ID, <log details>

- **Message Code:** 11118

  Severity: WARN

  Message Text: Message-Authenticator attribute is missing in RADIUS response

  Message Description: Message-Authenticator attribute is missing in RADIUS response

  Local Target Message Format: <timestamp> <seq_num>11118 WARN RADIUS-Client Message-Authenticator attribute is missing in RADIUS response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11118 WARN RADIUS-Client Message-Authenticator attribute is missing in RADIUS response, <log details>

- **Message Code:** 11200

  Severity: ERROR

  Message Text: Received invalid dynamic authorization request

  Message Description: An invalid dynamic authorization request was received.

  Local Target Message Format: <timestamp> <seq_num> 11200 ERROR Dynamic-Authorization: Received invalid dynamic authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11200 ERROR Dynamic-Authorization: Received invalid dynamic authorization request, <log details>

- **Message Code:** 11201

  Severity: DEBUG

  Message Text: Received disconnect dynamic authorization request

  Message Description: A disconnect dynamic authorization request was received

Local Target Message Format: <timestamp> <seq_num> 11201 DEBUG Dynamic-Authorization: Received disconnect dynamic authorization request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11201 DEBUG Dynamic-Authorization: Received disconnect dynamic authorization request, <log details>

- **Message Code:** 11202

  Severity: DEBUG

  Message Text: Received disconnect and port shutdown dynamic authorization request

  Message Description: A disconnect and port shutdown dynamic authorization request was received

  Local Target Message Format: <timestamp> <seq_num> 11202 DEBUG Dynamic-Authorization: Received disconnect and port shutdown dynamic authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11202 DEBUG Dynamic-Authorization: Received disconnect and port shutdown dynamic authorization request, <log details>

- **Message Code:** 11203

  Severity: DEBUG

  Message Text: Received disconnect and port bounce dynamic authorization request

  Message Description: A disconnect and port bounce dynamic authorization request was received

  Local Target Message Format: <timestamp> <seq_num> 11203 DEBUG Dynamic-Authorization: Received disconnect and port bounce dynamic authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11203 DEBUG Dynamic-Authorization: Received disconnect and port bounce dynamic authorization request, <log details>

- **Message Code:** 11204

  Severity: DEBUG

  Message Text: Received reauthenticate request

  Message Description: A reauthenticate request was received

  Local Target Message Format: <timestamp> <seq_num> 11204 DEBUG Dynamic-Authorization: Received reauthenticate request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11204 DEBUG Dynamic-Authorization: Received reauthenticate request, <log details>

- **Message Code:** 11205

  Severity: ERROR

  Message Text: Could not find Network Access Device

Message Description: Cannot find the Network Access Device designated for applying dynamic authorization change.

Local Target Message Format: <timestamp> <seq_num> 11205 ERROR Dynamic-Authorization: Could not find Network Access Device, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11205 ERROR Dynamic-Authorization: Could not find Network Access Device, <log details>

- **Message Code:** 11206

  Severity: ERROR

  Message Text: Could not find Client ISE Node

  Message Description: Cannot find the Client ISE Node.

  Local Target Message Format: <timestamp> <seq_num> 11206 ERROR Dynamic-Authorization: Could not find Client ISE Node, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11206 ERROR Dynamic-Authorization: Could not find Client ISE Node, <log details>

- **Message Code:** 11207

  Severity: DEBUG

  Message Text: Received disconnect dynamic authorization response

  Message Description: A disconnect dynamic authorization response has been received

  Local Target Message Format: <timestamp> <seq_num> 11207 DEBUG Dynamic-Authorization: Received disconnect dynamic authorization response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11207 DEBUG Dynamic-Authorization: Received disconnect dynamic authorization response, <log details>

- **Message Code:** 11208

  Severity: DEBUG

  Message Text: Received disconnect and port shutdown dynamic authorization response

  Message Description: A disconnect and port shutdown dynamic authorization response has been received

  Local Target Message Format: <timestamp> <seq_num> 11208 DEBUG Dynamic-Authorization: Received disconnect and port shutdown dynamic authorization response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11208 DEBUG Dynamic-Authorization: Received disconnect and port shutdown dynamic authorization response, <log details>

- **Message Code:** 11209

  Severity: DEBUG

  Message Text: Received disconnect and port bounce dynamic authorization response

Message Description: Received disconnect and port bounce dynamic authorization response.

Local Target Message Format: <timestamp> <seq_num> 11209 DEBUG Dynamic-Authorization: Received disconnect and port bounce dynamic authorization response, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11209 DEBUG Dynamic-Authorization: Received disconnect and port bounce dynamic authorization response, <log details>

- **Message Code:** 11210

  Severity: DEBUG

  Message Text: Received a reauthenticate response

  Message Description: Received a reauthenticate response.

  Local Target Message Format: <timestamp> <seq_num> 11210 DEBUG Dynamic-Authorization: Received a reauthenticate response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11210 DEBUG Dynamic-Authorization: Received a reauthenticate response, <log details>

- **Message Code:** 11211

  Severity: DEBUG

  Message Text: Proxying request to Dynamic Authorization Client ISE

  Message Description: Forwarding your request to Dynamic Authorization Client in ISE.

  Local Target Message Format: <timestamp> <seq_num> 11211 DEBUG Dynamic-Authorization: Proxying request to Dynamic Authorization Client ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11211 DEBUG Dynamic-Authorization: Proxying request to Dynamic Authorization Client ISE, <log details>

- **Message Code:** 11212

  Severity: DEBUG

  Message Text: Forwarding your request to Network Access Device

  Message Description: Forwarding your request to Network Access Device.

  Local Target Message Format: <timestamp> <seq_num> 11212 DEBUG Dynamic-Authorization: Forwarding your request to Network Access Device, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11212 DEBUG Dynamic-Authorization: Forwarding your request to Network Access Device, <log details>

- **Message Code:** 11213

  Severity: WARN

  Message Text: No response received from Network Access Device after sending a Dynamic Authorization request

Message Description: No response received from Network Access Device after sending a Dynamic Authorization request

Local Target Message Format: <timestamp> <seq_num> 11213 WARN Dynamic-Authorization: No response received from Network Access Device after sending a Dynamic Authorization request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11213 WARN Dynamic-Authorization: No response received from Network Access Device after sending a Dynamic Authorization request, <log details>

- **Message Code:** 11214

  Severity: WARN

  Message Text: An invalid response received from Network Access Device

  Message Description: An invalid response received from Network Access Device.

  Local Target Message Format: <timestamp> <seq_num> 11214 WARN Dynamic-Authorization: An invalid response received from Network Access Device, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11214 WARN Dynamic-Authorization: An invalid response received from Network Access Device, <log details>

- **Message Code:** 11215

  Severity: WARN

  Message Text: No response has been received from Dynamic Authorization Client in ISE

  Message Description: No response has been received from Dynamic Authorization Client in ISE.

  Local Target Message Format: <timestamp> <seq_num> 11215 WARN Dynamic-Authorization: No response has been received from Dynamic Authorization Client in ISE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11215 WARN Dynamic-Authorization: No response has been received from Dynamic Authorization Client in ISE, <log details>

- **Message Code:** 11216

  Severity: ERROR

  Message Text: The Internal Proxy PAC generation has failed

  Message Description: The Internal Proxy PAC generation has failed.

  Local Target Message Format: <timestamp> <seq_num> 11216 ERROR Dynamic-Authorization: The Internal Proxy PAC generation has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11216 ERROR Dynamic-Authorization: The Internal Proxy PAC generation has failed, <log details>

- **Message Code:** 11217

Severity: DEBUG

Message Text: Prepared the disconnect dynamic authorization request

Message Description: Prepared the disconnect dynamic authorization request.

Local Target Message Format: <timestamp> <seq_num> 11217 DEBUG Dynamic-Authorization: Prepared the disconnect dynamic authorization request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11217 DEBUG Dynamic-Authorization: Prepared the disconnect dynamic authorization request, <log details>

- **Message Code:** 11218

  Severity: DEBUG

  Message Text: Prepared the disconnect and port shutdown dynamic authorization request

  Message Description: Prepared the disconnect and port shutdown dynamic authorization request.

  Local Target Message Format: <timestamp> <seq_num> 11218 DEBUG Dynamic-Authorization: Prepared the disconnect and port shutdown dynamic authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11218 DEBUG Dynamic-Authorization: Prepared the disconnect and port shutdown dynamic authorization request, <log details>

- **Message Code:** 11219

  Severity: DEBUG

  Message Text: Prepared the disconnect and port bounce dynamic authorization request

  Message Description: Prepared the disconnect and port bounce dynamic authorization request.

  Local Target Message Format: <timestamp> <seq_num> 11219 DEBUG Dynamic-Authorization: Prepared the disconnect and port bounce dynamic authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11219 DEBUG Dynamic-Authorization: Prepared the disconnect and port bounce dynamic authorization request, <log details>

- **Message Code:** 11220

  Severity: DEBUG

  Message Text: Prepared the reauthenticate request

  Message Description: Prepared the reauthenticate request.

  Local Target Message Format: <timestamp> <seq_num> 11220 DEBUG Dynamic-Authorization: Prepared the reauthenticate request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11220 DEBUG Dynamic-Authorization: Prepared the reauthenticate request, <log details>

- **Message Code:** 11221

Severity: DEBUG

Message Text: Received a disconnect dynamic authorization ACK response

Message Description: Received a disconnect dynamic authorization ACK response.

Local Target Message Format: <timestamp> <seq_num> 11221 DEBUG Dynamic-Authorization: Received a disconnect dynamic authorization ACK response, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11221 DEBUG Dynamic-Authorization: Received a disconnect dynamic authorization ACK response, <log details>

- **Message Code:** 11222

  Severity: DEBUG

  Message Text: Received a disconnect dynamic authorization NAK response

  Message Description: Received a disconnect dynamic authorization NAK response.

  Local Target Message Format: <timestamp> <seq_num> 11222 DEBUG Dynamic-Authorization: Received a disconnect dynamic authorization NAK response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11222 DEBUG Dynamic-Authorization: Received a disconnect dynamic authorization NAK response, <log details>

- **Message Code:** 11223

  Severity: DEBUG

  Message Text: Received a dynamic authorization CoA ACK response

  Message Description: Received a dynamic authorization CoA ACK response.

  Local Target Message Format: <timestamp> <seq_num> 11223 DEBUG Dynamic-Authorization: Received a dynamic authorization CoA ACK response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11223 DEBUG Dynamic-Authorization: Received a dynamic authorization CoA ACK response, <log details>

- **Message Code:** 11224

  Severity: DEBUG

  Message Text: Received a dynamic authorization CoA NAK response

  Message Description: Received a dynamic authorization CoA NAK response.

  Local Target Message Format: <timestamp> <seq_num> 11224 DEBUG Dynamic-Authorization: Received a dynamic authorization CoA NAK response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11224 DEBUG Dynamic-Authorization: Received a dynamic authorization CoA NAK response, <log details>

- **Message Code:** 11225

  Severity: INFO

Message Text: The dynamic authorization request was rejected due to a critical logging error

Message Description: The dynamic authorization request was rejected due to a critical logging error.

Local Target Message Format: <timestamp> <seq_num> 11225 INFO Dynamic-Authorization: The dynamic authorization request was rejected due to a critical logging error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11225 INFO Dynamic-Authorization: The dynamic authorization request was rejected due to a critical logging error, <log details>

- **Message Code:** 11226

  Severity: ERROR

  Message Text: ISE Proxy Node, functioning as Dynamic Authorization Client, is deregistered from the deployment

  Message Description: ISE Proxy Node, functioning as Dynamic Authorization Client, is deregistered from the deployment.

  Local Target Message Format: <timestamp> <seq_num> 11226 ERROR Dynamic-Authorization: ISE Proxy Node, functioning as Dynamic Authorization Client, is deregistered from the deployment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11226 ERROR Dynamic-Authorization: ISE Proxy Node, functioning as Dynamic Authorization Client, is deregistered from the deployment, <log details>

- **Message Code:** 11227

  Severity: ERROR

  Message Text: ISE Proxy Node, functioning as Dynamic Authorization Client, is marked as inactive in the deployment

  Message Description: ISE Proxy Node, functioning as Dynamic Authorization Client, is marked as inactive in the deployment.

  Local Target Message Format: <timestamp> <seq_num> 11227 ERROR Dynamic-Authorization: ISE Proxy Node, functioning as Dynamic Authorization Client, is marked as inactive in the deployment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11227 ERROR Dynamic-Authorization: ISE Proxy Node, functioning as Dynamic Authorization Client, is marked as inactive in the deployment, <log details>

- **Message Code:** 11300

  Severity: WARN

  Message Text: Could not locate TrustSec Device

  Message Description: Could not find an TrustSec device using the SGA ID.

  Local Target Message Format: <timestamp> <seq_num> 11300 WARN SGA: Could not locate TrustSec Device, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11300 WARN SGA: Could not locate TrustSec Device, <log details>

- **Message Code:** 11301

  Severity: INFO

  Message Text: TrustSec Device found

  Message Description: Succeeded in locating the TrustSec device using the TrustSec ID.

  Local Target Message Format: <timestamp> <seq_num> 11301 INFO SGA: TrustSec Device found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11301 INFO SGA: TrustSec Device found, <log details>

- **Message Code:** 11302

  Severity: WARN

  Message Text: Received Secure RADIUS request without a cts-pac-opaque cisco-av-pair attribute

  Message Description: The request does not have a cisco-av-pair attribute starting with the value cts-pac-opaque. This value is a required attribute for Secure RADIUS requests.

  Local Target Message Format: <timestamp> <seq_num> 11302 WARN RADIUS: Received Secure RADIUS request without a cts-pac-opaque cisco-av-pair attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11302 WARN RADIUS: Received Secure RADIUS request without a cts-pac-opaque cisco-av-pair attribute, <log details>

- **Message Code:** 11303

  Severity: WARN

  Message Text: Could not parse the cts-pac-opaque attribute

  Message Description: The cts-pac-opaque cisco-av-pair attribute contained in the Secure RADIUS request did not parse.

  Local Target Message Format: <timestamp> <seq_num> 11303 WARN RADIUS: Could not parse the cts-pac-opaque attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11303 WARN RADIUS: Could not parse the cts-pac-opaque attribute, <log details>

- **Message Code:** 11304

  Severity: WARN

  Message Text: Could not retrieve requested Security Group Tag

  Message Description: The request for a Security Group Tag contains a non-exist value.

  Local Target Message Format: <timestamp> <seq_num> 11304 WARN SGA: Could not retrieve requested Security Group Tag, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11304 WARN SGA: Could not retrieve requested Security Group Tag, <log details>

- **Message Code:** 11305

  Severity: INFO

  Message Text: Could not retrieve requested Security Group ACL

  Message Description: The request for a Security Group ACL contains a non-exist value.

  Local Target Message Format: <timestamp> <seq_num> 11305 INFO SGA: Could not retrieve requested Security Group ACL, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11305 INFO SGA: Could not retrieve requested Security Group ACL, <log details>

- **Message Code:** 11306

  Severity: WARN

  Message Text: PAC has expired

  Message Description: The PAC received in the cts-pac-opaque RADIUS attribute has expired.

  Local Target Message Format: <timestamp> <seq_num> 11306 WARN RADIUS: PAC has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11306 WARN RADIUS: PAC has expired, <log details>

- **Message Code:** 11307

  Severity: ERROR

  Message Text: Incorrect RADIUS CHAP attribute

  Message Description: Incorrect RADIUS CHAP attribute.

  Local Target Message Format: <timestamp> <seq_num> 11307 ERROR RADIUS: Incorrect RADIUS CHAP attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11307 ERROR RADIUS: Incorrect RADIUS CHAP attribute, <log details>

- **Message Code:** 11308

  Severity: ERROR

  Message Text: Incorrect RADIUS MS-CHAP v1 attribute

  Message Description: Incorrect RADIUS MS-CHAP v1 attribute.

  Local Target Message Format: <timestamp> <seq_num> 11308 ERROR RADIUS: Incorrect RADIUS MS-CHAP v1 attribute, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11308 ERROR RADIUS: Incorrect RADIUS MS-CHAP v1 attribute, <log details>

- **Message Code:** 11309

  Severity: ERROR

  Message Text: Incorrect RADIUS MS-CHAP v2 attribute

  Message Description: Incorrect RADIUS MS-CHAP v2 attribute.

  Local Target Message Format: <timestamp> <seq_num> 11309 ERROR RADIUS: Incorrect RADIUS MS-CHAP v2 attribute, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11309 ERROR RADIUS: Incorrect RADIUS MS-CHAP v2 attribute, <log details>

- **Message Code:** 11310

  Severity: INFO

  Message Text: Sent Security Group Access Control List to client

  Message Description: Successfully sent the Security Group Access Control List to the client.

  Local Target Message Format: <timestamp> <seq_num> 11310 INFO SGA: Sent Security Group Access Control List to client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11310 INFO SGA: Sent Security Group Access Control List to client, <log details>

- **Message Code:** 11311

  Severity: INFO

  Message Text: Failed to locate ACE of Security Group Access Control List

  Message Description: Failed to locate the ACE number in the Security Group Access Control List.

  Local Target Message Format: <timestamp> <seq_num> 11311 INFO SGA: Failed to locate ACE of Security Group Access Control List, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11311 INFO SGA: Failed to locate ACE of Security Group Access Control List, <log details>

- **Message Code:** 11312

  Severity: INFO

  Message Text: Sent fragmented Security Group Access Control List data to client; awaiting follow-up request to download remaining ACEs

  Message Description: Successfully sent fragmented Security Group Access Control List data to the client.

Local Target Message Format: <timestamp> <seq_num> 11312 INFO SGA: Sent fragmented Security Group Access Control List data to client; awaiting follow-up request to download remaining ACEs, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11312 INFO SGA: Sent fragmented Security Group Access Control List data to client; awaiting follow-up request to download remaining ACEs, <log details>

- **Message Code:** 11313

  Severity: WARN

  Message Text: ISE detected that the Unknown SGT was provisioned to a network device or endpoint.

  Message Description: ISE provisioned the Unknown SGT as part of the authorization flow. Unknown SGT should not be assigned as part of a known flow

  Local Target Message Format: <timestamp> <seq_num> 11313 WARN SGA: ISE detected that the Unknown SGT was provisioned to a network device or endpoint., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11313 WARN SGA: ISE detected that the Unknown SGT was provisioned to a network device or endpoint., <log details>

- **Message Code:** 11314

  Severity: WARN

  Message Text: ISE detected a malformed TrustSec PAC.

  Message Description: ISE could not parse a TrustSec PAC recieved from device.

  Local Target Message Format: <timestamp> <seq_num> 11314 WARN SGA: ISE detected a malformed TrustSec PAC., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11314 WARN SGA: ISE detected a malformed TrustSec PAC., <log details>

- **Message Code:** 11315

  Severity: WARN

  Message Text: TrustSec environment data request failed

  Message Description: ISE recieved illigal Environment Data request

  Local Target Message Format: <timestamp> <seq_num> 11315 WARN SGA: TrustSec environment data request failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11315 WARN SGA: TrustSec environment data request failed, <log details>

- **Message Code:** 11316

  Severity: WARN

  Message Text: TrustSec CoA message ignored

Message Description: ISE sent a TrustSec CoA message and didn't receive a response. Verify network device is CoA capable. Check network device configuration

Local Target Message Format: <timestamp> <seq_num> 11316 WARN SGA: TrustSec CoA message ignored, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11316 WARN SGA: TrustSec CoA message ignored, <log details>

- **Message Code:** 11317

  Severity: WARN

  Message Text: TrustSec SSH connection failed

  Message Description: ISE failed to establish SSH connection to a network device. Verify network device SSH credentials in the Network Device page are similar to the credentials configured on the network device. Check network device enabled ssh connections from ISE (ip address)

  Local Target Message Format: <timestamp> <seq_num> 11317 WARN SGA: TrustSec SSH connection failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11317 WARN SGA: TrustSec SSH connection failed, <log details>

- **Message Code:** 11318

  Severity: WARN

  Message Text: Some TrustSec network devices don't have the latest ISE IP-SGT mapping configuration

  Message Description: ISE identified some network devices have a different IP-SGT mapping sets then ISE. Use the IP-SGT mapping Deploy option to update the devices

  Local Target Message Format: <timestamp> <seq_num> 11318 WARN SGA: Some TrustSec network devices don't have the latest ISE IP-SGT mapping configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11318 WARN SGA: Some TrustSec network devices don't have the latest ISE IP-SGT mapping configuration, <log details>

- **Message Code:** 11320

  Severity: DEBUG

  Message Text: Sent fragmented Environment data to client; awaiting follow-up request to download remaining data

  Message Description: Successfully sent fragmented Environment data to the client.

  Local Target Message Format: <timestamp> <seq_num> 11320 DEBUG SGA: Sent fragmented Environment data to client; awaiting follow-up request to download remaining data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11320 DEBUG SGA: Sent fragmented Environment data to client; awaiting follow-up request to download remaining data, <log details>

- **Message Code:** 11321

  Severity: WARN

  Message Text: TrustSec default egress policy was modified

  Message Description: The TrustSec default egress policy cell was modified, make sure it is aligned with your security policy

  Local Target Message Format: <timestamp> <seq_num> 11321 WARN SGA: TrustSec default egress policy was modified, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11321 WARN SGA: TrustSec default egress policy was modified, <log details>

- **Message Code:** 11322

  Severity: INFO

  Message Text: Trustsec egress policy was successfully downloaded

  Message Description: Trustsec egress policy was successfully downloaded

  Local Target Message Format: <timestamp> <seq_num> 11322 INFO SGA: Trustsec egress policy was successfully downloaded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11322 INFO SGA: Trustsec egress policy was successfully downloaded, <log details>

- **Message Code:** 11323

  Severity: INFO

  Message Text: Failed to download Trustsec egress policy

  Message Description: Failed to download Trustsec egress policy

  Local Target Message Format: <timestamp> <seq_num> 11323 INFO SGA: Failed to download Trustsec egress policy, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11323 INFO SGA: Failed to download Trustsec egress policy, <log details>

- **Message Code:** 11324

  Severity: WARN

  Message Text: Failed to send mail regarding workflow operation

  Message Description: Failed to send mail regarding workflow operation

  Local Target Message Format: <timestamp> <seq_num> 11324 WARN SGA: Failed to send mail regarding workflow operation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11324 WARN SGA: Failed to send mail regarding workflow operation, <log details>

- **Message Code:** 11325

  Severity: INFO

  Message Text: Trustsec security group access control list (SGACL) was successfully downloaded

  Message Description: Successfully sent Security Group Access Control List data to the client.

  Local Target Message Format: <timestamp> <seq_num> 11325 INFO SGA: Trustsec security group access control list (SGACL) was successfully downloaded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11325 INFO SGA: Trustsec security group access control list (SGACL) was successfully downloaded, <log details>

- **Message Code:** 11350

  Severity: WARN

  Message Text: Detected proxy loop; dropping request

  Message Description: ISE has detected a proxy loop, because the IP address of this ISE server is already present in the sequence of RADIUS proxy servers that have forwarded this RADIUS request. In order to avoid the senseless further forwarding of this request in an endless proxy loop, ISE has dropped this request.

  Local Target Message Format: <timestamp> <seq_num> 11350 WARN RADIUS-Proxy: Detected proxy loop; dropping request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11350 WARN RADIUS-Proxy: Detected proxy loop; dropping request, <log details>

- **Message Code:** 11351

  Severity: WARN

  Message Text: Failed to read RADIUS server sequence configuration; dropping request

  Message Description: ISE detected an error when trying to read the RADIUS server sequence configuration. Dropping the request.

  Local Target Message Format: <timestamp> <seq_num> 11351 WARN RADIUS-Proxy: Failed to read RADIUS server sequence configuration; dropping request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11351 WARN RADIUS-Proxy: Failed to read RADIUS server sequence configuration; dropping request, <log details>

- **Message Code:** 11352

  Severity: WARN

  Message Text: Response Proxy-State attribute validation failed

  Message Description: Response Proxy-State attribute must contain this ISE stamp to allow verification that the response from external RADIUS server matches the request sent to it. Verification failed. Dropping the request.

  Local Target Message Format: <timestamp> <seq_num> 11352 WARN RADIUS-Proxy: Response Proxy-State attribute validation failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11352 WARN RADIUS-Proxy: Response Proxy-State attribute validation failed, <log details>

- **Message Code:** 11353

  Severity: WARN

  Message Text: No more external RADIUS servers; can't perform failover

  Message Description: Failover is not possible because no more external RADIUS servers are configured. Dropping the request.

  Local Target Message Format: <timestamp> <seq_num> 11353 WARN RADIUS-Proxy: No more external RADIUS servers; can't perform failover, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11353 WARN RADIUS-Proxy: No more external RADIUS servers; can't perform failover, <log details>

- **Message Code:** 11354

  Severity: WARN

  Message Text: Accounting request received but neither local nor remote accounting is configured

  Message Description: An accounting request was received; however, neither local nor remote accounting is configured.

  Local Target Message Format: <timestamp> <seq_num> 11354 WARN RADIUS-Proxy: Accounting request received but neither local nor remote accounting is configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11354 WARN RADIUS-Proxy: Accounting request received but neither local nor remote accounting is configured, <log details>

- **Message Code:** 11355

  Severity: INFO

  Message Text: Start forwarding request to remote RADIUS server

  Message Description: The request is being forwarded to the next remote RADIUS server from the list configured for the selected ISE proxy service.

  Local Target Message Format: <timestamp> <seq_num> 11355 INFO RADIUS-Proxy: Start forwarding request to remote RADIUS server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11355 INFO RADIUS-Proxy: Start forwarding request to remote RADIUS server, <log details>

- **Message Code:** 11356

  Severity: WARN

  Message Text: Failed to forward request to current remote RADIUS server

Message Description: Current remote RADIUS server has failed to process the forwarded request due to any of the following reasons: The remote RADIUS server is down ; The remote RADIUS server is not configured properly ; The remote RADIUS server dropped the request.

Local Target Message Format: <timestamp> <seq_num> 11356 WARN RADIUS-Proxy: Failed to forward request to current remote RADIUS server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11356 WARN RADIUS-Proxy: Failed to forward request to current remote RADIUS server, <log details>

- **Message Code:** 11357

  Severity: INFO

  Message Text: Successfully forwarded request to current remote RADIUS server

  Message Description: Current remote RADIUS server successfully processed the forwarded request and replied with a valid response, which is being forwarded back to the NAS.

  Local Target Message Format: <timestamp> <seq_num> 11357 INFO RADIUS-Proxy: Successfully forwarded request to current remote RADIUS server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11357 INFO RADIUS-Proxy: Successfully forwarded request to current remote RADIUS server, <log details>

- **Message Code:** 11358

  Severity: INFO

  Message Text: Received request for RADIUS server sequence.

  Message Description: The RADIUS server sequence has received an incoming request. Validating the request and preparing to forward it to a configured external RADIUS server.

  Local Target Message Format: <timestamp> <seq_num> 11358 INFO RADIUS-Proxy: Received request for RADIUS server sequence., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11358 INFO RADIUS-Proxy: Received request for RADIUS server sequence., <log details>

- **Message Code:** 11359

  Severity: INFO

  Message Text: Failed to forward request to current remote RADIUS server; an invalid response was received

  Message Description: The current remote RADIUS server has replied with an invalid response that would be forwarded to the next remote RADIUS server, if available.

  Local Target Message Format: <timestamp> <seq_num> 11359 INFO RADIUS-Proxy: Failed to forward request to current remote RADIUS server; an invalid response was received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11359 INFO RADIUS-Proxy: Failed to forward request to current remote RADIUS server; an invalid response was received, <log details>

- **Message Code:** 11360

  Severity: WARN

  Message Text: RADIUS server sequence failed to validate incoming request

  Message Description: RADIUS server sequence failed to validate the incoming request.

  Local Target Message Format: <timestamp> <seq_num> 11360 WARN RADIUS-Proxy: RADIUS server sequence failed to validate incoming request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11360 WARN RADIUS-Proxy: RADIUS server sequence failed to validate incoming request, <log details>

- **Message Code:** 11361

  Severity: INFO

  Message Text: Valid incoming authentication request

  Message Description: The RADIUS server sequence has received a valid incoming authentication request.

  Local Target Message Format: <timestamp> <seq_num> 11361 INFO RADIUS-Proxy: Valid incoming authentication request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11361 INFO RADIUS-Proxy: Valid incoming authentication request, <log details>

- **Message Code:** 11362

  Severity: INFO

  Message Text: Valid incoming accounting request

  Message Description: The RADIUS server sequence has received a valid incoming accounting request.

  Local Target Message Format: <timestamp> <seq_num> 11362 INFO RADIUS-Proxy: Valid incoming accounting request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11362 INFO RADIUS-Proxy: Valid incoming accounting request, <log details>

- **Message Code:** 11363

  Severity: INFO

  Message Text: RADIUS server sequence performing local accounting

  Message Description: The RADIUS server sequence is performing a local accounting based on the incoming accounting request received.

  Local Target Message Format: <timestamp> <seq_num> 11363 INFO RADIUS-Proxy: RADIUS server sequence performing local accounting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11363 INFO RADIUS-Proxy: RADIUS server sequence performing local accounting, <log details>

- **Message Code:** 11364

  Severity: INFO

  Message Text: RADIUS server sequence performing remote accounting

  Message Description: The RADIUS server sequence is performing a remote accounting based on the incoming accounting request received.

  Local Target Message Format: <timestamp> <seq_num> 11364 INFO RADIUS-Proxy: RADIUS server sequence performing remote accounting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11364 INFO RADIUS-Proxy: RADIUS server sequence performing remote accounting, <log details>

- **Message Code:** 11365

  Severity: INFO

  Message Text: Modify attributes before sending request to external radius server

  Message Description: The RADIUS server sequence is modifing attributes before sending request to external radius server

  Local Target Message Format: <timestamp> <seq_num> 11365 INFO RADIUS-Proxy: Modify attributes before sending request to external radius server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11365 INFO RADIUS-Proxy: Modify attributes before sending request to external radius server, <log details>

- **Message Code:** 11366

  Severity: INFO

  Message Text: Modify attributes before sending RADIUS Access-Accept

  Message Description: The RADIUS server sequence is modify attributes before sending RADIUS-accept.

  Local Target Message Format: <timestamp> <seq_num> 11366 INFO RADIUS-Proxy: Modify attributes before sending RADIUS Access-Accept, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11366 INFO RADIUS-Proxy: Modify attributes before sending RADIUS Access-Accept, <log details>

- **Message Code:** 11367

  Severity: INFO

  Message Text: Could not add attribute(s) since attribute already exist

  Message Description: Could not add attribute(s) to the request since attribute already exist and the attribute is not multiple allowed.

  Local Target Message Format: <timestamp> <seq_num> 11367 INFO RADIUS-Proxy: Could not add attribute(s) since attribute already exist, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11367 INFO RADIUS-Proxy: Could not add attribute(s) since attribute already exist, <log details>

- **Message Code:** 11368

  Severity: DEBUG

  Message Text: Please review logs on the External RADIUS Server to determine the precise failure reason.

  Message Description: Please review logs on the External RADIUS Server to determine the precise failure reason.

  Local Target Message Format: <timestamp> <seq_num> 11368 DEBUG RADIUS-Proxy: Please review logs on the External RADIUS Server to determine the precise failure reason., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11368 DEBUG RADIUS-Proxy: Please review logs on the External RADIUS Server to determine the precise failure reason., <log details>

- **Message Code:** 11369

  Severity: WARN

  Message Text: Proxy request was rejected, as the external RADIUS server that handled previous related EAP messages is now down

  Message Description: ISE received an RADIUS proxy request but the external RADIUS server that handled previous related EAP messages is now down. Without the context of the previous EAP messages, there is no point in sending this request to another external RADIUS server

  Local Target Message Format: <timestamp> <seq_num> 11369 WARN RADIUS-Proxy: Proxy request was rejected, as the external RADIUS server that handled previous related EAP messages is now down, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11369 WARN RADIUS-Proxy: Proxy request was rejected, as the external RADIUS server that handled previous related EAP messages is now down, <log details>

- **Message Code:** 11400

  Severity: WARN

  Message Text: EAP-MSCHAP password change not allowed by the Allowed Protocols

  Message Description: The attempt to change the password failed because password change for the MS-CHAPv2 inner method is disabled in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 11400 WARN EAP: EAP-MSCHAP password change not allowed by the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11400 WARN EAP: EAP-MSCHAP password change not allowed by the Allowed Protocols, <log details>

- **Message Code:** 11401

Severity: INFO

Message Text: Prepared RADIUS Access-Reject after the successful in-band PAC provisioning

Message Description: As part of the standard in-band PAC provisioning behavior, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC request was successfully approved. This admittedly-misleading result value is nevertheless normal, does not truly imply a failure, and can/should be safely ignored. (Most likely, the ISE logs will show a subsequent EAP-FAST conversation for this user attempting to actually authenticate using the PAC that was currently provisioned.)

Local Target Message Format: <timestamp> <seq_num> 11401 INFO EAP: Prepared RADIUS Access-Reject after the successful in-band PAC provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11401 INFO EAP: Prepared RADIUS Access-Reject after the successful in-band PAC provisioning, <log details>

- **Message Code:** 11402

  Severity: WARN

  Message Text: EAP-GTC password change not allowed by the Allowed Protocols

  Message Description: The attempt to change the password failed because the relevant Allowed Protocols does not allow password change for the EAP-GTC inner method.

  Local Target Message Format: <timestamp> <seq_num> 11402 WARN EAP: EAP-GTC password change not allowed by the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11402 WARN EAP: EAP-GTC password change not allowed by the Allowed Protocols, <log details>

- **Message Code:** 11500

  Severity: WARN

  Message Text: Invalid or unexpected EAP payload received

  Message Description: Internal error, possibly in the supplicant: Could not validate an EAP payload.

  Local Target Message Format: <timestamp> <seq_num> 11500 WARN EAP: Invalid or unexpected EAP payload received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11500 WARN EAP: Invalid or unexpected EAP payload received, <log details>

- **Message Code:** 11501

  Severity: WARN

  Message Text: Invalid EAP payload

  Message Description: Internal error, possibly in the supplicant: Could not validate an EAP payload.

  Local Target Message Format: <timestamp> <seq_num> 11501 WARN EAP: Invalid EAP payload, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11501 WARN EAP: Invalid EAP payload, <log details>

- **Message Code:** 11502

  Severity: WARN

  Message Text: EAP packet contains invalid type

  Message Description: Internal error, possibly in the supplicant: The EAP packet contains an invalid EAP type; Could not find a corresponding protocol handler.

  Local Target Message Format: <timestamp> <seq_num> 11502 WARN EAP: EAP packet contains invalid type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11502 WARN EAP: EAP packet contains invalid type, <log details>

- **Message Code:** 11503

  Severity: INFO

  Message Text: Prepared EAP-Success

  Message Description: Created an EAP-Success packet, to be attached to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11503 INFO EAP: Prepared EAP-Success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11503 INFO EAP: Prepared EAP-Success, <log details>

- **Message Code:** 11504

  Severity: INFO

  Message Text: Prepared EAP-Failure

  Message Description: Created an EAP-Failure packet, to be attached to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11504 INFO EAP: Prepared EAP-Failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11504 INFO EAP: Prepared EAP-Failure, <log details>

- **Message Code:** 11506

  Severity: INFO

  Message Text: Prepared EAP-Request/Identity

  Message Description: Created an EAP-Request/Identity packet, to be attached to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11506 INFO EAP: Prepared EAP-Request/Identity, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11506 INFO EAP: Prepared EAP-Request/Identity, <log details>

- **Message Code:** 11507

  Severity: INFO

  Message Text: Extracted EAP-Response/Identity

  Message Description: Extracted an EAP-Response/Identity packet from the RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11507 INFO EAP: Extracted EAP-Response/Identity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11507 INFO EAP: Extracted EAP-Response/Identity, <log details>

- **Message Code:** 11508

  Severity: WARN

  Message Text: EAP-Response/Identity contains invalid identity data

  Message Description: As part of fallback processing due to an invalid PAC, the inner method extracted an EAP-Response/Identity packet. Since this packet's identity data does not match the originally received identity, it is considered as invalid.

  Local Target Message Format: <timestamp> <seq_num> 11508 WARN EAP: EAP-Response/Identity contains invalid identity data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11508 WARN EAP: EAP-Response/Identity contains invalid identity data, <log details>

- **Message Code:** 11509

  Severity: WARN

  Message Text: Allowed Protocols does not allow any EAP protocols

  Message Description: EAP-negotiation failed because the Allowed Protocols has no EAP-based protocols enabled.

  Local Target Message Format: <timestamp> <seq_num> 11509 WARN EAP: Allowed Protocols does not allow any EAP protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11509 WARN EAP: Allowed Protocols does not allow any EAP protocols, <log details>

- **Message Code:** 11510

  Severity: WARN

  Message Text: Supplicant declined EAP method selected by Authentication Policy but did not propose another one; EAP negotiation failed

Message Description: In previous EAP message ISE started an EAP method selected by Authentication Policy. Supplicant declined this EAP method by sending EAP NAK message but did not propose another EAP method that it is ready to conduct. Owing to this, EAP-negotiation failed.

Local Target Message Format: <timestamp> <seq_num> 11510 WARN EAP: Supplicant declined EAP method selected by Authentication Policy but did not propose another one; EAP negotiation failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11510 WARN EAP: Supplicant declined EAP method selected by Authentication Policy but did not propose another one; EAP negotiation failed, <log details>

- **Message Code:** 11511

  Severity: WARN

  Message Text: Extracted EAP-Response/NAK packet not requesting any EAP protocols; EAP-negotiation failed

  Message Description: An invalid EAP-Response/NAK packet was extracted from the RADIUS message. This packet rejected the EAP-based protocol that was proposed earlier. However, it is not requesting any other protocols, based on the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 11511 WARN EAP: Extracted EAP-Response/NAK packet not requesting any EAP protocols; EAP-negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11511 WARN EAP: Extracted EAP-Response/NAK packet not requesting any EAP protocols; EAP-negotiation failed, <log details>

- **Message Code:** 11512

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK packet requesting to use unsupported EAP protocol; EAP-negotiation failed

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use another protocol instead, per the configuration of the client's supplicant. However, the requested EAP-based protocol is currently not supported by ISE.

  Local Target Message Format: <timestamp> <seq_num> 11512 INFO EAP: Extracted EAP-Response/NAK packet requesting to use unsupported EAP protocol; EAP-negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11512 INFO EAP: Extracted EAP-Response/NAK packet requesting to use unsupported EAP protocol; EAP-negotiation failed, <log details>

- **Message Code:** 11513

  Severity: WARN

  Message Text: Extracted second EAP-Response/NAK in current EAP conversation; failed to negotiate EAP

Message Description: For the second time in the current EAP conversation, extracted from the RADIUS message an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol.

Local Target Message Format: <timestamp> <seq_num> 11513 WARN EAP: Extracted second EAP-Response/NAK in current EAP conversation; failed to negotiate EAP, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11513 WARN EAP: Extracted second EAP-Response/NAK in current EAP conversation; failed to negotiate EAP, <log details>

- **Message Code:** 11514

  Severity: WARN

  Message Text: Unexpectedly received empty TLS message; treating as a rejection by the client

  Message Description: While trying to negotiate a TLS handshake with the client, ISE expected to receive a non-empty TLS message or TLS alert message, but instead received an empty TLS message. This could be due to an inconformity in the implementation of the protocol between ISE and the supplicant. For example, it is a known issue that the XP supplicant sends an empty TLS message instead of a non-empty TLS alert message. It might also involve the supplicant not trusting the ISE server certificate for some reason. ISE treated the unexpected message as a sign that the client rejected the tunnel establishment.

  Local Target Message Format: <timestamp> <seq_num> 11514 WARN EAP: Unexpectedly received empty TLS message; treating as a rejection by the client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11514 WARN EAP: Unexpectedly received empty TLS message; treating as a rejection by the client, <log details>

- **Message Code:** 11515

  Severity: WARN

  Message Text: Supplicant declined inner EAP method selected by Authentication Policy but did not proposed another one; inner EAP negotiation failed

  Message Description: In previous inner EAP message ISE started an inner EAP method selected by Authentication Policy. Supplicant declined this inner EAP method by sending inner EAP NAK message but did not proposed another inner EAP method that it is ready to conduct. Owing to this, inner EAP negotiation failed.

  Local Target Message Format: <timestamp> <seq_num> 11515 WARN EAP: Supplicant declined inner EAP method selected by Authentication Policy but did not proposed another one; inner EAP negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11515 WARN EAP: Supplicant declined inner EAP method selected by Authentication Policy but did not proposed another one; inner EAP negotiation failed, <log details>

- **Message Code:** 11516

  Severity: WARN

  Message Text: Extracted EAP-Response/NAK packet not requesting any EAP protocols for inner EAP method; inner EAP-negotiation failed

Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner EAP method, but -- per the configuration of the client's supplicant -- not requesting any other protocols. Negotiation of the inner EAP method failed.

Local Target Message Format: <timestamp> <seq_num> 11516 WARN EAP: Extracted EAP-Response/NAK packet not requesting any EAP protocols for inner EAP method; inner EAP-negotiation failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11516 WARN EAP: Extracted EAP-Response/NAK packet not requesting any EAP protocols for inner EAP method; inner EAP-negotiation failed, <log details>

- **Message Code:** 11517

  Severity: WARN

  Message Text: Extracted EAP-Response/NAK packet requesting to use unsupported inner EAP protocol; inner EAP-negotiation failed

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner EAP method, and requesting to use another protocol instead, per the configuration of the client's supplicant. However, the requested inner EAP-based protocol is currently not supported by ISE. Negotiation of the inner EAP method failed.

  Local Target Message Format: <timestamp> <seq_num> 11517 WARN EAP: Extracted EAP-Response/NAK packet requesting to use unsupported inner EAP protocol; inner EAP-negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11517 WARN EAP: Extracted EAP-Response/NAK packet requesting to use unsupported inner EAP protocol; inner EAP-negotiation failed, <log details>

- **Message Code:** 11518

  Severity: WARN

  Message Text: Extracted second EAP-Response/NAK in current inner EAP conversation; inner EAP-negotiation failed

  Message Description: For the second time in the current inner EAP conversation, extracted from the EAP-Response packet in the outer EAP method an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner EAP method. Negotiation of the inner EAP method failed.

  Local Target Message Format: <timestamp> <seq_num> 11518 WARN EAP: Extracted second EAP-Response/NAK in current inner EAP conversation; inner EAP-negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11518 WARN EAP: Extracted second EAP-Response/NAK in current inner EAP conversation; inner EAP-negotiation failed, <log details>

- **Message Code:** 11519

  Severity: INFO

Message Text: Prepared EAP-Success for inner EAP method

Message Description: Created an EAP-Success packet, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

Local Target Message Format: <timestamp> <seq_num> 11519 INFO EAP: Prepared EAP-Success for inner EAP method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11519 INFO EAP: Prepared EAP-Success for inner EAP method, <log details>

- **Message Code:** 11520

  Severity: INFO

  Message Text: Prepared EAP-Failure for inner EAP method

  Message Description: Created an EAP-Failure packet, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11520 INFO EAP: Prepared EAP-Failure for inner EAP method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11520 INFO EAP: Prepared EAP-Failure for inner EAP method, <log details>

- **Message Code:** 11521

  Severity: INFO

  Message Text: Prepared EAP-Request/Identity for inner EAP method

  Message Description: Created an EAP-Request/Identity packet, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11521 INFO EAP: Prepared EAP-Request/Identity for inner EAP method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11521 INFO EAP: Prepared EAP-Request/Identity for inner EAP method, <log details>

- **Message Code:** 11522

  Severity: INFO

  Message Text: Extracted EAP-Response/Identity for inner EAP method

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/Identity packet for the inner EAP method.

  Local Target Message Format: <timestamp> <seq_num> 11522 INFO EAP: Extracted EAP-Response/Identity for inner EAP method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11522 INFO EAP: Extracted EAP-Response/Identity for inner EAP method, <log details>

- **Message Code:** 11523

  Severity: WARN

  Message Text: Invalid or unexpected inner-EAP payload received

  Message Description: Internal error, possibly in the supplicant: failed to validate an EAP inner-method payload.

  Local Target Message Format: <timestamp> <seq_num> 11523 WARN EAP: Invalid or unexpected inner-EAP payload received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11523 WARN EAP: Invalid or unexpected inner-EAP payload received, <log details>

- **Message Code:** 11524

  Severity: WARN

  Message Text: Invalid inner-EAP payload

  Message Description: Internal error, possibly in the supplicant: failed to validate an EAP inner-method payload.

  Local Target Message Format: <timestamp> <seq_num> 11524 WARN EAP: Invalid inner-EAP payload, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11524 WARN EAP: Invalid inner-EAP payload, <log details>

- **Message Code:** 11800

  Severity: INFO

  Message Text: Prepared EAP-Request proposing EAP-MSCHAP with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-MSCHAP protocol, and also providing an MSCHAP challenge, for attachment to a RADIUS message. The EAP-MSCHAP protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 11800 INFO EAP: Prepared EAP-Request proposing EAP-MSCHAP with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11800 INFO EAP: Prepared EAP-Request proposing EAP-MSCHAP with challenge, <log details>

- **Message Code:** 11801

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use EAP-MSCHAP instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-MSCHAP instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 11801 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-MSCHAP instead, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11801 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-MSCHAP instead, <log details>

- **Message Code:** 11802

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-MSCHAP challenge-response and accepting EAP-MSCHAP as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing an EAP-MSCHAP challenge-response, and accepting EAP-MSCHAP as negotiated.

  Local Target Message Format: <timestamp> <seq_num> 11802 INFO EAP: Extracted EAP-Response containing EAP-MSCHAP challenge-response and accepting EAP-MSCHAP as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11802 INFO EAP: Extracted EAP-Response containing EAP-MSCHAP challenge-response and accepting EAP-MSCHAP as negotiated, <log details>

- **Message Code:** 11803

  Severity: WARN

  Message Text: Failed to negotiate EAP because EAP-MSCHAP not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-MSCHAP instead. However, EAP-MSCHAP is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 11803 WARN EAP: Failed to negotiate EAP because EAP-MSCHAP not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11803 WARN EAP: Failed to negotiate EAP because EAP-MSCHAP not allowed in the Allowed Protocols, <log details>

- **Message Code:** 11804

  Severity: INFO

  Message Text: Extracted EAP-Response containing MSCHAP challenge-response

  Message Description: Continuing the EAP-MSCHAP protocol; processing the EAP-MSCHAP challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 11804 INFO EAP: Extracted EAP-Response containing MSCHAP challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11804 INFO EAP: Extracted EAP-Response containing MSCHAP challenge-response, <log details>

- **Message Code:** 11805

  Severity: INFO

  Message Text: Prepared EAP-Request with another EAP-MSCHAP challenge

Message Description: As part of the continuation of the EAP-MSCHAP protocol, created an EAP-Request packet containing another EAP-MSCHAP challenge, for attachment to a RADIUS message.

Local Target Message Format: <timestamp> <seq_num> 11805 INFO EAP: Prepared EAP-Request with another EAP-MSCHAP challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11805 INFO EAP: Prepared EAP-Request with another EAP-MSCHAP challenge, <log details>

- **Message Code:** 11806

  Severity: INFO

  Message Text: Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-MSCHAP protocol for the inner method, and also providing an MSCHAP challenge, for attachment to a RADIUS message. The EAP-MSCHAP protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 11806 INFO EAP: Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11806 INFO EAP: Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge, <log details>

- **Message Code:** 11807

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK for inner method requesting to use EAP-MSCHAP instead

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/NAK packet, rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-MSCHAP instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 11807 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-MSCHAP instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11807 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-MSCHAP instead, <log details>

- **Message Code:** 11808

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response packet containing an EAP-MSCHAP challenge-response, and accepting EAP-MSCHAP as negotiated for the inner method.

  Local Target Message Format: <timestamp> <seq_num> 11808 INFO EAP: Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11808 INFO EAP: Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated, <log details>

- **Message Code:** 11809

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-MSCHAPv2 not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-MSCHAPv2 instead. However, EAP-MSCHAPv2 is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 11809 WARN EAP: Failed to negotiate EAP for inner method because EAP-MSCHAPv2 not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11809 WARN EAP: Failed to negotiate EAP for inner method because EAP-MSCHAPv2 not allowed in the Allowed Protocols, <log details>

- **Message Code:** 11810

  Severity: INFO

  Message Text: Extracted EAP-Response for inner method containing MSCHAP challenge-response

  Message Description: Continuing the inner EAP-MSCHAP protocol; processing the EAP-MSCHAP challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 11810 INFO EAP: Extracted EAP-Response for inner method containing MSCHAP challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11810 INFO EAP: Extracted EAP-Response for inner method containing MSCHAP challenge-response, <log details>

- **Message Code:** 11811

  Severity: INFO

  Message Text: Prepared EAP-Request for inner method with another EAP-MSCHAP challenge

  Message Description: As part of the continuation of the inner EAP-MSCHAP protocol, created an EAP-Request packet containing another EAP-MSCHAP challenge, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 11811 INFO EAP: Prepared EAP-Request for inner method with another EAP-MSCHAP challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11811 INFO EAP: Prepared EAP-Request for inner method with another EAP-MSCHAP challenge, <log details>

- **Message Code:** 11812

Severity: INFO

Message Text: EAP-MSCHAP authentication succeeded

Message Description: EAP-MSCHAP authentication succeeded.

Local Target Message Format: <timestamp> <seq_num> 11812 INFO EAP: EAP-MSCHAP authentication succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11812 INFO EAP: EAP-MSCHAP authentication succeeded, <log details>

- **Message Code:** 11813

  Severity: INFO

  Message Text: EAP-MSCHAP authentication failed

  Message Description: EAP-MSCHAP authentication failed.

  Local Target Message Format: <timestamp> <seq_num> 11813 INFO EAP: EAP-MSCHAP authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11813 INFO EAP: EAP-MSCHAP authentication failed, <log details>

- **Message Code:** 11814

  Severity: INFO

  Message Text: Inner EAP-MSCHAP authentication succeeded

  Message Description: EAP-MSCHAP authentication for the inner EAP method succeeded.

  Local Target Message Format: <timestamp> <seq_num> 11814 INFO EAP: Inner EAP-MSCHAP authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11814 INFO EAP: Inner EAP-MSCHAP authentication succeeded, <log details>

- **Message Code:** 11815

  Severity: INFO

  Message Text: Inner EAP-MSCHAP authentication failed

  Message Description: EAP-MSCHAP authentication for the inner EAP method failed.

  Local Target Message Format: <timestamp> <seq_num> 11815 INFO EAP: Inner EAP-MSCHAP authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11815 INFO EAP: Inner EAP-MSCHAP authentication failed, <log details>

- **Message Code:** 11816

  Severity: WARN

Message Text: MSCHAP username doesn't match inner method EAP-Response/Identity

Message Description: The MSCHAP username does not match the username received in the inner method EAP-Response/Identity packet. One possible reason might be that the client's supplicant is preconfigured with another username not matching that entered by the user.

Local Target Message Format: <timestamp> <seq_num> 11816 WARN EAP: MSCHAP username doesn't match inner method EAP-Response/Identity, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11816 WARN EAP: MSCHAP username doesn't match inner method EAP-Response/Identity, <log details>

- **Message Code:** 11817

  Severity: WARN

  Message Text: Received unexpected EAP-MSCHAP message

  Message Description: ISE was expecting certain EAP-MSCHAP message, but received another one. This could be due to a possible inconformity in the implementation of the protocol between ISE and the supplicant.

  Local Target Message Format: <timestamp> <seq_num> 11817 WARN EAP: Received unexpected EAP-MSCHAP message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11817 WARN EAP: Received unexpected EAP-MSCHAP message, <log details>

- **Message Code:** 11818

  Severity: INFO

  Message Text: Failed to parse EAP-MSCHAP packet

  Message Description: Failed to parse EAP-MSCHAP packet.

  Local Target Message Format: <timestamp> <seq_num> 11818 INFO EAP: Failed to parse EAP-MSCHAP packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11818 INFO EAP: Failed to parse EAP-MSCHAP packet, <log details>

- **Message Code:** 11819

  Severity: INFO

  Message Text: Received EAP-MSCHAP packet with invalid argument

  Message Description: Received EAP-MSCHAP packet with invalid argument.

  Local Target Message Format: <timestamp> <seq_num> 11819 INFO EAP: Received EAP-MSCHAP packet with invalid argument, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11819 INFO EAP: Received EAP-MSCHAP packet with invalid argument, <log details>

- **Message Code:** 11821

  Severity: INFO

  Message Text: EAP-MSCHAP password change attempt failed

  Message Description: The attempt to change the password failed because password change for the MS-CHAPv2 inner method is not enabled in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 11821 INFO EAP: EAP-MSCHAP password change attempt failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11821 INFO EAP: EAP-MSCHAP password change attempt failed, <log details>

- **Message Code:** 11822

  Severity: DEBUG

  Message Text: EAP-MSCHAP password change attempt passed

  Message Description: The attempt to change the EAP-MSCHAP password passed.

  Local Target Message Format: <timestamp> <seq_num> 11822 DEBUG EAP: EAP-MSCHAP password change attempt passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11822 DEBUG EAP: EAP-MSCHAP password change attempt passed, <log details>

- **Message Code:** 11823

  Severity: INFO

  Message Text: EAP-MSCHAP authentication attempt failed

  Message Description: EAP-MSCHAP authentication attempt failed.

  Local Target Message Format: <timestamp> <seq_num> 11823 INFO EAP: EAP-MSCHAP authentication attempt failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11823 INFO EAP: EAP-MSCHAP authentication attempt failed, <log details>

- **Message Code:** 11824

  Severity: DEBUG

  Message Text: EAP-MSCHAP authentication attempt passed

  Message Description: EAP-MSCHAP authentication attempt passed.

  Local Target Message Format: <timestamp> <seq_num> 11824 DEBUG EAP: EAP-MSCHAP authentication attempt passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11824 DEBUG EAP: EAP-MSCHAP authentication attempt passed, <log details>

- **Message Code:** 11825

  Severity: WARN

  Message Text: MSCHAP inner method username is missing

  Message Description: The username received in the inner method EAP-Response/Identity packet was empty. One possible reason might be that the user did not enter a username.

  Local Target Message Format: <timestamp> <seq_num> 11825 WARN EAP: MSCHAP inner method username is missing, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 11825 WARN EAP: MSCHAP inner method username is missing, <log details>

- **Message Code:** 11525

  Severity: INFO

  Message Text: Sent NDAC Authentication to client

  Message Description: Sent NDAC Authentication to client.

  Local Target Message Format: <timestamp> <seq_num>11525 INFO EAP Sent NDAC Authentication to client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11525 INFO EAP Sent NDAC Authentication to client, <log details>

- **Message Code:** 11526

  Severity: INFO

  Message Text: Received NDAC Authentication response from client

  Message Description: Received NDAC Authentication response from client.

  Local Target Message Format: <timestamp> <seq_num>11526 INFO EAP Received NDAC Authentication response from client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11526 INFO EAP Received NDAC Authentication response from client, <log details>

- **Message Code:** 11527

  Severity: INFO

  Message Text: Successfully finished TEAP tunnel PAC provisioning/update

  Message Description: Successfully finished the TEAP tunnel PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num>11527 INFO EAP Successfully finished TEAP tunnel PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11527 INFO EAP Successfully finished TEAP tunnel PAC provisioning/update, <log details>

- **Message Code:** 11528

  Severity: INFO

  Message Text: Successfully finished TEAP machine PAC provisioning/update

  Message Description: Successfully finished the TEAP machine PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num>11528 INFO EAP Successfully finished TEAP machine PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11528 INFO EAP Successfully finished TEAP machine PAC provisioning/update, <log details>

- **Message Code:** 11529

  Severity: INFO

  Message Text: Successfully finished TEAP user authorization PAC provisioning/update

  Message Description: Successfully finished the TEAP user authorization PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num>11529 INFO EAP Successfully finished TEAP user authorization PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11529 INFO EAP Successfully finished TEAP user authorization PAC provisioning/update, <log details>

- **Message Code:** 11530

  Severity: INFO

  Message Text: Successfully finished TEAP machine authorization PAC provisioning/update

  Message Description: Successfully finished the TEAP machine authorization PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num>11530 INFO EAP Successfully finished TEAP machine authorization PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11530 INFO EAP Successfully finished TEAP machine authorization PAC provisioning/update, <log details>

- **Message Code:** 11531

  Severity: INFO

  Message Text: Successfully finished TEAP CTS PAC provisioning/update

  Message Description: Successfully finished the TEAP CTS PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num>11531 INFO EAP Successfully finished TEAP CTS PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11531 INFO EAP Successfully finished TEAP CTS PAC provisioning/update, <log details>

- **Message Code:** 11532

  Severity: INFO

  Message Text: Successfully finished TEAP posture PAC provisioning/update

  Message Description: Successfully finished the TEAP posture PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num>11532 INFO EAP Successfully finished TEAP posture PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11532 INFO EAP Successfully finished TEAP posture PAC provisioning/update, <log details>

- **Message Code:** 11533

  Severity: INFO

  Message Text: Successfully finished TEAP PAC provisioning/update

  Message Description: Successfully finished TEAP PAC provisioning/update.

  Local Target Message Format: <timestamp> <seq_num>11533 INFO EAP Successfully finished TEAP PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11533 INFO EAP Successfully finished TEAP PAC provisioning/update, <log details>

- **Message Code:** 11534

  Severity: WARN

  Message Text: One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Message Description: One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num>11534 WARN EAP One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11534 WARN EAP One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

- **Message Code:** 11535

  Severity: WARN

  Message Text: One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Message Description: One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num>11535 WARN EAP One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11535 WARN EAP One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

- **Message Code:** 11536

  Severity: WARN

  Message Text: One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Message Description: One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num>11536 WARN EAP One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11536 WARN EAP One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

- **Message Code:** 11537

  Severity: WARN

  Message Text: One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Message Description: One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num>11537 WARN EAP One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11537 WARN EAP One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

- **Message Code:** 11538

  Severity: WARN

  Message Text: One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored

  Message Description: One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num>11538 WARN EAP One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11538 WARN EAP One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored, <log details>

- **Message Code:** 11539

  Severity: WARN

  Message Text: One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored

  Message Description: One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num>11539 WARN EAP One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11539 WARN EAP One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored, <log details>

- **Message Code:** 11540

  Severity: WARN

  Message Text: Invalid PAC type requested. Ignoring this request

  Message Description: Invalid PAC type requested. Ignoring this request

  Local Target Message Format: <timestamp> <seq_num>11540 WARN EAP Invalid PAC type requested. Ignoring this request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11540 WARN EAP Invalid PAC type requested. Ignoring this request, <log details>

- **Message Code:** 11541

  Severity: INFO

  Message Text: Ignore PAC send by supplicant during fallback to provisioning conversation

  Message Description: ISE performed fallback on invalid PAC to provisioning. However during this provisioning conversation supplicant sent the PAC again. ISE will ignore this PAC.

  Local Target Message Format: <timestamp> <seq_num>11541 INFO EAP Ignore PAC send by supplicant during fallback to provisioning conversation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11541 INFO EAP Ignore PAC send by supplicant during fallback to provisioning conversation, <log details>

- **Message Code:** 11542

  Severity: INFO

  Message Text: User Authorization PAC request ignored because PAC of the same type was already used to skip inner method

  Message Description: User Authorization PAC request ignored because PAC of the same type was already used to skip inner method. Authorization PAC could be provided only after full authentication conversation.

Local Target Message Format: <timestamp> <seq_num>11542 INFO EAP User Authorization PAC request ignored because PAC of the same type was already used to skip inner method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11542 INFO EAP User Authorization PAC request ignored because PAC of the same type was already used to skip inner method, <log details>

- **Message Code:** 11543

  Severity: INFO

  Message Text: Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method

  Message Description: Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method. Authorization PAC could be provided only after full authentication conversation.

  Local Target Message Format: <timestamp> <seq_num>11543 INFO EAP Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11543 INFO EAP Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method, <log details>

- **Message Code:** 11544

  Severity: INFO

  Message Text: Ignore Machine Authorization PAC request when there is no EAP chaining

  Message Description: ISE ignores Machine Authorization PAC request when there is no EAP chaining happens in the conversation. Machine Authorization PAC can be provided only during EAP chaining conversation. Note that EAP chaining can be configured in ISE but disabled or not supported in client so the conversation was conducted in no chaining mode.

  Local Target Message Format: <timestamp> <seq_num>11544 INFO EAP Ignore Machine Authorization PAC request when there is no EAP chaining, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11544 INFO EAP Ignore Machine Authorization PAC request when there is no EAP chaining, <log details>

- **Message Code:** 11545

  Severity: WARN

  Message Text: Machine Authentication is disabled

  Message Description: TEAP authentication failed because Machine Authentication is disabled.

  Local Target Message Format: <timestamp> <seq_num>11545 WARN EAP Machine Authentication is disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11545 WARN EAP Machine Authentication is disabled, <log details>

- **Message Code:** 11546

  Severity: INFO

  Message Text: Allowed Protocols does not allow Stateless Session Resume; performing full authentication

  Message Description: Allowed Protocols configuration does not allow Stateless Session Resume; performing full authentication.

  Local Target Message Format: <timestamp> <seq_num>11546 INFO EAP Allowed Protocols does not allow Stateless Session Resume; performing full authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11546 INFO EAP Allowed Protocols does not allow Stateless Session Resume; performing full authentication, <log details>

- **Message Code:** 11547

  Severity: WARN

  Message Text: Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning

  Message Description: Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning

  Local Target Message Format: <timestamp> <seq_num>11547 WARN EAP Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11547 WARN EAP Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning, <log details>

- **Message Code:** 11548

  Severity: WARN

  Message Text: Cannot provision Authorization PAC when the stateless session resume is disabled

  Message Description: Cannot provision Authorization PAC when the stateless session resume is disabled. Enable the stateless session resume in service settings to allow Authorization PAC provisioning

  Local Target Message Format: <timestamp> <seq_num>11548 WARN EAP Cannot provision Authorization PAC when the stateless session resume is disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11548 WARN EAP Cannot provision Authorization PAC when the stateless session resume is disabled, <log details>

- **Message Code:** 11549

  Severity: WARN

  Message Text: Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning

  Message Description: Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning

Local Target Message Format: <timestamp> <seq_num>11549 WARN EAP Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11549 WARN EAP Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning, <log details>

- **Message Code:** 11550

  Severity: WARN

  Message Text: Authorization PAC can be provided only with Tunnel PAC

  Message Description: Authorization PAC can be provided only with Tunnel PAC

  Local Target Message Format: <timestamp> <seq_num>11550 WARN EAP Authorization PAC can be provided only with Tunnel PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11550 WARN EAP Authorization PAC can be provided only with Tunnel PAC, <log details>

- **Message Code:** 11551

  Severity: WARN

  Message Text: Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request

  Message Description: Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request

  Local Target Message Format: <timestamp> <seq_num>11551 WARN EAP Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11551 WARN EAP Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request, <log details>

- **Message Code:** 11552

  Severity: WARN

  Message Text: Machine PAC request does not contain I-ID. Ignoring this Machine PAC request

  Message Description: Machine PAC request does not contain I-ID. Ignoring this Machine PAC request

  Local Target Message Format: <timestamp> <seq_num>11552 WARN EAP Machine PAC request does not contain I-ID. Ignoring this Machine PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11552 WARN EAP Machine PAC request does not contain I-ID. Ignoring this Machine PAC request, <log details>

- **Message Code:** 11553

  Severity: WARN

Message Text: Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID

Message Description: Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID

Local Target Message Format: <timestamp> <seq_num>11553 WARN RADIUS Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11553 WARN RADIUS Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID, <log details>

- **Message Code:** 11554

  Severity: INFO

  Message Text: Received Authorization PAC

  Message Description: Received Authorization PAC from client.

  Local Target Message Format: <timestamp> <seq_num>11554 INFO EAP Received Authorization PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11554 INFO EAP Received Authorization PAC, <log details>

- **Message Code:** 11555

  Severity: INFO

  Message Text: Received User Authorization PAC

  Message Description: Received User Authorization PAC from client.

  Local Target Message Format: <timestamp> <seq_num>11555 INFO EAP Received User Authorization PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11555 INFO EAP Received User Authorization PAC, <log details>

- **Message Code:** 11556

  Severity: INFO

  Message Text: Received Machine Authorization PAC

  Message Description: Received Machine Authorization PAC from client.

  Local Target Message Format: <timestamp> <seq_num>11556 INFO EAP Received Machine Authorization PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11556 INFO EAP Received Machine Authorization PAC, <log details>

- **Message Code:** 11557

  Severity: INFO

Message Text: Using client certificate for authentication

Message Description: ISE received client certificate during tunnel establishment or inside the tunnel. ISE is going to verify this certificate and use it for authentication.

Local Target Message Format: <timestamp> <seq_num>11557 INFO EAP Using client certificate for authentication, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11557 INFO EAP Using client certificate for authentication, <log details>

- **Message Code:** 11558

  Severity: INFO

  Message Text: Client certificate was received inside the tunnel

  Message Description: The supplicant provided client certificate inside the tunnel (certificate was send encrypted)

  Local Target Message Format: <timestamp> <seq_num>11558 INFO EAP Client certificate was received inside the tunnel, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11558 INFO EAP Client certificate was received inside the tunnel, <log details>

- **Message Code:** 11559

  Severity: INFO

  Message Text: Client certificate was requested but not received inside the tunnel. Will continue with inner method.

  Message Description: ISE requested client certificate inside the tunnel but the supplicant has not provided the client certificate. ISE will continue authenticating the supplicant by running the inner method.

  Local Target Message Format: <timestamp> <seq_num>11559 INFO EAP Client certificate was requested but not received inside the tunnel. Will continue with inner method., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11559 INFO EAP Client certificate was requested but not received inside the tunnel. Will continue with inner method., <log details>

- **Message Code:** 11560

  Severity: INFO

  Message Text: Client certificate was received during tunnel establishment

  Message Description: The supplicant provided a client certificate during tunnel establishment (certificate was sent not encrypted)

  Local Target Message Format: <timestamp> <seq_num>11560 INFO EAP Client certificate was received during tunnel establishment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11560 INFO EAP Client certificate was received during tunnel establishment, <log details>

- **Message Code:** 11561

  Severity: INFO

  Message Text: Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel.

  Message Description: ISE requested client certificate during tunnel establishment but the supplicant did not provided the client certificate. The supplicant may be configured to not send the client certificte unless encrypted. ISE will renegotiate and request the client certificate inside the tunnel.

  Local Target Message Format: <timestamp> <seq_num>11561 INFO EAP Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11561 INFO EAP Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel., <log details>

- **Message Code:** 11562

  Severity: INFO

  Message Text: Client certificate was received but authentication failed

  Message Description: ISE received client certificate during tunnel establishment or inside the tunnel but the authentication failed.

  Local Target Message Format: <timestamp> <seq_num>11562 INFO EAP Client certificate was received but authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11562 INFO EAP Client certificate was received but authentication failed, <log details>

- **Message Code:** 11563

  Severity: INFO

  Message Text: TEAP inner method skipped

  Message Description: Skipped the TEAP inner method.

  Local Target Message Format: <timestamp> <seq_num>11563 INFO EAP TEAP inner method skipped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11563 INFO EAP TEAP inner method skipped, <log details>

- **Message Code:** 11564

  Severity: INFO

  Message Text: TEAP inner method started

  Message Description: Started the TEAP inner method.

  Local Target Message Format: <timestamp> <seq_num>11564 INFO EAP TEAP inner method started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11564 INFO EAP TEAP inner method started, <log details>

- **Message Code:** 11565

  Severity: INFO

  Message Text: TEAP inner method finished successfully

  Message Description: TEAP inner method finished successfully.

  Local Target Message Format: <timestamp> <seq_num>11565 INFO EAP TEAP inner method finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11565 INFO EAP TEAP inner method finished successfully, <log details>

- **Message Code:** 11566

  Severity: WARN

  Message Text: TEAP inner method finished with failure

  Message Description: TEAP inner method finished with failure.

  Local Target Message Format: <timestamp> <seq_num>11566 WARN EAP TEAP inner method finished with failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11566 WARN EAP TEAP inner method finished with failure, <log details>

- **Message Code:** 11567

  Severity: INFO

  Message Text: Identity type provided by client is equal to requested

  Message Description: ISE requested a specific identity type from the client for current inner method and the client confirmed usage of this identity type.

  Local Target Message Format: <timestamp> <seq_num>11567 INFO EAP Identity type provided by client is equal to requested, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11567 INFO EAP Identity type provided by client is equal to requested, <log details>

- **Message Code:** 11568

  Severity: INFO

  Message Text: Identity type provided by client is not equal to requested type

  Message Description: ISE requested a specific identity type from the client for the current inner method and the client denied usage of this identity type.

  Local Target Message Format: <timestamp> <seq_num>11568 INFO EAP Identity type provided by client is not equal to requested type, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11568 INFO EAP Identity type provided by client is not equal to requested type, <log details>

- **Message Code:** 11569

  Severity: INFO

  Message Text: Client suggested 'User' identity type instead

  Message Description: Client sugested using the identity type 'User' in the current inner method.

  Local Target Message Format: <timestamp> <seq_num>11569 INFO EAP Client suggested 'User' identity type instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11569 INFO EAP Client suggested 'User' identity type instead, <log details>

- **Message Code:** 11570

  Severity: INFO

  Message Text: Client suggested 'Machine' identity type instead

  Message Description: Client sugested using the identity type 'Machine' in the current inner method.

  Local Target Message Format: <timestamp> <seq_num>11570 INFO EAP Client suggested 'Machine' identity type instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11570 INFO EAP Client suggested 'Machine' identity type instead, <log details>

- **Message Code:** 11571

  Severity: INFO

  Message Text: Identity type provided by client was already used for authentication

  Message Description: Client sugested to use an identity type in the current inner method that was already used in a previous inner method. ISE is rejecting this identity type.

  Local Target Message Format: <timestamp> <seq_num>11571 INFO EAP Identity type provided by client was already used for authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11571 INFO EAP Identity type provided by client was already used for authentication, <log details>

- **Message Code:** 11572

  Severity: INFO

  Message Text: Identity type provided by client is currently unsupported

  Message Description: Client sugested using an identity type in current inner method that is not supported by ISE. ISE is rejecting this identity type.

  Local Target Message Format: <timestamp> <seq_num>11572 INFO EAP Identity type provided by client is currently unsupported, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11572 INFO EAP Identity type provided by client is currently unsupported, <log details>

- **Message Code:** 11573

  Severity: INFO

  Message Text: Selected identity type 'User'

  Message Description: ISE selected identity type 'User' to use in current inner method.

  Local Target Message Format: <timestamp> <seq_num>11573 INFO EAP Selected identity type 'User', <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11573 INFO EAP Selected identity type 'User', <log details>

- **Message Code:** 11574

  Severity: INFO

  Message Text: Selected identity type 'Machine'

  Message Description: ISE selected identity type 'Machine' to use in current inner method.

  Local Target Message Format: <timestamp> <seq_num>11574 INFO EAP Selected identity type 'Machine', <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11574 INFO EAP Selected identity type 'Machine', <log details>

- **Message Code:** 11575

  Severity: INFO

  Message Text: Client does not support EAP chaining. Switching to usual mode

  Message Description: ISE send Identity Type TLV in EAP request to client to conduct EP chaining. However Identity Type TLV is not present in client response. So EAP chaining is not supported by the client. ISE is switching to usual mode.

  Local Target Message Format: <timestamp> <seq_num>11575 INFO EAP Client does not support EAP chaining. Switching to usual mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11575 INFO EAP Client does not support EAP chaining. Switching to usual mode, <log details>

- **Message Code:** 11576

  Severity: DEBUG

  Message Text: TEAP cryptobinding verification passed

  Message Description: TEAP cryptobinding verification passed.

  Local Target Message Format: <timestamp> <seq_num>11576 DEBUG EAP TEAP cryptobinding verification passed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11576 DEBUG EAP TEAP cryptobinding verification passed, <log details>

- **Message Code:** 11577

  Severity: WARN

  Message Text: TEAP cryptobinding verification failed

  Message Description: TEAP cryptobinding verification failed.

  Local Target Message Format: <timestamp> <seq_num>11577 WARN EAP TEAP cryptobinding verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11577 WARN EAP TEAP cryptobinding verification failed, <log details>

- **Message Code:** 11578

  Severity: WARN

  Message Text: Rejected PAC provisioning request because supplicant failed to adhere to protocol

  Message Description: Rejected the PAC provisioning request because the client's supplicant failed to properly adhere to the TEAP protocol. Not only did it fail to send an ACK for the almost-provisioned PAC, but it also failed to properly follow up by sending a valid additional request for a Tunnel PAC or a Machine PAC.

  Local Target Message Format: <timestamp> <seq_num>11578 WARN EAP Rejected PAC provisioning request because supplicant failed to adhere to protocol, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11578 WARN EAP Rejected PAC provisioning request because supplicant failed to adhere to protocol, <log details>

- **Message Code:** 11579

  Severity: WARN

  Message Text: No valid PAC requests on provisioning

  Message Description: Client did not send valid PAC request at the end of TEAP provisioning conversation. Provisioning conversation should always finish with sending requested one or more PACs to the client. Legacy client may not ask for specific PAC since in initial draft of TEAP protocol there was only one PAC type and it was unnecessary to specify it. ISE provides legacy Tunnel V1 PAC in such case. More advanced client may reequest several PAC types but they need to conform certain rules. For example, ISE cannot provide User Authorization PAC if Tunnel PAC was not requested.

  Local Target Message Format: <timestamp> <seq_num>11579 WARN EAP No valid PAC requests on provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11579 WARN EAP No valid PAC requests on provisioning, <log details>

- **Message Code:** 11580

Severity: WARN

Message Text: Rejected PAC unexpectedly received during PAC-less mode of TEAP

Message Description: Despite the fact that Allowed protocols has configured TEAP to use the PAC-less mode of operation, the client's supplicant has sent a PAC to ISE, as if the PAC-based mode is being used.

Local Target Message Format: <timestamp> <seq_num>11580 WARN EAP Rejected PAC unexpectedly received during PAC-less mode of TEAP, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11580 WARN EAP Rejected PAC unexpectedly received during PAC-less mode of TEAP, <log details>

- **Message Code:** 11581

  Severity: INFO

  Message Text: Perform fallback on invalid PAC to provisioning

  Message Description: ISE received an invalid PAC during authentication and perform fallback to PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num>11581 INFO EAP Perform fallback on invalid PAC to provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11581 INFO EAP Perform fallback on invalid PAC to provisioning, <log details>

- **Message Code:** 11582

  Severity: INFO

  Message Text: Approved TEAP client Tunnel PAC request

  Message Description: Approved the TEAP request by the client's supplicant to provision a Tunnel PAC.

  Local Target Message Format: <timestamp> <seq_num>11582 INFO EAP Approved TEAP client Tunnel PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11582 INFO EAP Approved TEAP client Tunnel PAC request, <log details>

- **Message Code:** 11583

  Severity: INFO

  Message Text: Approved TEAP client Machine PAC request

  Message Description: Approved the TEAP request by the client's supplicant to provision a Machine PAC.

  Local Target Message Format: <timestamp> <seq_num>11583 INFO EAP Approved TEAP client Machine PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11583 INFO EAP Approved TEAP client Machine PAC request, <log details>

- **Message Code:** 11584

  Severity: INFO

  Message Text: Approved TEAP client Authorization PAC request

  Message Description: Approved the TEAP request by the client's supplicant to provision an Authorization PAC.

  Local Target Message Format: <timestamp> <seq_num>11584 INFO EAP Approved TEAP client Authorization PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11584 INFO EAP Approved TEAP client Authorization PAC request, <log details>

- **Message Code:** 11585

  Severity: INFO

  Message Text: Received Tunnel PAC

  Message Description: Received Tunnel PAC from client.

  Local Target Message Format: <timestamp> <seq_num>11585 INFO EAP Received Tunnel PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11585 INFO EAP Received Tunnel PAC, <log details>

- **Message Code:** 11586

  Severity: INFO

  Message Text: Received Machine PAC

  Message Description: Received Machine PAC from client.

  Local Target Message Format: <timestamp> <seq_num>11586 INFO EAP Received Machine PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11586 INFO EAP Received Machine PAC, <log details>

- **Message Code:** 11587

  Severity: INFO

  Message Text: Received CTS PAC

  Message Description: Received CTS PAC from client

  Local Target Message Format: <timestamp> <seq_num>11587 INFO EAP Received CTS PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11587 INFO EAP Received CTS PAC, <log details>

- **Message Code:** 11588

  Severity: WARN

  Message Text: Supplicant failed to adhere to protocol

  Message Description: Client's supplicant failed to properly adhere to the TEAP protocol. It did fail to send a correct Result Tlv.

  Local Target Message Format: <timestamp> <seq_num>11588 WARN EAP Supplicant failed to adhere to protocol, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11588 WARN EAP Supplicant failed to adhere to protocol, <log details>

- **Message Code:** 11589

  Severity: INFO

  Message Text: Anonymous TLS renegotiation succeeded

  Message Description: TEAP Anonymous TLS renegotiation finished with success

  Local Target Message Format: <timestamp> <seq_num>11589 INFO EAP Anonymous TLS renegotiation succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11589 INFO EAP Anonymous TLS renegotiation succeeded, <log details>

- **Message Code:** 11590

  Severity: WARN

  Message Text: Anonymous TLS renegotiation failed

  Message Description: Anonymous TLS renegotiation failed.

  Local Target Message Format: <timestamp> <seq_num>11590 WARN EAP Anonymous TLS renegotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11590 WARN EAP Anonymous TLS renegotiation failed, <log details>

- **Message Code:** 11591

  Severity: INFO

  Message Text: Accept client on authenticated provisioning

  Message Description: Accept client on authenticated provisioning

  Local Target Message Format: <timestamp> <seq_num>11591 INFO EAP Accept client on authenticated provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11591 INFO EAP Accept client on authenticated provisioning, <log details>

- **Message Code:** 11592

  Severity: INFO

  Message Text: Prepared RADIUS Access-Reject after the successful in-band PAC provisioning

  Message Description: As part of the standard in-band PAC provisioning behavior, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC request was successfully approved. This admittedly-misleading result value is nevertheless normal, does not truly imply a failure, and can/should be safely ignored. (Most likely, the ISE logs will show a subsequent EAP- conversation for this user attempting to actually authenticate using the PAC that was currently provisioned.)

  Local Target Message Format: <timestamp> <seq_num>11592 INFO EAP Prepared RADIUS Access-Reject after the successful in-band PAC provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11592 INFO EAP Prepared RADIUS Access-Reject after the successful in-band PAC provisioning, <log details>

- **Message Code:** 11593

  Severity: WARN

  Message Text: TEAP provisioning failed. General error

  Message Description: TEAP provisioning failed. Could not build secure tunnel.

  Local Target Message Format: <timestamp> <seq_num>11593 WARN EAP TEAP provisioning failed. General error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11593 WARN EAP TEAP provisioning failed. General error, <log details>

- **Message Code:** 11594

  Severity: WARN

  Message Text: Client certificate authentication failed

  Message Description: Client certificate authentication failed

  Local Target Message Format: <timestamp> <seq_num>11594 WARN EAP Client certificate authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11594 WARN EAP Client certificate authentication failed, <log details>

- **Message Code:** 11595

  Severity: INFO

  Message Text: Extracted EAP-Response containing TEAP challenge-response

  Message Description: Continuing the TEAP protocol; processing the TEAP challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num>11595 INFO EAP Extracted EAP-Response containing TEAP challenge-response, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11595 INFO EAP Extracted EAP-Response containing TEAP challenge-response, <log details>

- **Message Code:** 11596

  Severity: INFO

  Message Text: Prepared EAP-Request with another TEAP challenge

  Message Description: As part of the continuation of the TEAP protocol, created an EAP-Request packet containing another TEAP challenge, for attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num>11596 INFO EAP Prepared EAP-Request with another TEAP challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11596 INFO EAP Prepared EAP-Request with another TEAP challenge, <log details>

- **Message Code:** 11597

  Severity: INFO

  Message Text: TEAP authentication phase finished successfully

  Message Description: TEAP authentication phase finished successfully.

  Local Target Message Format: <timestamp> <seq_num>11597 INFO EAP TEAP authentication phase finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11597 INFO EAP TEAP authentication phase finished successfully, <log details>

- **Message Code:** 11598

  Severity: WARN

  Message Text: TEAP authentication failed

  Message Description: TEAP authentication failed.

  Local Target Message Format: <timestamp> <seq_num>11598 WARN EAP TEAP authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11598 WARN EAP TEAP authentication failed, <log details>

- **Message Code:** 11599

  Severity: INFO

  Message Text: TEAP provisioning phase finished successfully

  Message Description: TEAP provisioning phase finished successfully.

  Local Target Message Format: <timestamp> <seq_num>11599 INFO EAP TEAP provisioning phase finished successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11599 INFO EAP TEAP provisioning phase finished successfully, <log details>

- **Message Code:** 11600

  Severity: INFO

  Message Text: TEAP provisioning phase finished

  Message Description: Completed the TEAP PAC-provisioning phase. According to the standard, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC request was successfully approved. Thus, there is a need to check if the PAC was indeed actually issued or not.

  Local Target Message Format: <timestamp> <seq_num>11600 INFO EAP TEAP provisioning phase finished, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11600 INFO EAP TEAP provisioning phase finished, <log details>

- **Message Code:** 11601

  Severity: WARN

  Message Text: TEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Message Description: TEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Local Target Message Format: <timestamp> <seq_num>11601 WARN EAP TEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11601 WARN EAP TEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

- **Message Code:** 11602

  Severity: WARN

  Message Text: TEAP failed SSL/TLS handshake after a client alert

  Message Description: TEAP failed SSL/TLS handshake after a client alert

  Local Target Message Format: <timestamp> <seq_num>11602 WARN EAP TEAP failed SSL/TLS handshake after a client alert, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11602 WARN EAP TEAP failed SSL/TLS handshake after a client alert, <log details>

- **Message Code:** 11603

  Severity: WARN

  Message Text: PAC verification failed

  Message Description: Received from the client a PAC that failed to pass verification.

Local Target Message Format: <timestamp> <seq_num>11603 WARN EAP PAC verification failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11603 WARN EAP PAC verification failed, <log details>

- **Message Code:** 11604

  Severity: WARN

  Message Text: PAC contains invalid Authority ID

  Message Description: The Authority ID of the client's PAC does not match that of the ISE server that processed the authentication request, probably because the client's PAC was created by another ISE.

  Local Target Message Format: <timestamp> <seq_num>11604 WARN EAP PAC contains invalid Authority ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11604 WARN EAP PAC contains invalid Authority ID, <log details>

- **Message Code:** 11605

  Severity: WARN

  Message Text: PAC contains invalid PAC type

  Message Description: Received from the client a PAC containing an invalid PAC type.

  Local Target Message Format: <timestamp> <seq_num>11605 WARN EAP PAC contains invalid PAC type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11605 WARN EAP PAC contains invalid PAC type, <log details>

- **Message Code:** 11606

  Severity: WARN

  Message Text: PAC has expired - rejecting it

  Message Description: Received from the client a PAC that has expired. Rejecting it.

  Local Target Message Format: <timestamp> <seq_num>11606 WARN EAP PAC has expired - rejecting it, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11606 WARN EAP PAC has expired - rejecting it, <log details>

- **Message Code:** 11607

  Severity: INFO

  Message Text: User Authorization PAC has expired - will run inner method

Message Description: Received from the client User Authorization PAC that has expired. Expired Authorization PAC cannot be used for fast reconnect so ISE will run inner method to authenticate the user.

Local Target Message Format: <timestamp> <seq_num>11607 INFO EAP User Authorization PAC has expired - will run inner method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11607 INFO EAP User Authorization PAC has expired - will run inner method, <log details>

- **Message Code:** 11608

  Severity: INFO

  Message Text: Machine Authorization PAC has expired - will run inner method

  Message Description: Received from the client Machine Authorization PAC that has expired. Expired Authorization PAC cannot be used for fast reconnect so ISE will run inner method to authenticate the machine.

  Local Target Message Format: <timestamp> <seq_num>11608 INFO EAP Machine Authorization PAC has expired - will run inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11608 INFO EAP Machine Authorization PAC has expired - will run inner method, <log details>

- **Message Code:** 11609

  Severity: WARN

  Message Text: Cannot decrypt PAC because of specified master key was not found - rejecting the PAC

  Message Description: Received from the client a PAC that cannot be decrypted because of specified master key was not found. Rejecting it.

  Local Target Message Format: <timestamp> <seq_num>11609 WARN EAP Cannot decrypt PAC because of specified master key was not found - rejecting the PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11609 WARN EAP Cannot decrypt PAC because of specified master key was not found - rejecting the PAC, <log details>

- **Message Code:** 11610

  Severity: WARN

  Message Text: PAC contains invalid Authentication Tag

  Message Description: Received from the client a PAC containing an invalid Authentication Tag.

  Local Target Message Format: <timestamp> <seq_num>11610 WARN EAP PAC contains invalid Authentication Tag, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11610 WARN EAP PAC contains invalid Authentication Tag, <log details>

- **Message Code:** 11611

Severity: WARN

Message Text: Failed to decrypt PAC

Message Description: Failed to decrypt the PAC received from the client's supplicant.

Local Target Message Format: <timestamp> <seq_num>11611 WARN EAP Failed to decrypt PAC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11611 WARN EAP Failed to decrypt PAC, <log details>

- **Message Code:** 11612

  Severity: WARN

  Message Text: Failed to derive TEAP Master Key

  Message Description: Failed to derive TEAP Master Key.

  Local Target Message Format: <timestamp> <seq_num>11612 WARN EAP Failed to derive TEAP Master Key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11612 WARN EAP Failed to derive TEAP Master Key, <log details>

- **Message Code:** 11613

  Severity: WARN

  Message Text: Fallback on invalid PAC: no available additional cipher configured on server

  Message Description: Fallback on invalid PAC: no available additional cipher configured on server.

  Local Target Message Format: <timestamp> <seq_num>11613 WARN EAP Fallback on invalid PAC: no available additional cipher configured on server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11613 WARN EAP Fallback on invalid PAC: no available additional cipher configured on server, <log details>

- **Message Code:** 11614

  Severity: WARN

  Message Text: Cannot perform more then one invalid PAC fallback

  Message Description: There seems to be an internal problem with the client's supplicant, which is incorrectly trying to send an invalid PAC more then once during a single TEAP conversation.

  Local Target Message Format: <timestamp> <seq_num>11614 WARN EAP Cannot perform more then one invalid PAC fallback, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11614 WARN EAP Cannot perform more then one invalid PAC fallback, <log details>

- **Message Code:** 11615

Severity: WARN

Message Text: No cipher on client side for invalid PAC fallback

Message Description: ISE is unable to complete the TLS handshake, because none of the ciphersuites suggested by the client's supplicant are compatible with invalid PAC fallback. This might be due to the fact that a manually-provisioned PAC is no longer valid, and configuration in Allowed Protocols does not allow any of the forms of in-band PAC provisioning expected by the client.

Local Target Message Format: <timestamp> <seq_num>11615 WARN EAP No cipher on client side for invalid PAC fallback, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11615 WARN EAP No cipher on client side for invalid PAC fallback, <log details>

- **Message Code:** 11616

  Severity: WARN

  Message Text: Neither anonymous nor authenticated provisioning allowed by Allowed Protocols

  Message Description: The attempt to provision a PAC failed because the relevant Allowed Protocols allows neither anonymous nor authenticated in-band PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num>11616 WARN EAP Neither anonymous nor authenticated provisioning allowed by Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11616 WARN EAP Neither anonymous nor authenticated provisioning allowed by Allowed Protocols, <log details>

- **Message Code:** 11617

  Severity: WARN

  Message Text: Client didn't provide suitable ciphers for anonymous PAC-provisioning

  Message Description: The TEAP in-band PAC-provisioning request issued by the client's supplicant has internally specified a cipher. This cipher is not compatible with the provisioning method currently allowed by Allowed Protocols configuration: Anonymous In-Band PAC provisioning. If you need this provisioning method, this message indicates that the supplicant is either configured incorrectly or that it cannot be used to perform Anonymous provisioning using the current version of ISE. If you need Authenticated provisioning, this message indicates that the Allowed Protocols configuration currently does not allow Authenticated In-Band PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num>11617 WARN EAP Client didn't provide suitable ciphers for anonymous PAC-provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11617 WARN EAP Client didn't provide suitable ciphers for anonymous PAC-provisioning, <log details>

- **Message Code:** 11618

  Severity: WARN

  Message Text: Client didn't provide suitable ciphers for authenticated PAC provisioning

Message Description: The TEAP in-band PAC-provisioning request issued by the client's supplicant internally specified a cipher that is not compatible with the only provisioning method currently allowed by Allowed Protocols configuration: Authenticated In-Band PAC Provisioning. If this is indeed the desired provisioning method, then this message indicates that the supplicant is either configured improperly or that it cannot be used to perform authenticated provisioning with the current version of ISE. Alternatively, if anonymous provisioning is the method actually desired, then this message indicates that Allowed Protocols configuration currently does not allow Anonymous In-Band PAC Provisioning.

Local Target Message Format: <timestamp> <seq_num>11618 WARN EAP Client didn't provide suitable ciphers for authenticated PAC provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11618 WARN EAP Client didn't provide suitable ciphers for authenticated PAC provisioning, <log details>

- **Message Code:** 11619

  Severity: WARN

  Message Text: Client didn't provide suitable ciphers for either anonymous or authenticated PAC-provisioning

  Message Description: The TEAP in-band PAC-provisioning request issued by the client's supplicant has internally specified a cipher. This cipher is not compatible with either of the two provisioning methods currently allowed by Allowed Protocols configuration: Anonymous In-Band PAC provisioning or Authenticated In-Band PAC provisioning. The supplicant is either configured incorrectly or it cannot be used to perform PAC provisioning with the current version of ISE.

  Local Target Message Format: <timestamp> <seq_num>11619 WARN EAP Client didn't provide suitable ciphers for either anonymous or authenticated PAC-provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11619 WARN EAP Client didn't provide suitable ciphers for either anonymous or authenticated PAC-provisioning, <log details>

- **Message Code:** 11620

  Severity: INFO

  Message Text: TEAP full handshake finished successfully

  Message Description: TEAP full handshake finished successfully

  Local Target Message Format: <timestamp> <seq_num>11620 INFO EAP TEAP full handshake finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11620 INFO EAP TEAP full handshake finished successfully, <log details>

- **Message Code:** 11621

  Severity: INFO

  Message Text: TEAP PAC-less session resumed successfully

  Message Description: Using the PAC-less mode of TEAP authentication. The tunnel was successfully built using short handshake.

Local Target Message Format: <timestamp> <seq_num>11621 INFO EAP TEAP PAC-less session resumed successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11621 INFO EAP TEAP PAC-less session resumed successfully, <log details>

- **Message Code:** 11622

  Severity: INFO

  Message Text: TEAP built authenticated tunnel for purpose of PAC provisioning

  Message Description: TEAP full handshake finished successfully - built authenticated tunnel for purpose of phase-0 PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num>11622 INFO EAP TEAP built authenticated tunnel for purpose of PAC provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11622 INFO EAP TEAP built authenticated tunnel for purpose of PAC provisioning, <log details>

- **Message Code:** 11623

  Severity: INFO

  Message Text: TEAP built anonymous tunnel for purpose of PAC provisioning

  Message Description: TEAP full handshake finished successfully - built anonymous tunnel for purpose of phase-0 PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num>11623 INFO EAP TEAP built anonymous tunnel for purpose of PAC provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11623 INFO EAP TEAP built anonymous tunnel for purpose of PAC provisioning, <log details>

- **Message Code:** 11624

  Severity: INFO

  Message Text: TEAP built PAC-based tunnel for purpose of authentication

  Message Description: TEAP short handshake finished successfully - built PAC-based tunnel for purpose of phase-1 authentication.

  Local Target Message Format: <timestamp> <seq_num>11624 INFO EAP TEAP built PAC-based tunnel for purpose of authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11624 INFO EAP TEAP built PAC-based tunnel for purpose of authentication, <log details>

- **Message Code:** 11625

  Severity: WARN

  Message Text: No cipher for PAC-less TEAP authentication

Message Description: The cipher specified by the client's supplicant during the TLS handshake portion of TEAP is not compatible with the PAC-less mode of operation currently configured in Allowed protocols configuration. This could be because the supplicant is either incorrectly configured, or even inherently unable in general, to work with PAC-less TEAP authentication using the current version of ISE.

Local Target Message Format: <timestamp> <seq_num>11625 WARN EAP No cipher for PAC-less TEAP authentication, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11625 WARN EAP No cipher for PAC-less TEAP authentication, <log details>

- **Message Code:** 11626

  Severity: WARN

  Message Text: Unexpectedly received empty TLS message during TEAP handshake; treating as a rejection by the client

  Message Description: While trying to negotiate a TLS handshake with the client inside the TEAP tunnel, ISE expected to receive a non-empty TLS message or TLS alert message, but instead received an empty TLS message. This could be due to an inconformity in the implementation of the protocol between ISE and the supplicant. ISE treated the unexpected message as a sign that the client rejected the tunnel renegotiation.

  Local Target Message Format: <timestamp> <seq_num>11626 WARN EAP Unexpectedly received empty TLS message during TEAP handshake; treating as a rejection by the client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11626 WARN EAP Unexpectedly received empty TLS message during TEAP handshake; treating as a rejection by the client, <log details>

- **Message Code:** 11627

  Severity: INFO

  Message Text: Starting EAP chaining

  Message Description: ISE is configured to perform EAP chaining. ISE is starting EAP chanining and assume that client also supports EAP chaining.

  Local Target Message Format: <timestamp> <seq_num>11627 INFO EAP Starting EAP chaining, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11627 INFO EAP Starting EAP chaining, <log details>

- **Message Code:** 11628

  Severity: INFO

  Message Text: TEAP needs to proactively update PAC that is about to expire

  Message Description: TEAP needs to proactively update PAC that is about to expire.

  Local Target Message Format: <timestamp> <seq_num>11628 INFO EAP TEAP needs to proactively update PAC that is about to expire, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11628 INFO EAP TEAP needs to proactively update PAC that is about to expire, <log details>

- **Message Code:** 11629

  Severity: WARN

  Message Text: Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request

  Message Description: Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request

  Local Target Message Format: <timestamp> <seq_num>11629 WARN EAP Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11629 WARN EAP Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request, <log details>

- **Message Code:** 11630

  Severity: DEBUG

  Message Text: TEAP channelbinding verification passed

  Message Description: TEAP channelbinding verification passed.

  Local Target Message Format: <timestamp> <seq_num>11630 DEBUG EAP TEAP channelbinding verification passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11630 DEBUG EAP TEAP channelbinding verification passed, <log details>

- **Message Code:** 11631

  Severity: WARN

  Message Text: TEAP channelbinding verification failed

  Message Description: TEAP channelbinding verification failed.

  Local Target Message Format: <timestamp> <seq_num>11631 WARN EAP TEAP channelbinding verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11631 WARN EAP TEAP channelbinding verification failed, <log details>

- **Message Code:** 11632

  Severity: INFO

  Message Text: Prepared Identity Type Tlv for inner method

  Message Description: Created an Identity Type Tlv packet, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

Local Target Message Format: <timestamp> <seq_num>11632 INFO EAP Prepared Identity Type Tlv for inner method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11632 INFO EAP Prepared Identity Type Tlv for inner method, <log details>

- **Message Code:** 11633

  Severity: WARN

  Message Text: Client requested TLSv1.1 that is not allowed

  Message Description: Client requested TLSv1.1 as the highest version but it is not allowed.

  Local Target Message Format: <timestamp> <seq_num>11633 WARN EAP Client requested TLSv1.1 that is not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11633 WARN EAP Client requested TLSv1.1 that is not allowed, <log details>

- **Message Code:** 11634

  Severity: WARN

  Message Text: Client requested TLS of unknown version

  Message Description: Client requested TLS of version that does not supported.

  Local Target Message Format: <timestamp> <seq_num>11634 WARN EAP Client requested TLS of unknown version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11634 WARN EAP Client requested TLS of unknown version, <log details>

- **Message Code:** 11635

  Severity: WARN

  Message Text: Downgrading from EMSK to MSK is not allowed

  Message Description: Client send Crypto-Binding TLV without EMSK compound MAC. TEAP settings forbid downgrading to MSK when EMSK is available (e.g. w/ EAP-TLS inner method).

  Local Target Message Format: <timestamp> <seq_num>11635 WARN EAP Downgrading from EMSK to MSK is not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11635 WARN EAP Downgrading from EMSK to MSK is not allowed, <log details>

- **Message Code:** 11636

  Severity: INFO

  Message Text: Client certificate was requested but not received during tunnel establishment.

Message Description: ISE requested client certificate during tunnel establishment but the supplicant did not provide the client certificate. The supplicant may be not configured to send the client certificate in the clear.

Local Target Message Format: <timestamp> <seq_num>11636 INFO EAP Client certificate was requested but not received during tunnel establishment., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11636 INFO EAP Client certificate was requested but not received during tunnel establishment., <log details>

- **Message Code:** 11637

  Severity: INFO

  Message Text: Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration

  Message Description: Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration

  Local Target Message Format: <timestamp> <seq_num>11637 INFO EAP Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11637 INFO EAP Inner method supports EMSK but the client provided only MSK. Allow downgrade as per configuration, <log details>

- **Message Code:** 11639

  Severity: WARN

  Message Text: Client requested TLSv1.0 that is not allowed

  Message Description: Client requested TLSv1.0 as the highest version. This version is not allowed by ISE.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.0 that is not allowed WARN Client requested TLSv1.0 as the highest version. This version is not allowed by ISE., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.0 that is not allowed WARN Client requested TLSv1.0 as the highest version. This version is not allowed by ISE., <log details>

- **Message Code:** 11640

  Severity: WARN

  Message Text: Client requested TLSv1.2 that is not allowed

  Message Description: Client requested TLSv1.2 as the highest version. This version is not allowed by ISE.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.2 that is not allowed WARN Client requested TLSv1.2 as the highest version. This version is not allowed by ISE., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.2 that is not allowed WARN Client requested TLSv1.2 as the highest version. This version is not allowed by ISE., <log details>

- **Message Code:** 11641

  Severity: WARN

  Message Text: Client requested TLSv1.3 that is not allowed

  Message Description: Client requested TLSv1.3 as the highest version. This version is not allowed by ISE.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.3 that is not allowed WARN Client requested TLSv1.3 as the highest version. This version is not allowed by ISE., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.3 that is not allowed WARN Client requested TLSv1.3 as the highest version. This version is not allowed by ISE., <log details>

- **Message Code:** 11642

  Severity: WARN

  Message Text: Client requested TLSv1.3, but is not supported with EAP-TTLS

  Message Description: Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with EAP-TTLS by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.3, but is not supported with EAP-TTLS WARN Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with EAP-TTLS by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.3, but is not supported with EAP-TTLS WARN Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with EAP-TTLS by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3., <log details>

- **Message Code:** 11643

  Severity: WARN

  Message Text: Client requested TLSv1.3, but is not supported with PEAP

  Message Description: Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with PEAP by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.3, but is not supported with PEAP WARN Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with PEAP by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.3,

but is not supported with PEAP WARN Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with PEAP by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3., <log details>

- **Message Code:** 11644

  Severity: WARN

  Message Text: Client requested TLSv1.3, but is not supported with EAP-FAST

  Message Description: Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with EAP-FAST by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.3, but is not supported with EAP-FAST WARN Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with EAP-FAST by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.3, but is not supported with EAP-FAST WARN Client requested TLSv1.3 as the highest version. Currently TLSv1.2 is the highest version supported with EAP-FAST by ISE. EAP-TLS and TEAP protocols can be used with TLSv1.3., <log details>

- **Message Code:** 11645

  Severity: WARN

  Message Text: Client requested TLSv1.3 as EAP-TLS inner method, but this version is not supported as EAP-TLS inner method.

  Message Description: Client requested TLSv1.3 as EAP-TLS inner method. Currently TLSv1.2 is the highest version supported as EAP-TLS inner method.

  Local Target Message Format: <timestamp> <seq_num>EAP Client requested TLSv1.3 as EAP-TLS inner method, but this version is not supported as EAP-TLS inner method. WARN Client requested TLSv1.3 as EAP-TLS inner method. Currently TLSv1.2 is the highest version supported as EAP-TLS inner method., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client requested TLSv1.3 as EAP-TLS inner method, but this version is not supported as EAP-TLS inner method. WARN Client requested TLSv1.3 as EAP-TLS inner method. Currently TLSv1.2 is the highest version supported as EAP-TLS inner method., <log details>

- **Message Code:** 11700

  Severity: INFO

  Message Text: 5G AKA Authentication succeeded

  Message Description: 5G AKA Authentication succeeded.

  Local Target Message Format: <timestamp> <seq_num>11700 INFO RADIUS 5G AKA Authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11700 INFO RADIUS 5G AKA Authentication succeeded, <log details>

- **Message Code:** 11701

  Severity: INFO

  Message Text: 5G AKA request detected

  Message Description: 5G AKA request detected.

  Local Target Message Format: <timestamp> <seq_num>11701 INFO RADIUS 5G AKA request detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11701 INFO RADIUS 5G AKA request detected, <log details>

- **Message Code:** 11702

  Severity: INFO

  Message Text: 5G AKA is not allowed

  Message Description: 5G AKA Protocol is not allowed.

  Local Target Message Format: <timestamp> <seq_num>11702 INFO RADIUS 5G AKA is not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11702 INFO RADIUS 5G AKA is not allowed, <log details>

- **Message Code:** 11703

  Severity: INFO

  Message Text: IMSI was parsed successfully

  Message Description: IMSI was parsed successfully.

  Local Target Message Format: <timestamp> <seq_num>11703 INFO RADIUS IMSI was parsed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11703 INFO RADIUS IMSI was parsed successfully, <log details>

- **Message Code:** 11704

  Severity: INFO

  Message Text: IMSI was found in the internal database

  Message Description: IMSI was found in the internal database.

  Local Target Message Format: <timestamp> <seq_num>11704 INFO RADIUS IMSI was found in the internal database, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11704 INFO RADIUS IMSI was found in the internal database, <log details>

- **Message Code:** 11705

Severity: INFO

Message Text: 5G AKA Authentication data was generated successfully

Message Description: 5G AKA Authentication data was generated successfully.

Local Target Message Format: <timestamp> <seq_num>11705 INFO RADIUS 5G AKA Authentication data was generated successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11705 INFO RADIUS 5G AKA Authentication data was generated successfully, <log details>

- **Message Code:** 11706

  Severity: INFO

  Message Text: Single IMEI was found

  Message Description: Single IMEI was found, will return it in the response.

  Local Target Message Format: <timestamp> <seq_num>11706 INFO RADIUS Single IMEI was found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11706 INFO RADIUS Single IMEI was found, <log details>

- **Message Code:** 11707

  Severity: WARN

  Message Text: 5G AKA Authentication failed

  Message Description: 5G AKA Authentication failed.

  Local Target Message Format: <timestamp> <seq_num>11707 WARN RADIUS 5G AKA Authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11707 WARN RADIUS 5G AKA Authentication failed, <log details>

- **Message Code:** 11708

  Severity: WARN

  Message Text: 5G Serving Network Name is missing in request

  Message Description: 5G Serving Network Name is missing in request.

  Local Target Message Format: <timestamp> <seq_num>11708 WARN RADIUS 5G Serving Network Name is missing in request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11708 WARN RADIUS 5G Serving Network Name is missing in request, <log details>

- **Message Code:** 11709

  Severity: WARN

Message Text: 5G Serving Network Name has invalid format

Message Description: 5G Serving Network Name has invalid format.

Local Target Message Format: <timestamp> <seq_num>11709 WARN RADIUS 5G Serving Network Name has invalid format, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11709 WARN RADIUS 5G Serving Network Name has invalid format, <log details>

- **Message Code:** 11710

  Severity: WARN

  Message Text: 5G Invalid User Name Format

  Message Description: 5G Invalid User Name Format.

  Local Target Message Format: <timestamp> <seq_num>11710 WARN RADIUS 5G Invalid User Name Format, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11710 WARN RADIUS 5G Invalid User Name Format, <log details>

- **Message Code:** 11711

  Severity: WARN

  Message Text: 5G Invalid SUPI

  Message Description: 5G Invalid SUPI.

  Local Target Message Format: <timestamp> <seq_num>11711 WARN RADIUS 5G Invalid SUPI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11711 WARN RADIUS 5G Invalid SUPI, <log details>

- **Message Code:** 11712

  Severity: WARN

  Message Text: 5G AKA Invalid SUCI

  Message Description: 5G AKA Invalid SUCI.

  Local Target Message Format: <timestamp> <seq_num>11712 WARN RADIUS 5G AKA Invalid SUCI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11712 WARN RADIUS 5G AKA Invalid SUCI, <log details>

- **Message Code:** 11713

  Severity: INFO

  Message Text: 5G Serving Network Name Was Found

Message Description: 5G Serving Network Name Was Found.

Local Target Message Format: <timestamp> <seq_num>11713 INFO RADIUS 5G Serving Network Name Was Found, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11713 INFO RADIUS 5G Serving Network Name Was Found, <log details>

- **Message Code:** 11714

  Severity: INFO

  Message Text: Cellular request detected

  Message Description: Cellular request detected.

  Local Target Message Format: <timestamp> <seq_num>11714 INFO RADIUS Cellular request detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11714 INFO RADIUS Cellular request detected, <log details>

- **Message Code:** 11715

  Severity: INFO

  Message Text: No IMEI found for IMSI

  Message Description: No IMEI found for IMSI.

  Local Target Message Format: <timestamp> <seq_num>11715 INFO RADIUS No IMEI found for IMSI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11715 INFO RADIUS No IMEI found for IMSI, <log details>

- **Message Code:** 11716

  Severity: INFO

  Message Text: Multiple IMEIs found for IMSI

  Message Description: Multiple IMEIs found for IMSI.

  Local Target Message Format: <timestamp> <seq_num>11716 INFO RADIUS Multiple IMEIs found for IMSI, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11716 INFO RADIUS Multiple IMEIs found for IMSI, <log details>

- **Message Code:** 11717

  Severity: INFO

  Message Text: User Equipment with this IMEI was not found, creating user equipment

  Message Description: User Equipment with this IMEI was not found, creating user equipment.

Local Target Message Format: <timestamp> <seq_num>11717 INFO RADIUS User Equipment with this IMEI was not found, creating user equipment, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11717 INFO RADIUS User Equipment with this IMEI was not found, creating user equipment, <log details>

- **Message Code:** 11724

  Severity: INFO

  Message Text: 5G Authorize Only request detected

  Message Description: 5G Authorize Only request detected.

  Local Target Message Format: <timestamp> <seq_num>11724 INFO RADIUS 5G Authorize Only request detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11724 INFO RADIUS 5G Authorize Only request detected, <log details>

- **Message Code:** 11725

  Severity: WARN

  Message Text: 5G Authorize Only failed

  Message Description: 5G Authorize Only failed.

  Local Target Message Format: <timestamp> <seq_num>11725 WARN RADIUS 5G Authorize Only failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11725 WARN RADIUS 5G Authorize Only failed, <log details>

- **Message Code:** 11726

  Severity: WARN

  Message Text: 5G Authorize Only user lookup failed

  Message Description: 5G Authorize Only user lookup failed.

  Local Target Message Format: <timestamp> <seq_num>11726 WARN RADIUS 5G Authorize Only user lookup failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11726 WARN RADIUS 5G Authorize Only user lookup failed, <log details>

- **Message Code:** 11721

  Severity: WARN

  Message Text: 5G AKA user lookup failed

  Message Description: 5G AKA user lookup failed.

Local Target Message Format: <timestamp> <seq_num>11721 WARN RADIUS 5G AKA user lookup failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11721 WARN RADIUS 5G AKA user lookup failed, <log details>

- **Message Code:** 11722

  Severity: WARN

  Message Text: 5G AKA failed to generate auth data

  Message Description: 5G AKA failed to generate auth data.

  Local Target Message Format: <timestamp> <seq_num>11722 WARN RADIUS 5G AKA failed to generate auth data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11722 WARN RADIUS 5G AKA failed to generate auth data, <log details>

- **Message Code:** 11718

  Severity: INFO

  Message Text: Looking up User Equipment

  Message Description: Looking up User Equipment.

  Local Target Message Format: <timestamp> <seq_num>11718 INFO RADIUS Looking up User Equipment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11718 INFO RADIUS Looking up User Equipment, <log details>

- **Message Code:** 11719

  Severity: INFO

  Message Text: The User Equipment was not found

  Message Description: The User Equipment was not found.

  Local Target Message Format: <timestamp> <seq_num>11719 INFO RADIUS The User Equipment was not found, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11719 INFO RADIUS The User Equipment was not found, <log details>

- **Message Code:** 11720

  Severity: INFO

  Message Text: Found User Equipment

  Message Description: Found User Equipment.

Local Target Message Format: <timestamp> <seq_num>11720 INFO RADIUS Found User Equipment, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>11720 INFO RADIUS Found User Equipment, <log details>

- **Message Code:** 12000

  Severity: INFO

  Message Text: Prepared EAP-Request proposing EAP-MD5 with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-MD5 protocol, and also providing an EAP-MD5 challenge, for attachment to a RADIUS message. The EAP-MD5 protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12000 INFO EAP: Prepared EAP-Request proposing EAP-MD5 with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12000 INFO EAP: Prepared EAP-Request proposing EAP-MD5 with challenge, <log details>

- **Message Code:** 12001

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use EAP-MD5 instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-MD5 instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12001 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-MD5 instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12001 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-MD5 instead, <log details>

- **Message Code:** 12002

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-MD5 challenge-response and accepting EAP-MD5 as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing an EAP-MD5 challenge-response, and accepting EAP-MD5 as negotiated

  Local Target Message Format: <timestamp> <seq_num> 12002 INFO EAP: Extracted EAP-Response containing EAP-MD5 challenge-response and accepting EAP-MD5 as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12002 INFO EAP: Extracted EAP-Response containing EAP-MD5 challenge-response and accepting EAP-MD5 as negotiated, <log details>

- **Message Code:** 12003

  Severity: WARN

  Message Text: Failed to negotiate EAP because EAP-MD5 not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-MD5 instead. However, EAP-MD5 is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12003 WARN EAP: Failed to negotiate EAP because EAP-MD5 not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12003 WARN EAP: Failed to negotiate EAP because EAP-MD5 not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12004

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-MD5 challenge-response

  Message Description: Continuing the EAP-MD5 protocol; processing the EAP-MD5 challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12004 INFO EAP: Extracted EAP-Response containing EAP-MD5 challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12004 INFO EAP: Extracted EAP-Response containing EAP-MD5 challenge-response, <log details>

- **Message Code:** 12005

  Severity: INFO

  Message Text: EAP-MD5 authentication succeeded

  Message Description: EAP-MD5 authentication succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12005 INFO EAP: EAP-MD5 authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12005 INFO EAP: EAP-MD5 authentication succeeded, <log details>

- **Message Code:** 12006

  Severity: INFO

  Message Text: EAP-MD5 authentication failed

  Message Description: EAP-MD5 authentication failed.

  Local Target Message Format: <timestamp> <seq_num> 12006 INFO EAP: EAP-MD5 authentication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12006 INFO EAP: EAP-MD5 authentication failed, <log details>

- **Message Code:** 12007

  Severity: WARN

  Message Text: Internal error - invalid EAP-MD5 state

  Message Description: Internal error: invalid EAP-MD5 state.

  Local Target Message Format: <timestamp> <seq_num> 12007 WARN EAP: Internal error - invalid EAP-MD5 state, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12007 WARN EAP: Internal error - invalid EAP-MD5 state, <log details>

- **Message Code:** 12008

  Severity: INFO

  Message Text: Failed to parse EAP-MD5 packet

  Message Description: Failed to parse EAP-MD5 packet.

  Local Target Message Format: <timestamp> <seq_num> 12008 INFO EAP: Failed to parse EAP-MD5 packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12008 INFO EAP: Failed to parse EAP-MD5 packet, <log details>

- **Message Code:** 12100

  Severity: INFO

  Message Text: Prepared EAP-Request proposing EAP-FAST with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-FAST protocol, and also providing an EAP-FAST challenge, for attachment to a RADIUS message. The EAP-FAST protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12100 INFO EAP: Prepared EAP-Request proposing EAP-FAST with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12100 INFO EAP: Prepared EAP-Request proposing EAP-FAST with challenge, <log details>

- **Message Code:** 12101

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use EAP-FAST instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-FAST instead, per the configuration of the client's supplicant.

Local Target Message Format: <timestamp> <seq_num> 12101 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-FAST instead, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12101 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-FAST instead, <log details>

- **Message Code:** 12102

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing an EAP-FAST challenge-response, and accepting EAP-FAST as negotiated

  Local Target Message Format: <timestamp> <seq_num> 12102 INFO EAP: Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12102 INFO EAP: Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated, <log details>

- **Message Code:** 12103

  Severity: WARN

  Message Text: Failed to negotiate EAP because EAP-FAST not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-FAST instead. However, EAP-FAST is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12103 WARN EAP: Failed to negotiate EAP because EAP-FAST not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12103 WARN EAP: Failed to negotiate EAP because EAP-FAST not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12104

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-FAST challenge-response

  Message Description: Continuing the EAP-FAST protocol; processing the EAP-FAST challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12104 INFO EAP: Extracted EAP-Response containing EAP-FAST challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12104 INFO EAP: Extracted EAP-Response containing EAP-FAST challenge-response, <log details>

- **Message Code:** 12105

Severity: INFO

Message Text: Prepared EAP-Request with another EAP-FAST challenge

Message Description: As part of the continuation of the EAP-FAST protocol, created an EAP-Request packet containing another EAP-FAST challenge, for attachment to a RADIUS message.

Local Target Message Format: <timestamp> <seq_num> 12105 INFO EAP: Prepared EAP-Request with another EAP-FAST challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12105 INFO EAP: Prepared EAP-Request with another EAP-FAST challenge, <log details>

- **Message Code:** 12106

  Severity: INFO

  Message Text: EAP-FAST authentication phase finished successfully

  Message Description: EAP-FAST authentication phase finished successfully.

  Local Target Message Format: <timestamp> <seq_num> 12106 INFO EAP: EAP-FAST authentication phase finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12106 INFO EAP: EAP-FAST authentication phase finished successfully, <log details>

- **Message Code:** 12107

  Severity: INFO

  Message Text: EAP-FAST provisioning phase finished successfully

  Message Description: EAP-FAST provisioning phase finished successfully.

  Local Target Message Format: <timestamp> <seq_num> 12107 INFO EAP: EAP-FAST provisioning phase finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12107 INFO EAP: EAP-FAST provisioning phase finished successfully, <log details>

- **Message Code:** 12108

  Severity: WARN

  Message Text: EAP-FAST authentication failed

  Message Description: EAP-FAST authentication failed.

  Local Target Message Format: <timestamp> <seq_num> 12108 WARN EAP: EAP-FAST authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12108 WARN EAP: EAP-FAST authentication failed, <log details>

- **Message Code:** 12109

Severity: INFO

Message Text: EAP-FAST provisioning phase finished

Message Description: Completed the EAP-FAST PAC-provisioning phase. According to the standard, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC request was successfully approved. Thus, there is a need to check if the PAC was indeed actually issued or not.

Local Target Message Format: <timestamp> <seq_num> 12109 INFO EAP: EAP-FAST provisioning phase finished, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12109 INFO EAP: EAP-FAST provisioning phase finished, <log details>

- **Message Code:** 12110

  Severity: WARN

  Message Text: PAC verification failed

  Message Description: Received from the client a PAC that failed to pass verification.

  Local Target Message Format: <timestamp> <seq_num> 12110 WARN EAP: PAC verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12110 WARN EAP: PAC verification failed, <log details>

- **Message Code:** 12111

  Severity: WARN

  Message Text: PAC contains invalid Authority ID

  Message Description: The Authority ID of the client's PAC does not match that of the ISE server that processed the authentication request, probably because the client's PAC was created by another ISE.

  Local Target Message Format: <timestamp> <seq_num> 12111 WARN EAP: PAC contains invalid Authority ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12111 WARN EAP: PAC contains invalid Authority ID, <log details>

- **Message Code:** 12112

  Severity: WARN

  Message Text: PAC contains invalid PAC type

  Message Description: Received from the client a PAC containing an invalid PAC type.

  Local Target Message Format: <timestamp> <seq_num> 12112 WARN EAP: PAC contains invalid PAC type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12112 WARN EAP: PAC contains invalid PAC type, <log details>

- **Message Code:** 12113

  Severity: WARN

  Message Text: PAC has expired - rejecting it

  Message Description: Received from the client a PAC that has expired. Rejecting it.

  Local Target Message Format: <timestamp> <seq_num> 12113 WARN EAP: PAC has expired - rejecting it, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12113 WARN EAP: PAC has expired - rejecting it, <log details>

- **Message Code:** 12114

  Severity: WARN

  Message Text: PAC contains invalid Authentication Tag

  Message Description: Received from the client a PAC containing an invalid Authentication Tag.

  Local Target Message Format: <timestamp> <seq_num> 12114 WARN EAP: PAC contains invalid Authentication Tag, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12114 WARN EAP: PAC contains invalid Authentication Tag, <log details>

- **Message Code:** 12115

  Severity: INFO

  Message Text: Successfully finished EAP-FAST PAC provisioning/update

  Message Description: Successfully finished EAP-FAST PAC provisioning/update.

  Local Target Message Format: <timestamp> <seq_num> 12115 INFO EAP: Successfully finished EAP-FAST PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12115 INFO EAP: Successfully finished EAP-FAST PAC provisioning/update, <log details>

- **Message Code:** 12116

  Severity: WARN

  Message Text: Client sent Result TLV indicating failure

  Message Description: EAP-FAST authentication failed because client sent Result TLV indicating failure.

  Local Target Message Format: <timestamp> <seq_num> 12116 WARN EAP: Client sent Result TLV indicating failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12116 WARN EAP: Client sent Result TLV indicating failure, <log details>

- **Message Code:** 12117

Severity: WARN

Message Text: EAP-FAST inner method finished with failure

Message Description: EAP-FAST inner method finished with failure.

Local Target Message Format: <timestamp> <seq_num> 12117 WARN EAP: EAP-FAST inner method finished with failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12117 WARN EAP: EAP-FAST inner method finished with failure, <log details>

- **Message Code:** 12118

  Severity: WARN

  Message Text: EAP-FAST cryptobinding verification failed

  Message Description: EAP-FAST cryptobinding verification failed.

  Local Target Message Format: <timestamp> <seq_num> 12118 WARN EAP: EAP-FAST cryptobinding verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12118 WARN EAP: EAP-FAST cryptobinding verification failed, <log details>

- **Message Code:** 12119

  Severity: INFO

  Message Text: EAP-FAST needs to proactively update PAC that is about to expire

  Message Description: EAP-FAST needs to proactively update PAC that is about to expire.

  Local Target Message Format: <timestamp> <seq_num> 12119 INFO EAP: EAP-FAST needs to proactively update PAC that is about to expire, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12119 INFO EAP: EAP-FAST needs to proactively update PAC that is about to expire, <log details>

- **Message Code:** 12120

  Severity: WARN

  Message Text: Neither anonymous nor authenticated provisioning allowed by Allowed Protocols

  Message Description: The attempt to provision a PAC failed because the relevant Allowed Protocols allows neither anonymous nor authenticated in-band PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num> 12120 WARN EAP: Neither anonymous nor authenticated provisioning allowed by Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12120 WARN EAP: Neither anonymous nor authenticated provisioning allowed by Allowed Protocols, <log details>

- **Message Code:** 12121

Severity: WARN

Message Text: Client didn't provide suitable ciphers for anonymous PAC-provisioning

Message Description: The EAP-FAST in-band PAC-provisioning request issued by the client's supplicant has internally specified a cipher. This cipher is not compatible with the provisioning method currently allowed by Allowed Protocols configuration: Anonymous In-Band PAC provisioning. If you need this provisioning method, this message indicates that the supplicant is either configured incorrectly or that it cannot be used to perform Anonymous provisioning using the current version of ISE. If you need Authenticated provisioning, this message indicates that the Allowed Protocols configuration currently does not allow Authenticated In-Band PAC provisioning.

Local Target Message Format: <timestamp> <seq_num> 12121 WARN EAP: Client didn't provide suitable ciphers for anonymous PAC-provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12121 WARN EAP: Client didn't provide suitable ciphers for anonymous PAC-provisioning, <log details>

- **Message Code:** 12122

  Severity: WARN

  Message Text: Client didn't provide suitable ciphers for authenticated PAC provisioning

  Message Description: The EAP-FAST in-band PAC-provisioning request issued by the client's supplicant internally specified a cipher that is not compatible with the only provisioning method currently allowed by Allowed Protocols configuration: Authenticated In-Band PAC Provisioning. If this is indeed the desired provisioning method, then this message indicates that the supplicant is either configured improperly or that it cannot be used to perform authenticated provisioning with the current version of ISE. Alternatively, if anonymous provisioning is the method actually desired, then this message indicates that Allowed Protocols configuration currently does not allow Anonymous In-Band PAC Provisioning.

  Local Target Message Format: <timestamp> <seq_num> 12122 WARN EAP: Client didn't provide suitable ciphers for authenticated PAC provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12122 WARN EAP: Client didn't provide suitable ciphers for authenticated PAC provisioning, <log details>

- **Message Code:** 12123

  Severity: WARN

  Message Text: Client didn't provide suitable ciphers for either anonymous or authenticated PAC-provisioning

  Message Description: The EAP-FAST in-band PAC-provisioning request issued by the client's supplicant has internally specified a cipher. This cipher is not compatible with either of the two provisioning methods currently allowed by Allowed Protocols configuration: Anonymous In-Band PAC provisioning or Authenticated In-Band PAC provisioning. The supplicant is either configured incorrectly or it cannot be used to perform PAC provisioning with the current version of ISE.

  Local Target Message Format: <timestamp> <seq_num> 12123 WARN EAP: Client didn't provide suitable ciphers for either anonymous or authenticated PAC-provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12123 WARN EAP: Client didn't provide suitable ciphers for either anonymous or authenticated PAC-provisioning, <log details>

- **Message Code:** 12124

  Severity: INFO

  Message Text: EAP-FAST inner method skipped

  Message Description: Skipped the EAP-FAST inner method.

  Local Target Message Format: <timestamp> <seq_num> 12124 INFO EAP: EAP-FAST inner method skipped, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12124 INFO EAP: EAP-FAST inner method skipped, <log details>

- **Message Code:** 12125

  Severity: INFO

  Message Text: EAP-FAST inner method started

  Message Description: Started the EAP-FAST inner method.

  Local Target Message Format: <timestamp> <seq_num> 12125 INFO EAP: EAP-FAST inner method started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12125 INFO EAP: EAP-FAST inner method started, <log details>

- **Message Code:** 12126

  Severity: DEBUG

  Message Text: EAP-FAST cryptobinding verification passed

  Message Description: EAP-FAST cryptobinding verification passed.

  Local Target Message Format: <timestamp> <seq_num> 12126 DEBUG EAP: EAP-FAST cryptobinding verification passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12126 DEBUG EAP: EAP-FAST cryptobinding verification passed, <log details>

- **Message Code:** 12127

  Severity: INFO

  Message Text: Approved EAP-FAST client PAC request

  Message Description: Approved the EAP-FAST request by the client's supplicant to provision a PAC.

  Local Target Message Format: <timestamp> <seq_num> 12127 INFO EAP: Approved EAP-FAST client PAC request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12127 INFO EAP: Approved EAP-FAST client PAC request, <log details>

- **Message Code:** 12128

  Severity: INFO

  Message Text: EAP-FAST inner method finished successfully

  Message Description: EAP-FAST inner method finished successfully.

  Local Target Message Format: <timestamp> <seq_num> 12128 INFO EAP: EAP-FAST inner method finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12128 INFO EAP: EAP-FAST inner method finished successfully, <log details>

- **Message Code:** 12129

  Severity: WARN

  Message Text: EAP-FAST provisioning failed. General error

  Message Description: EAP-FAST provisioning failed. Could not build secure tunnel.

  Local Target Message Format: <timestamp> <seq_num> 12129 WARN EAP: EAP-FAST provisioning failed. General error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12129 WARN EAP: EAP-FAST provisioning failed. General error, <log details>

- **Message Code:** 12130

  Severity: WARN

  Message Text: Failed to decrypt PAC

  Message Description: Failed to decrypt the PAC received from the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12130 WARN EAP: Failed to decrypt PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12130 WARN EAP: Failed to decrypt PAC, <log details>

- **Message Code:** 12131

  Severity: INFO

  Message Text: EAP-FAST built anonymous tunnel for purpose of PAC provisioning

  Message Description: EAP-FAST full handshake finished successfully - built anonymous tunnel for purpose of phase-0 PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num> 12131 INFO EAP: EAP-FAST built anonymous tunnel for purpose of PAC provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12131 INFO EAP: EAP-FAST built anonymous tunnel for purpose of PAC provisioning, <log details>

- **Message Code:** 12132

  Severity: INFO

  Message Text: EAP-FAST built PAC-based tunnel for purpose of authentication

  Message Description: EAP-FAST short handshake finished successfully - built PAC-based tunnel for purpose of phase-1 authentication.

  Local Target Message Format: <timestamp> <seq_num> 12132 INFO EAP: EAP-FAST built PAC-based tunnel for purpose of authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12132 INFO EAP: EAP-FAST built PAC-based tunnel for purpose of authentication, <log details>

- **Message Code:** 12133

  Severity: WARN

  Message Text: Successfully updated Seed key

  Message Description: Successfully updated the Seed key, used for further generation of master keys.

  Local Target Message Format: <timestamp> <seq_num> 12133 WARN EAP: Successfully updated Seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12133 WARN EAP: Successfully updated Seed key, <log details>

- **Message Code:** 12134

  Severity: WARN

  Message Text: Failed to update seed key

  Message Description: Internal error: failed to update seed key, needed for further generation of master keys, most likely because an internal configuration object could not be properly fetched.

  Local Target Message Format: <timestamp> <seq_num> 12134 WARN EAP: Failed to update seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12134 WARN EAP: Failed to update seed key, <log details>

- **Message Code:** 12135

  Severity: INFO

  Message Text: Updated Master Key Generation period

  Message Description: Updated the Master Key Generation period.

  Local Target Message Format: <timestamp> <seq_num> 12135 INFO EAP: Updated Master Key Generation period, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12135 INFO EAP: Updated Master Key Generation period, <log details>

- **Message Code:** 12136

  Severity: INFO

  Message Text: Sent NDAC Authentication to client

  Message Description: Sent NDAC Authentication to client.

  Local Target Message Format: <timestamp> <seq_num> 12136 INFO EAP: Sent NDAC Authentication to client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12136 INFO EAP: Sent NDAC Authentication to client, <log details>

- **Message Code:** 12137

  Severity: INFO

  Message Text: Received NDAC Authentication response from client

  Message Description: Received NDAC Authentication response from client.

  Local Target Message Format: <timestamp> <seq_num> 12137 INFO EAP: Received NDAC Authentication response from client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12137 INFO EAP: Received NDAC Authentication response from client, <log details>

- **Message Code:** 12138

  Severity: INFO

  Message Text: Received Authorization PAC

  Message Description: Received Authorization PAC from client.

  Local Target Message Format: <timestamp> <seq_num> 12138 INFO EAP: Received Authorization PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12138 INFO EAP: Received Authorization PAC, <log details>

- **Message Code:** 12139

  Severity: INFO

  Message Text: Anonymous TLS renegotiation succeeded

  Message Description: EAP-FAST Anonymous TLS renegotiation finished with success

  Local Target Message Format: <timestamp> <seq_num> 12139 INFO EAP: Anonymous TLS renegotiation succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12139 INFO EAP: Anonymous TLS renegotiation succeeded, <log details>

- **Message Code:** 12140

  Severity: WARN

  Message Text: Anonymous TLS renegotiation failed

  Message Description: Anonymous TLS renegotiation failed.

  Local Target Message Format: <timestamp> <seq_num> 12140 WARN EAP: Anonymous TLS renegotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12140 WARN EAP: Anonymous TLS renegotiation failed, <log details>

- **Message Code:** 12141

  Severity: WARN

  Message Text: Failed to find Legacy Master Key

  Message Description: Failed to find EAP-FAST Legacy Master Key.

  Local Target Message Format: <timestamp> <seq_num> 12141 WARN EAP: Failed to find Legacy Master Key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12141 WARN EAP: Failed to find Legacy Master Key, <log details>

- **Message Code:** 12142

  Severity: WARN

  Message Text: Legacy Master Key expired

  Message Description: EAP-FAST Legacy Master Key expired.

  Local Target Message Format: <timestamp> <seq_num> 12142 WARN EAP: Legacy Master Key expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12142 WARN EAP: Legacy Master Key expired, <log details>

- **Message Code:** 12143

  Severity: WARN

  Message Text: Failed to derive EAP-FAST Master Key

  Message Description: Failed to derive EAP-FAST Master Key.

  Local Target Message Format: <timestamp> <seq_num> 12143 WARN EAP: Failed to derive EAP-FAST Master Key, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12143 WARN EAP: Failed to derive EAP-FAST Master Key, <log details>

- **Message Code:** 12144

  Severity: WARN

  Message Text: Fallback on invalid PAC: no available additional cipher configured on server

  Message Description: Fallback on invalid PAC: no available additional cipher configured on server.

  Local Target Message Format: <timestamp> <seq_num> 12144 WARN EAP: Fallback on invalid PAC: no available additional cipher configured on server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12144 WARN EAP: Fallback on invalid PAC: no available additional cipher configured on server, <log details>

- **Message Code:** 12145

  Severity: WARN

  Message Text: Cannot perform more then one invalid PAC fallback

  Message Description: There seems to be an internal problem with the client's supplicant, which is incorrectly trying to send an invalid PAC more then once during a single EAP-FAST conversation.

  Local Target Message Format: <timestamp> <seq_num> 12145 WARN EAP: Cannot perform more then one invalid PAC fallback, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12145 WARN EAP: Cannot perform more then one invalid PAC fallback, <log details>

- **Message Code:** 12146

  Severity: WARN

  Message Text: No cipher on client side for invalid PAC fallback

  Message Description: ISE is unable to complete the TLS handshake, because none of the ciphersuites suggested by the client's supplicant are compatible with invalid PAC fallback. This might be due to the fact that a manually-provisioned PAC is no longer valid, and configuration in Allowed Protocols does not allow any of the forms of in-band PAC provisioning expected by the client.

  Local Target Message Format: <timestamp> <seq_num> 12146 WARN EAP: No cipher on client side for invalid PAC fallback, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12146 WARN EAP: No cipher on client side for invalid PAC fallback, <log details>

- **Message Code:** 12147

  Severity: WARN

  Message Text: Machine Authentication is disabled

  Message Description: EAP-FAST authentication failed because Machine Authentication is disabled.

Local Target Message Format: <timestamp> <seq_num> 12147 WARN EAP: Machine Authentication is disabled, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12147 WARN EAP: Machine Authentication is disabled, <log details>

- **Message Code:** 12148

  Severity: INFO

  Message Text: Allowed Protocols does not allow Stateless Session Resume; performing full authentication

  Message Description: Allowed Protocols configuration does not allow Stateless Session Resume; performing full authentication.

  Local Target Message Format: <timestamp> <seq_num> 12148 INFO EAP: Allowed Protocols does not allow Stateless Session Resume; performing full authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12148 INFO EAP: Allowed Protocols does not allow Stateless Session Resume; performing full authentication, <log details>

- **Message Code:** 12149

  Severity: INFO

  Message Text: EAP-FAST built authenticated tunnel for purpose of PAC provisioning

  Message Description: EAP-FAST full handshake finished successfully - built authenticated tunnel for purpose of phase-0 PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num> 12149 INFO EAP: EAP-FAST built authenticated tunnel for purpose of PAC provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12149 INFO EAP: EAP-FAST built authenticated tunnel for purpose of PAC provisioning, <log details>

- **Message Code:** 12151

  Severity: INFO

  Message Text: Perform fallback on invalid PAC to provisioning

  Message Description: ISE received an invalid PAC during authentication and perform fallback to PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num> 12151 INFO EAP: Perform fallback on invalid PAC to provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12151 INFO EAP: Perform fallback on invalid PAC to provisioning, <log details>

- **Message Code:** 12152

  Severity: WARN

  Message Text: Rejected PAC provisioning request because supplicant failed to adhere to protocol

Message Description: Rejected the PAC provisioning request because the client's supplicant failed to properly adhere to the EAP-FAST protocol. Not only did it fail to send an ACK for the almost-provisioned PAC, but it also failed to properly follow up by sending a valid additional request for a Tunnel PAC or a Machine PAC.

Local Target Message Format: <timestamp> <seq_num> 12152 WARN EAP: Rejected PAC provisioning request because supplicant failed to adhere to protocol, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12152 WARN EAP: Rejected PAC provisioning request because supplicant failed to adhere to protocol, <log details>

- **Message Code:** 12153

  Severity: WARN

  Message Text: EAP-FAST failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Message Description: EAP-FAST failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Local Target Message Format: <timestamp> <seq_num> 12153 WARN EAP: EAP-FAST failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12153 WARN EAP: EAP-FAST failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

- **Message Code:** 12154

  Severity: WARN

  Message Text: EAP-FAST failed SSL/TLS handshake after a client alert

  Message Description: EAP-FAST failed SSL/TLS handshake after a client alert

  Local Target Message Format: <timestamp> <seq_num> 12154 WARN EAP: EAP-FAST failed SSL/TLS handshake after a client alert, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12154 WARN EAP: EAP-FAST failed SSL/TLS handshake after a client alert, <log details>

- **Message Code:** 12155

  Severity: WARN

  Message Text: One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Message Description: One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num> 12155 WARN EAP: One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12155 WARN EAP: One Tunnel PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

- **Message Code:** 12156

  Severity: WARN

  Message Text: One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Message Description: One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num> 12156 WARN EAP: One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12156 WARN EAP: One CTS PAC has already been requested in this conversation. Another Tunnel PAC request will be ignored, <log details>

- **Message Code:** 12157

  Severity: WARN

  Message Text: One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Message Description: One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num> 12157 WARN EAP: One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12157 WARN EAP: One Tunnel PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

- **Message Code:** 12158

  Severity: WARN

  Message Text: One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Message Description: One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num> 12158 WARN EAP: One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12158 WARN EAP: One CTS PAC has already been requested in this conversation. Another CTS PAC request will be ignored, <log details>

- **Message Code:** 12159

  Severity: WARN

  Message Text: One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored

Message Description: One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored

Local Target Message Format: <timestamp> <seq_num> 12159 WARN EAP: One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12159 WARN EAP: One Machine PAC has already been requested in this conversation. Another Machine PAC request will be ignored, <log details>

- **Message Code:** 12160

  Severity: WARN

  Message Text: Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning

  Message Description: Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning

  Local Target Message Format: <timestamp> <seq_num> 12160 WARN EAP: Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12160 WARN EAP: Cannot provision Machine PAC on anonymous provisioning. Machine PAC can be provisioned only on authenticated provisioning, <log details>

- **Message Code:** 12161

  Severity: WARN

  Message Text: Cannot provision Authorization PAC when the stateless session resume is disabled

  Message Description: Cannot provision Authorization PAC when the stateless session resume is disabled. Enable the stateless session resume in service settings to allow Authorization PAC provisioning

  Local Target Message Format: <timestamp> <seq_num> 12161 WARN EAP: Cannot provision Authorization PAC when the stateless session resume is disabled, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12161 WARN EAP: Cannot provision Authorization PAC when the stateless session resume is disabled, <log details>

- **Message Code:** 12162

  Severity: WARN

  Message Text: Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning

  Message Description: Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning

  Local Target Message Format: <timestamp> <seq_num> 12162 WARN EAP: Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12162 WARN EAP: Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning, <log details>

- **Message Code:** 12163

  Severity: WARN

  Message Text: One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored

  Message Description: One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored

  Local Target Message Format: <timestamp> <seq_num> 12163 WARN EAP: One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12163 WARN EAP: One Authorization PAC has already been requested in this conversation. Another Authorization PAC request will be ignored, <log details>

- **Message Code:** 12164

  Severity: WARN

  Message Text: Invalid PAC type requested. Ignoring this request

  Message Description: Invalid PAC type requested. Ignoring this request

  Local Target Message Format: <timestamp> <seq_num> 12164 WARN EAP: Invalid PAC type requested. Ignoring this request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12164 WARN EAP: Invalid PAC type requested. Ignoring this request, <log details>

- **Message Code:** 12165

  Severity: WARN

  Message Text: Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request

  Message Description: Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request

  Local Target Message Format: <timestamp> <seq_num> 12165 WARN EAP: Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12165 WARN EAP: Authorization PAC I-ID does not match user identity. Ignoring this Authorization PAC request, <log details>

- **Message Code:** 12166

  Severity: WARN

Message Text: Machine PAC request does not contain I-ID. Ignoring this Machine PAC request

Message Description: Machine PAC request does not contain I-ID. Ignoring this Machine PAC request

Local Target Message Format: <timestamp> <seq_num> 12166 WARN EAP: Machine PAC request does not contain I-ID. Ignoring this Machine PAC request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12166 WARN EAP: Machine PAC request does not contain I-ID. Ignoring this Machine PAC request, <log details>

- **Message Code:** 12167

  Severity: WARN

  Message Text: Authorization PAC can be provided only with Tunnel PAC

  Message Description: Authorization PAC can be provided only with Tunnel PAC

  Local Target Message Format: <timestamp> <seq_num> 12167 WARN EAP: Authorization PAC can be provided only with Tunnel PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12167 WARN EAP: Authorization PAC can be provided only with Tunnel PAC, <log details>

- **Message Code:** 12168

  Severity: INFO

  Message Text: Received CTS PAC

  Message Description: Received CTS PAC from client

  Local Target Message Format: <timestamp> <seq_num> 12168 INFO EAP: Received CTS PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12168 INFO EAP: Received CTS PAC, <log details>

- **Message Code:** 12169

  Severity: INFO

  Message Text: Successfully finished EAP-FAST tunnel PAC provisioning/update

  Message Description: Successfully finished the EAP-FAST tunnel PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num> 12169 INFO EAP: Successfully finished EAP-FAST tunnel PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12169 INFO EAP: Successfully finished EAP-FAST tunnel PAC provisioning/update, <log details>

- **Message Code:** 12170

  Severity: INFO

  Message Text: Successfully finished EAP-FAST machine PAC provisioning/update

Message Description: Successfully finished the EAP-FAST machine PAC provisioning or update.

Local Target Message Format: <timestamp> <seq_num> 12170 INFO EAP: Successfully finished EAP-FAST machine PAC provisioning/update, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12170 INFO EAP: Successfully finished EAP-FAST machine PAC provisioning/update, <log details>

- **Message Code:** 12171

  Severity: INFO

  Message Text: Successfully finished EAP-FAST user authorization PAC provisioning/update

  Message Description: Successfully finished the EAP-FAST user authorization PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num> 12171 INFO EAP: Successfully finished EAP-FAST user authorization PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12171 INFO EAP: Successfully finished EAP-FAST user authorization PAC provisioning/update, <log details>

- **Message Code:** 12172

  Severity: INFO

  Message Text: Successfully finished EAP-FAST posture PAC provisioning/update

  Message Description: Successfully finished the EAP-FAST posture PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num> 12172 INFO EAP: Successfully finished EAP-FAST posture PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12172 INFO EAP: Successfully finished EAP-FAST posture PAC provisioning/update, <log details>

- **Message Code:** 12173

  Severity: INFO

  Message Text: Successfully finished EAP-FAST CTS PAC provisioning/update

  Message Description: Successfully finished the EAP-FAST CTS PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num> 12173 INFO EAP: Successfully finished EAP-FAST CTS PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12173 INFO EAP: Successfully finished EAP-FAST CTS PAC provisioning/update, <log details>

- **Message Code:** 12174

  Severity: INFO

  Message Text: Received Machine PAC

Message Description: Received Machine PAC from client.

Local Target Message Format: <timestamp> <seq_num> 12174 INFO EAP: Received Machine PAC, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12174 INFO EAP: Received Machine PAC, <log details>

- **Message Code:** 12175

  Severity: INFO

  Message Text: Received Tunnel PAC

  Message Description: Received Tunnel PAC from client.

  Local Target Message Format: <timestamp> <seq_num> 12175 INFO EAP: Received Tunnel PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12175 INFO EAP: Received Tunnel PAC, <log details>

- **Message Code:** 12176

  Severity: INFO

  Message Text: EAP-FAST PAC-less full handshake finished successfully

  Message Description: Using the PAC-less mode of EAP-FAST authentication. The tunnel was successfully built using full handshake.

  Local Target Message Format: <timestamp> <seq_num> 12176 INFO EAP: EAP-FAST PAC-less full handshake finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12176 INFO EAP: EAP-FAST PAC-less full handshake finished successfully, <log details>

- **Message Code:** 12177

  Severity: WARN

  Message Text: No cipher for PAC-less EAP-FAST authentication

  Message Description: The cipher specified by the client's supplicant during the TLS handshake portion of EAP-FAST is not compatible with the PAC-less mode of operation currently configured in Allowed protocols configuration. This could be because the supplicant is either incorrectly configured, or even inherently unable in general, to work with PAC-less EAP-FAST authentication using the current version of ISE.

  Local Target Message Format: <timestamp> <seq_num> 12177 WARN EAP: No cipher for PAC-less EAP-FAST authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12177 WARN EAP: No cipher for PAC-less EAP-FAST authentication, <log details>

- **Message Code:** 12178

Severity: WARN

Message Text: Rejected PAC unexpectedly received during PAC-less mode of EAP-FAST

Message Description: Despite the fact that Allowed protocols has configured EAP-FAST to use the PAC-less mode of operation, the client's supplicant has sent a PAC to ISE, as if the PAC-based mode is being used.

Local Target Message Format: <timestamp> <seq_num> 12178 WARN EAP: Rejected PAC unexpectedly received during PAC-less mode of EAP-FAST, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12178 WARN EAP: Rejected PAC unexpectedly received during PAC-less mode of EAP-FAST, <log details>

- **Message Code:** 12179

  Severity: INFO

  Message Text: Successfully finished EAP-FAST machine authorization PAC provisioning/update

  Message Description: Successfully finished the EAP-FAST machine authorization PAC provisioning or update.

  Local Target Message Format: <timestamp> <seq_num> 12179 INFO EAP: Successfully finished EAP-FAST machine authorization PAC provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12179 INFO EAP: Successfully finished EAP-FAST machine authorization PAC provisioning/update, <log details>

- **Message Code:** 12200

  Severity: INFO

  Message Text: Approved EAP-FAST client Tunnel PAC request

  Message Description: Approved the EAP-FAST request by the client's supplicant to provision a Tunnel PAC.

  Local Target Message Format: <timestamp> <seq_num> 12200 INFO EAP: Approved EAP-FAST client Tunnel PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12200 INFO EAP: Approved EAP-FAST client Tunnel PAC request, <log details>

- **Message Code:** 12201

  Severity: INFO

  Message Text: Approved EAP-FAST client Machine PAC request

  Message Description: Approved the EAP-FAST request by the client's supplicant to provision a Machine PAC.

  Local Target Message Format: <timestamp> <seq_num> 12201 INFO EAP: Approved EAP-FAST client Machine PAC request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12201 INFO EAP: Approved EAP-FAST client Machine PAC request, <log details>

- **Message Code:** 12202

  Severity: INFO

  Message Text: Approved EAP-FAST client Authorization PAC request

  Message Description: Approved the EAP-FAST request by the client's supplicant to provision an Authorization PAC.

  Local Target Message Format: <timestamp> <seq_num> 12202 INFO EAP: Approved EAP-FAST client Authorization PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12202 INFO EAP: Approved EAP-FAST client Authorization PAC request, <log details>

- **Message Code:** 12203

  Severity: INFO

  Message Text: Using client certificate for authentication

  Message Description: ISE received client certificate during tunnel establishment or inside the tunnel. ISE is going to verify this certificate and use it for authentication.

  Local Target Message Format: <timestamp> <seq_num> 12203 INFO EAP: Using client certificate for authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12203 INFO EAP: Using client certificate for authentication, <log details>

- **Message Code:** 12204

  Severity: INFO

  Message Text: Client certificate was received inside the tunnel

  Message Description: The supplicant provided client certificate inside the tunnel (certificate was send encrypted)

  Local Target Message Format: <timestamp> <seq_num> 12204 INFO EAP: Client certificate was received inside the tunnel, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12204 INFO EAP: Client certificate was received inside the tunnel, <log details>

- **Message Code:** 12205

  Severity: INFO

  Message Text: Client certificate was requested but not received inside the tunnel. Will continue with inner method.

Message Description: ISE requested client certificate inside the tunnel but the supplicant has not provided the client certificate. ISE will continue authenticating the supplicant by running the inner method.

Local Target Message Format: <timestamp> <seq_num> 12205 INFO EAP: Client certificate was requested but not received inside the tunnel. Will continue with inner method., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12205 INFO EAP: Client certificate was requested but not received inside the tunnel. Will continue with inner method., <log details>

- **Message Code:** 12206

  Severity: INFO

  Message Text: Client certificate was received during tunnel establishment

  Message Description: The supplicant provided a client certificate during tunnel establishment (certificate was sent not encrypted)

  Local Target Message Format: <timestamp> <seq_num> 12206 INFO EAP: Client certificate was received during tunnel establishment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12206 INFO EAP: Client certificate was received during tunnel establishment, <log details>

- **Message Code:** 12207

  Severity: INFO

  Message Text: Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel.

  Message Description: ISE requested client certificate during tunnel establishment but the supplicant did not provided the client certificate. The supplicant may be configured to not send the client certificte unless encrypted. ISE will renegotiate and request the client certificate inside the tunnel.

  Local Target Message Format: <timestamp> <seq_num> 12207 INFO EAP: Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12207 INFO EAP: Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel., <log details>

- **Message Code:** 12208

  Severity: INFO

  Message Text: Client certificate was received but authentication failed

  Message Description: ISE received client certificate during tunnel establishment or inside the tunnel but the authentication failed.

  Local Target Message Format: <timestamp> <seq_num> 12208 INFO EAP: Client certificate was received but authentication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12208 INFO EAP: Client certificate was received but authentication failed, <log details>

- **Message Code:** 12209

  Severity: INFO

  Message Text: Starting EAP chaining

  Message Description: ISE is configured to perform EAP chaining. ISE is starting EAP chanining and assume that client also supports EAP chaining.

  Local Target Message Format: <timestamp> <seq_num> 12209 INFO EAP: Starting EAP chaining, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12209 INFO EAP: Starting EAP chaining, <log details>

- **Message Code:** 12210

  Severity: INFO

  Message Text: Received User Authorization PAC

  Message Description: Received User Authorization PAC from client.

  Local Target Message Format: <timestamp> <seq_num> 12210 INFO EAP: Received User Authorization PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12210 INFO EAP: Received User Authorization PAC, <log details>

- **Message Code:** 12211

  Severity: INFO

  Message Text: Received Machine Authorization PAC

  Message Description: Received Machine Authorization PAC from client.

  Local Target Message Format: <timestamp> <seq_num> 12211 INFO EAP: Received Machine Authorization PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12211 INFO EAP: Received Machine Authorization PAC, <log details>

- **Message Code:** 12212

  Severity: INFO

  Message Text: Identity type provided by client is equal to requested

  Message Description: ISE requested a specific identity type from the client for current inner method and the client confirmed usage of this identity type.

  Local Target Message Format: <timestamp> <seq_num> 12212 INFO EAP: Identity type provided by client is equal to requested, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12212 INFO EAP: Identity type provided by client is equal to requested, <log details>

- **Message Code:** 12213

  Severity: INFO

  Message Text: Identity type provided by client is not equal to requested type

  Message Description: ISE requested a specific identity type from the client for the current inner method and the client denied usage of this identity type.

  Local Target Message Format: <timestamp> <seq_num> 12213 INFO EAP: Identity type provided by client is not equal to requested type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12213 INFO EAP: Identity type provided by client is not equal to requested type, <log details>

- **Message Code:** 12214

  Severity: INFO

  Message Text: Client suggested 'User' identity type instead

  Message Description: Client sugested using the identity type 'User' in the current inner method.

  Local Target Message Format: <timestamp> <seq_num> 12214 INFO EAP: Client suggested 'User' identity type instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12214 INFO EAP: Client suggested 'User' identity type instead, <log details>

- **Message Code:** 12215

  Severity: INFO

  Message Text: Client suggested 'Machine' identity type instead

  Message Description: Client sugested using the identity type 'Machine' in the current inner method.

  Local Target Message Format: <timestamp> <seq_num> 12215 INFO EAP: Client suggested 'Machine' identity type instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12215 INFO EAP: Client suggested 'Machine' identity type instead, <log details>

- **Message Code:** 12216

  Severity: INFO

  Message Text: Identity type provided by client was already used for authentication

  Message Description: Client sugested to use an identity type in the current inner method that was already used in a previous inner method. ISE is rejecting this identity type.

  Local Target Message Format: <timestamp> <seq_num> 12216 INFO EAP: Identity type provided by client was already used for authentication, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12216 INFO EAP: Identity type provided by client was already used for authentication, <log details>

- **Message Code:** 12217

  Severity: INFO

  Message Text: Identity type provided by client is currently unsupported

  Message Description: Client sugested using an identity type in current inner method that is not supported by ISE. ISE is rejecting this identity type.

  Local Target Message Format: <timestamp> <seq_num> 12217 INFO EAP: Identity type provided by client is currently unsupported, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12217 INFO EAP: Identity type provided by client is currently unsupported, <log details>

- **Message Code:** 12218

  Severity: INFO

  Message Text: Selected identity type 'User'

  Message Description: ISE selected identity type 'User' to use in current inner method.

  Local Target Message Format: <timestamp> <seq_num> 12218 INFO EAP: Selected identity type 'User', <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12218 INFO EAP: Selected identity type 'User', <log details>

- **Message Code:** 12219

  Severity: INFO

  Message Text: Selected identity type 'Machine'

  Message Description: ISE selected identity type 'Machine' to use in current inner method.

  Local Target Message Format: <timestamp> <seq_num> 12219 INFO EAP: Selected identity type 'Machine', <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12219 INFO EAP: Selected identity type 'Machine', <log details>

- **Message Code:** 12220

  Severity: INFO

  Message Text: Client does not support EAP chaining. Switching to usual mode

  Message Description: ISE send Identity Type TLV in EAP request to client to conduct EP chaining. However Identity Type TLV is not present in client response. So EAP chaining is not supported by the client. ISE is switching to usual mode.

Local Target Message Format: <timestamp> <seq_num> 12220 INFO EAP: Client does not support EAP chaining. Switching to usual mode, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12220 INFO EAP: Client does not support EAP chaining. Switching to usual mode, <log details>

- **Message Code:** 12221

  Severity: INFO

  Message Text: Client does not support TLS renegotiation. Will continue with inner method

  Message Description: ISE tried to renegotiate handshake to ask for client certificate inside the tunnel but client does not support TLS renegotiation

  Local Target Message Format: <timestamp> <seq_num> 12221 INFO EAP: Client does not support TLS renegotiation. Will continue with inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12221 INFO EAP: Client does not support TLS renegotiation. Will continue with inner method, <log details>

- **Message Code:** 12222

  Severity: INFO

  Message Text: EAP-FAST PAC-less session resumed successfully

  Message Description: Using the PAC-less mode of EAP-FAST authentication. The tunnel was successfully built using short handshake.

  Local Target Message Format: <timestamp> <seq_num> 12222 INFO EAP: EAP-FAST PAC-less session resumed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12222 INFO EAP: EAP-FAST PAC-less session resumed successfully, <log details>

- **Message Code:** 12223

  Severity: INFO

  Message Text: Ignore PAC send by supplicant during fallback to provisioning conversation

  Message Description: ISE performed fallback on invalid PAC to provisioning. However during this provisioning conversation supplicant sent the PAC again. ISE will ignore this PAC.

  Local Target Message Format: <timestamp> <seq_num> 12223 INFO EAP: Ignore PAC send by supplicant during fallback to provisioning conversation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12223 INFO EAP: Ignore PAC send by supplicant during fallback to provisioning conversation, <log details>

- **Message Code:** 12224

  Severity: INFO

Message Text: User Authorization PAC request ignored because PAC of the same type was already used to skip inner method

Message Description: User Authorization PAC request ignored because PAC of the same type was already used to skip inner method. Authorization PAC could be provided only after full authentication conversation.

Local Target Message Format: <timestamp> <seq_num> 12224 INFO EAP: User Authorization PAC request ignored because PAC of the same type was already used to skip inner method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12224 INFO EAP: User Authorization PAC request ignored because PAC of the same type was already used to skip inner method, <log details>

- **Message Code:** 12225

  Severity: INFO

  Message Text: Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method

  Message Description: Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method. Authorization PAC could be provided only after full authentication conversation.

  Local Target Message Format: <timestamp> <seq_num> 12225 INFO EAP: Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12225 INFO EAP: Ignore Machine Authorization PAC request because of current PAC of the same type was used to skip inner method, <log details>

- **Message Code:** 12226

  Severity: INFO

  Message Text: Started renegotiated TLS handshake

  Message Description: ISE preformed TLS renegotiation and started another TLS handshake.

  Local Target Message Format: <timestamp> <seq_num> 12226 INFO EAP: Started renegotiated TLS handshake, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12226 INFO EAP: Started renegotiated TLS handshake, <log details>

- **Message Code:** 12227

  Severity: INFO

  Message Text: User Authorization PAC has expired - will run inner method

  Message Description: Received from the client User Authorization PAC that has expired. Expired Authorization PAC cannot be used for fast reconnect so ISE will run inner method to authenticate the user.

Local Target Message Format: <timestamp> <seq_num> 12227 INFO EAP: User Authorization PAC has expired - will run inner method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12227 INFO EAP: User Authorization PAC has expired - will run inner method, <log details>

- **Message Code:** 12228

  Severity: INFO

  Message Text: Machine Authorization PAC has expired - will run inner method

  Message Description: Received from the client Machine Authorization PAC that has expired. Expired Authorization PAC cannot be used for fast reconnect so ISE will run inner method to authenticate the machine.

  Local Target Message Format: <timestamp> <seq_num> 12228 INFO EAP: Machine Authorization PAC has expired - will run inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12228 INFO EAP: Machine Authorization PAC has expired - will run inner method, <log details>

- **Message Code:** 12229

  Severity: WARN

  Message Text: No valid PAC requests on provisioning

  Message Description: Client did not send valid PAC request at the end of EAP-FAST provisioning conversation. Provisioning conversation should always finish with sending requested one or more PACs to the client. Legacy client may not ask for specific PAC since in initial draft of EAP-FAST protocol there was only one PAC type and it was unnecessary to specify it. ISE provides legacy Tunnel V1 PAC in such case. More advanced client may reequest several PAC types but they need to conform certain rules. For example, ISE cannot provide User Authorization PAC if Tunnel PAC was not requested.

  Local Target Message Format: <timestamp> <seq_num> 12229 WARN EAP: No valid PAC requests on provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12229 WARN EAP: No valid PAC requests on provisioning, <log details>

- **Message Code:** 12230

  Severity: INFO

  Message Text: Ignore any PAC requests in PAC-less mode

  Message Description: ISE ignores any PAC requests when it is configured for PAC-less mode

  Local Target Message Format: <timestamp> <seq_num> 12230 INFO EAP: Ignore any PAC requests in PAC-less mode, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12230 INFO EAP: Ignore any PAC requests in PAC-less mode, <log details>

- **Message Code:** 12231

  Severity: INFO

  Message Text: Ignore Machine Authorization PAC request when there is no EAP chaining

  Message Description: ISE ignores Machine Authorization PAC request when there is no EAP chaining happens in the conversation. Machine Authorization PAC can be provided only during EAP chaining conversation. Note that EAP chaining can be configured in ISE but disabled or not supported in client so the conversation was conducted in no chaining mode.

  Local Target Message Format: <timestamp> <seq_num> 12231 INFO EAP: Ignore Machine Authorization PAC request when there is no EAP chaining, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12231 INFO EAP: Ignore Machine Authorization PAC request when there is no EAP chaining, <log details>

- **Message Code:** 12232

  Severity: WARN

  Message Text: Cannot decrypt PAC because of specified master key was not found - rejecting the PAC

  Message Description: Received from the client a PAC that cannot be decrypted because of specified master key was not found. Rejecting it.

  Local Target Message Format: <timestamp> <seq_num> 12232 WARN EAP: Cannot decrypt PAC because of specified master key was not found - rejecting the PAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12232 WARN EAP: Cannot decrypt PAC because of specified master key was not found - rejecting the PAC, <log details>

- **Message Code:** 12233

  Severity: INFO

  Message Text: Cisco IP Phone detected. Turn EAP chaining off

  Message Description: Turn EAP chaining off for Cisco IP Phone authentication

  Local Target Message Format: <timestamp> <seq_num> 12233 INFO EAP: Cisco IP Phone detected. Turn EAP chaining off, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12233 INFO EAP: Cisco IP Phone detected. Turn EAP chaining off, <log details>

- **Message Code:** 12234

  Severity: INFO

  Message Text: Client is detected as Cisco IP Phone

  Message Description: Client is detected as Cisco IP Phone

  Local Target Message Format: <timestamp> <seq_num> 12234 INFO EAP: Client is detected as Cisco IP Phone, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12234 INFO EAP: Client is detected as Cisco IP Phone, <log details>

- **Message Code:** 12235

  Severity: WARN

  Message Text: Unexpectedly received empty TLS message during EAP-FAST handshake; treating as a rejection by the client

  Message Description: While trying to negotiate a TLS handshake with the client inside the EAP-FAST tunnel, ISE expected to receive a non-empty TLS message or TLS alert message, but instead received an empty TLS message. This could be due to an inconformity in the implementation of the protocol between ISE and the supplicant. ISE treated the unexpected message as a sign that the client rejected the tunnel renegotiation.

  Local Target Message Format: <timestamp> <seq_num> 12235 WARN EAP: Unexpectedly received empty TLS message during EAP-FAST handshake; treating as a rejection by the client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12235 WARN EAP: Unexpectedly received empty TLS message during EAP-FAST handshake; treating as a rejection by the client, <log details>

- **Message Code:** 12236

  Severity: WARN

  Message Text: Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request

  Message Description: Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request

  Local Target Message Format: <timestamp> <seq_num> 12236 WARN EAP: Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12236 WARN EAP: Machine Authorization PAC I-ID does not match user identity. Ignoring this Machine Authorization PAC request, <log details>

- **Message Code:** 12237

  Severity: INFO

  Message Text: PAC-less request

  Message Description: PAC-less request by the client's supplicant to bypass PAC.

  Local Target Message Format: <timestamp> <seq_num>EAP PAC-less request INFO PAC-less request by the client's supplicant to bypass PAC., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP PAC-less request INFO PAC-less request by the client's supplicant to bypass PAC., <log details>

- **Message Code:** 12238

Severity: INFO

Message Text: Successfully processed PAC-less

Message Description: Successfully processed PAC-less

Local Target Message Format: <timestamp> <seq_num>EAP Successfully processed PAC-less INFO Successfully processed PAC-less, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Successfully processed PAC-less INFO Successfully processed PAC-less, <log details>

- **Message Code:** 12239

  Severity: INFO

  Message Text: Prepared RADIUS Access-Reject after PAC-less provisioning.

  Message Description: As part of the standard PAC provisioning behavior, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC-less request was successfully approved. This admittedly-misleading result value is nevertheless normal, does not truly imply a failure, and can/should be safely ignored.

  Local Target Message Format: <timestamp> <seq_num>EAP Prepared RADIUS Access-Reject after PAC-less provisioning. INFO As part of the standard PAC provisioning behavior, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC-less request was successfully approved. This admittedly-misleading result value is nevertheless normal, does not truly imply a failure, and can/should be safely ignored., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Prepared RADIUS Access-Reject after PAC-less provisioning. INFO As part of the standard PAC provisioning behavior, a result of EAP-Failure and RADIUS Access-Reject will be returned, even when the PAC-less request was successfully approved. This admittedly-misleading result value is nevertheless normal, does not truly imply a failure, and can/should be safely ignored., <log details>

- **Message Code:** 12240

  Severity: WARN

  Message Text: PAC-less CTS DeviceID not found from the source IP

  Message Description: PAC-less CTS DeviceID not found from the source IP

  Local Target Message Format: <timestamp> <seq_num>12240 WARN EAP PAC-less CTS DeviceID not found from the source IP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12240 WARN EAP PAC-less CTS DeviceID not found from the source IP, <log details>

- **Message Code:** 12300

  Severity: INFO

  Message Text: Prepared EAP-Request proposing PEAP with challenge

Message Description: Created an EAP-Request packet proposing to use the PEAP protocol, and also providing a PEAP challenge, for attachment to a RADIUS message. The PEAP protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num> 12300 INFO EAP: Prepared EAP-Request proposing PEAP with challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12300 INFO EAP: Prepared EAP-Request proposing PEAP with challenge, <log details>

- **Message Code:** 12301

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use PEAP instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12301 INFO EAP: Extracted EAP-Response/NAK requesting to use PEAP instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12301 INFO EAP: Extracted EAP-Response/NAK requesting to use PEAP instead, <log details>

- **Message Code:** 12302

  Severity: INFO

  Message Text: Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing a PEAP challenge-response, and accepting PEAP as negotiated.

  Local Target Message Format: <timestamp> <seq_num> 12302 INFO EAP: Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12302 INFO EAP: Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated, <log details>

- **Message Code:** 12303

  Severity: WARN

  Message Text: Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12303 WARN EAP: Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12303 WARN EAP: Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12304

  Severity: INFO

  Message Text: Extracted EAP-Response containing PEAP challenge-response

  Message Description: Continuing the PEAP protocol; processing the PEAP challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12304 INFO EAP: Extracted EAP-Response containing PEAP challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12304 INFO EAP: Extracted EAP-Response containing PEAP challenge-response, <log details>

- **Message Code:** 12305

  Severity: INFO

  Message Text: Prepared EAP-Request with another PEAP challenge

  Message Description: As part of the continuation of the PEAP protocol, created an EAP-Request packet containing another PEAP challenge, for attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12305 INFO EAP: Prepared EAP-Request with another PEAP challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12305 INFO EAP: Prepared EAP-Request with another PEAP challenge, <log details>

- **Message Code:** 12306

  Severity: INFO

  Message Text: PEAP authentication succeeded

  Message Description: PEAP authentication succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12306 INFO EAP: PEAP authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12306 INFO EAP: PEAP authentication succeeded, <log details>

- **Message Code:** 12307

  Severity: INFO

  Message Text: PEAP authentication failed

  Message Description: PEAP authentication failed.

  Local Target Message Format: <timestamp> <seq_num> 12307 INFO EAP: PEAP authentication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12307 INFO EAP: PEAP authentication failed, <log details>

- **Message Code:** 12308

  Severity: WARN

  Message Text: Client sent Result TLV indicating failure

  Message Description: Internal error, possibly in the supplicant: PEAP v0 authentication failed because client sent Result TLV indicating failure. Client indicates that it does not support Crypto-Binding TLV

  Local Target Message Format: <timestamp> <seq_num> 12308 WARN EAP: Client sent Result TLV indicating failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12308 WARN EAP: Client sent Result TLV indicating failure, <log details>

- **Message Code:** 12309

  Severity: WARN

  Message Text: PEAP handshake failed

  Message Description: PEAP handshake failed.

  Local Target Message Format: <timestamp> <seq_num> 12309 WARN EAP: PEAP handshake failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12309 WARN EAP: PEAP handshake failed, <log details>

- **Message Code:** 12310

  Severity: INFO

  Message Text: PEAP full handshake finished successfully

  Message Description: PEAP full handshake finished successfully.

  Local Target Message Format: <timestamp> <seq_num> 12310 INFO EAP: PEAP full handshake finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12310 INFO EAP: PEAP full handshake finished successfully, <log details>

- **Message Code:** 12311

  Severity: INFO

  Message Text: PEAP session resumed successfully

  Message Description: PEAP short handshake finished successfully - resumed previous session.

  Local Target Message Format: <timestamp> <seq_num> 12311 INFO EAP: PEAP session resumed successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12311 INFO EAP: PEAP session resumed successfully, <log details>

- **Message Code:** 12312

  Severity: INFO

  Message Text: PEAP fast-reconnect - skipping inner method

  Message Description: PEAP fast-reconnect - skipping inner method.

  Local Target Message Format: <timestamp> <seq_num> 12312 INFO EAP: PEAP fast-reconnect - skipping inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12312 INFO EAP: PEAP fast-reconnect - skipping inner method, <log details>

- **Message Code:** 12313

  Severity: INFO

  Message Text: PEAP inner method started

  Message Description: Started the PEAP inner method.

  Local Target Message Format: <timestamp> <seq_num> 12313 INFO EAP: PEAP inner method started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12313 INFO EAP: PEAP inner method started, <log details>

- **Message Code:** 12314

  Severity: INFO

  Message Text: PEAP inner method finished successfully

  Message Description: PEAP inner method finished successfully.

  Local Target Message Format: <timestamp> <seq_num> 12314 INFO EAP: PEAP inner method finished successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12314 INFO EAP: PEAP inner method finished successfully, <log details>

- **Message Code:** 12315

  Severity: INFO

  Message Text: PEAP inner method finished with failure

  Message Description: PEAP inner method finished with failure.

  Local Target Message Format: <timestamp> <seq_num> 12315 INFO EAP: PEAP inner method finished with failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12315 INFO EAP: PEAP inner method finished with failure, <log details>

- **Message Code:** 12316

  Severity: WARN

  Message Text: PEAP version negotiation failed

  Message Description: PEAP version negotiation failed, apparently because the supplicant supports neither v0 nor v1.

  Local Target Message Format: <timestamp> <seq_num> 12316 WARN EAP: PEAP version negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12316 WARN EAP: PEAP version negotiation failed, <log details>

- **Message Code:** 12317

  Severity: INFO

  Message Text: PEAP fast-reconnect failed; starting inner method

  Message Description: PEAP fast-reconnect failed, possibly due to internal caching-related issues, or to the possibility that the inner method used in the previous authentication is no longer enabled for PEAP. ISE needs to conduct the full PEAP authentication when fast reconnect is enabled in PEAP settings. Starting inner method.

  Local Target Message Format: <timestamp> <seq_num> 12317 INFO EAP: PEAP fast-reconnect failed; starting inner method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12317 INFO EAP: PEAP fast-reconnect failed; starting inner method, <log details>

- **Message Code:** 12318

  Severity: INFO

  Message Text: Successfully negotiated PEAP version 0

  Message Description: Successfully negotiated PEAP version 0.

  Local Target Message Format: <timestamp> <seq_num> 12318 INFO EAP: Successfully negotiated PEAP version 0, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12318 INFO EAP: Successfully negotiated PEAP version 0, <log details>

- **Message Code:** 12319

  Severity: INFO

  Message Text: Successfully negotiated PEAP version 1

  Message Description: Successfully negotiated PEAP version 1.

Local Target Message Format: <timestamp> <seq_num> 12319 INFO EAP: Successfully negotiated PEAP version 1, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12319 INFO EAP: Successfully negotiated PEAP version 1, <log details>

- **Message Code:** 12320

  Severity: WARN

  Message Text: Client failed to acknowledge receipt of success or failure result

  Message Description: Internal error, possibly in the supplicant: PEAP v1 authentication failed because client failed to acknowledge receipt of success or failure result.

  Local Target Message Format: <timestamp> <seq_num> 12320 WARN EAP: Client failed to acknowledge receipt of success or failure result, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12320 WARN EAP: Client failed to acknowledge receipt of success or failure result, <log details>

- **Message Code:** 12321

  Severity: WARN

  Message Text: PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Message Description: PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Local Target Message Format: <timestamp> <seq_num> 12321 WARN EAP: PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12321 WARN EAP: PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

- **Message Code:** 12322

  Severity: WARN

  Message Text: PEAP failed SSL/TLS handshake after a client alert

  Message Description: PEAP failed SSL/TLS handshake after a client alert

  Local Target Message Format: <timestamp> <seq_num> 12322 WARN EAP: PEAP failed SSL/TLS handshake after a client alert, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12322 WARN EAP: PEAP failed SSL/TLS handshake after a client alert, <log details>

- **Message Code:** 12323

  Severity: WARN

  Message Text: PEAP cryptobinding verification failed

  Message Description: PEAP cryptobinding verification failed.

Local Target Message Format: <timestamp> <seq_num> 12323 WARN EAP: PEAP cryptobinding verification failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12323 WARN EAP: PEAP cryptobinding verification failed, <log details>

- **Message Code:** 12324

  Severity: DEBUG

  Message Text: PEAP cryptobinding verification passed

  Message Description: PEAP cryptobinding verification passed.

  Local Target Message Format: <timestamp> <seq_num> 12324 DEBUG EAP: PEAP cryptobinding verification passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12324 DEBUG EAP: PEAP cryptobinding verification passed, <log details>

- **Message Code:** 12500

  Severity: INFO

  Message Text: Prepared EAP-Request proposing EAP-TLS with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-TLS protocol, and also providing an EAP-TLS challenge, for attachment to a RADIUS message. The TLS protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12500 INFO EAP: Prepared EAP-Request proposing EAP-TLS with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12500 INFO EAP: Prepared EAP-Request proposing EAP-TLS with challenge, <log details>

- **Message Code:** 12501

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use EAP-TLS instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-TLS instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12501 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-TLS instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12501 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-TLS instead, <log details>

- **Message Code:** 12502

  Severity: INFO

Message Text: Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated

Message Description: Extracted from the RADIUS message an EAP-Response packet containing an EAP-TLS challenge-response, and accepting EAP-TLS as negotiated

Local Target Message Format: <timestamp> <seq_num> 12502 INFO EAP: Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12502 INFO EAP: Extracted EAP-Response containing EAP-TLS challenge-response and accepting EAP-TLS as negotiated, <log details>

- **Message Code:** 12503

  Severity: WARN

  Message Text: Failed to negotiate EAP because EAP-TLS not enabled in Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-TLS instead. However, EAP-TLS is not allowed in the Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12503 WARN EAP: Failed to negotiate EAP because EAP-TLS not enabled in Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12503 WARN EAP: Failed to negotiate EAP because EAP-TLS not enabled in Allowed Protocols, <log details>

- **Message Code:** 12504

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-TLS challenge-response

  Message Description: Continuing the EAP-TLS protocol; processing the EAP-TLS challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12504 INFO EAP: Extracted EAP-Response containing EAP-TLS challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12504 INFO EAP: Extracted EAP-Response containing EAP-TLS challenge-response, <log details>

- **Message Code:** 12505

  Severity: INFO

  Message Text: Prepared EAP-Request with another EAP-TLS challenge

  Message Description: As part of the continuation of the EAP-TLS protocol, created an EAP-Request packet containing another EAP-TLS challenge, for attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12505 INFO EAP: Prepared EAP-Request with another EAP-TLS challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12505 INFO EAP: Prepared EAP-Request with another EAP-TLS challenge, <log details>

- **Message Code:** 12506

  Severity: INFO

  Message Text: EAP-TLS authentication succeeded

  Message Description: EAP-TLS authentication succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12506 INFO EAP: EAP-TLS authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12506 INFO EAP: EAP-TLS authentication succeeded, <log details>

- **Message Code:** 12507

  Severity: INFO

  Message Text: EAP-TLS authentication failed

  Message Description: EAP-TLS authentication failed.

  Local Target Message Format: <timestamp> <seq_num> 12507 INFO EAP: EAP-TLS authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12507 INFO EAP: EAP-TLS authentication failed, <log details>

- **Message Code:** 12508

  Severity: WARN

  Message Text: EAP-TLS handshake failed

  Message Description: EAP-TLS handshake failed.

  Local Target Message Format: <timestamp> <seq_num> 12508 WARN EAP: EAP-TLS handshake failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12508 WARN EAP: EAP-TLS handshake failed, <log details>

- **Message Code:** 12509

  Severity: INFO

  Message Text: EAP-TLS full handshake finished successfully

  Message Description: EAP-TLS full handshake finished successfully.

  Local Target Message Format: <timestamp> <seq_num> 12509 INFO EAP: EAP-TLS full handshake finished successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12509 INFO EAP: EAP-TLS full handshake finished successfully, <log details>

- **Message Code:** 12510

  Severity: INFO

  Message Text: EAP-TLS session resumed successfully

  Message Description: EAP-TLS short handshake finished successfully - resumed previous session.

  Local Target Message Format: <timestamp> <seq_num> 12510 INFO EAP: EAP-TLS session resumed successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12510 INFO EAP: EAP-TLS session resumed successfully, <log details>

- **Message Code:** 12511

  Severity: WARN

  Message Text: Unexpectedly received TLS alert message; treating as a rejection by the client

  Message Description: While trying to negotiate a TLS handshake with the client, ISE received an unexpected TLS alert message. This might be due to the supplicant not trusting the ISE server certificate for some reason. ISE treated the unexpected message as a sign that the client rejected the tunnel establishment.

  Local Target Message Format: <timestamp> <seq_num> 12511 WARN EAP: Unexpectedly received TLS alert message; treating as a rejection by the client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12511 WARN EAP: Unexpectedly received TLS alert message; treating as a rejection by the client, <log details>

- **Message Code:** 12512

  Severity: WARN

  Message Text: Treat the unexpected TLS acknowledge message as a rejection from the client

  Message Description: Treat the unexpected TLS acknowledge message during tunnel building as a rejection from the client

  Local Target Message Format: <timestamp> <seq_num> 12512 WARN EAP: Treat the unexpected TLS acknowledge message as a rejection from the client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12512 WARN EAP: Treat the unexpected TLS acknowledge message as a rejection from the client, <log details>

- **Message Code:** 12513

  Severity: WARN

  Message Text: Could not establish the EAP TLS SSL session

  Message Description: Could not establish the EAP TLS SSL session

Local Target Message Format: <timestamp> <seq_num> 12513 WARN EAP: Could not establish the EAP TLS SSL session, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12513 WARN EAP: Could not establish the EAP TLS SSL session, <log details>

- **Message Code:** 12514

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

  Message Description: EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

  Local Target Message Format: <timestamp> <seq_num> 12514 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12514 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain, <log details>

- **Message Code:** 12515

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of an expired CRL associated with a CA in the client certificates chain

  Message Description: EAP-TLS failed SSL/TLS handshake because of an expired CRL associated with a CA in the client certificates chain

  Local Target Message Format: <timestamp> <seq_num> 12515 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an expired CRL associated with a CA in the client certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12515 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an expired CRL associated with a CA in the client certificates chain, <log details>

- **Message Code:** 12516

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of an expired certificate in the client certificates chain

  Message Description: EAP-TLS failed SSL/TLS handshake because of an expired certificate in the client certificates chain

  Local Target Message Format: <timestamp> <seq_num> 12516 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an expired certificate in the client certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12516 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an expired certificate in the client certificates chain, <log details>

- **Message Code:** 12517

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of a revoked certificate in the client certificate chain

  Message Description: EAP-TLS failed SSL/TLS handshake because of a revoked certificate in the client certificate chain

  Local Target Message Format: <timestamp> <seq_num> 12517 WARN EAP: EAP-TLS failed SSL/TLS handshake because of a revoked certificate in the client certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12517 WARN EAP: EAP-TLS failed SSL/TLS handshake because of a revoked certificate in the client certificate chain, <log details>

- **Message Code:** 12518

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of a bad certificate in the client certificate chain

  Message Description: EAP-TLS failed SSL/TLS handshake because of a bad certificate in the client certificate chain

  Local Target Message Format: <timestamp> <seq_num> 12518 WARN EAP: EAP-TLS failed SSL/TLS handshake because of a bad certificate in the client certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12518 WARN EAP: EAP-TLS failed SSL/TLS handshake because of a bad certificate in the client certificate chain, <log details>

- **Message Code:** 12519

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of an unsupported certificate in the client certificate chain

  Message Description: EAP-TLS failed SSL/TLS handshake because of an unsupported certificate in the client certificate chain

  Local Target Message Format: <timestamp> <seq_num> 12519 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an unsupported certificate in the client certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12519 WARN EAP: EAP-TLS failed SSL/TLS handshake because of an unsupported certificate in the client certificate chain, <log details>

- **Message Code:** 12520

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

  Message Description: EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

Local Target Message Format: <timestamp> <seq_num> 12520 WARN EAP: EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12520 WARN EAP: EAP-TLS failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

- **Message Code:** 12521

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake after a client alert

  Message Description: EAP-TLS failed SSL/TLS handshake after a client alert

  Local Target Message Format: <timestamp> <seq_num> 12521 WARN EAP: EAP-TLS failed SSL/TLS handshake after a client alert, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12521 WARN EAP: EAP-TLS failed SSL/TLS handshake after a client alert, <log details>

- **Message Code:** 12522

  Severity: INFO

  Message Text: Prepared EAP-Request for inner method proposing EAP-TLS with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-TLS protocol for the inner method, and also providing an TLS challenge, for attachment to a RADIUS message. The EAP-TLS protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12522 INFO EAP: Prepared EAP-Request for inner method proposing EAP-TLS with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12522 INFO EAP: Prepared EAP-Request for inner method proposing EAP-TLS with challenge, <log details>

- **Message Code:** 12523

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/NAK packet, rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-TLS instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12523 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12523 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead, <log details>

- **Message Code:** 12524

  Severity: INFO

Message Text: Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-TLS as negotiated

Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response packet containing an EAP-TLS challenge-response, and accepting EAP-TLS as negotiated for the inner method.

Local Target Message Format: <timestamp> <seq_num> 12524 INFO EAP: Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-TLS as negotiated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12524 INFO EAP: Extracted EAP-Response containing EAP-TLS challenge-response for inner method and accepting EAP-TLS as negotiated, <log details>

- **Message Code:** 12525

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-TLS not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-TLS instead. However, EAP-TLS is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12525 WARN EAP: Failed to negotiate EAP for inner method because EAP-TLS not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12525 WARN EAP: Failed to negotiate EAP for inner method because EAP-TLS not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12526

  Severity: INFO

  Message Text: Extracted EAP-Response for inner method containing TLS challenge-response

  Message Description: Continuing the inner EAP-TLS protocol; processing the EAP-TLS challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12526 INFO EAP: Extracted EAP-Response for inner method containing TLS challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12526 INFO EAP: Extracted EAP-Response for inner method containing TLS challenge-response, <log details>

- **Message Code:** 12527

  Severity: INFO

  Message Text: Prepared EAP-Request for inner method with another EAP-TLS challenge

  Message Description: As part of the continuation of the inner EAP-TLS protocol, created an EAP-Request packet containing another EAP-TLS challenge, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

Local Target Message Format: <timestamp> <seq_num> 12527 INFO EAP: Prepared EAP-Request for inner method with another EAP-TLS challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12527 INFO EAP: Prepared EAP-Request for inner method with another EAP-TLS challenge, <log details>

- **Message Code:** 12528

  Severity: INFO

  Message Text: Inner EAP-TLS authentication succeeded

  Message Description: EAP-TLS authentication for the inner EAP method succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12528 INFO EAP: Inner EAP-TLS authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12528 INFO EAP: Inner EAP-TLS authentication succeeded, <log details>

- **Message Code:** 12529

  Severity: INFO

  Message Text: Inner EAP-TLS authentication failed

  Message Description: EAP-TLS authentication for the inner EAP method failed.

  Local Target Message Format: <timestamp> <seq_num> 12529 INFO EAP: Inner EAP-TLS authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12529 INFO EAP: Inner EAP-TLS authentication failed, <log details>

- **Message Code:** 12530

  Severity: WARN

  Message Text: EAP-TLS failed SSL/TLS handshake because of the client certificate is not yet valid

  Message Description: EAP-TLS failed SSL/TLS handshake because of the client certificate is not yet valid

  Local Target Message Format: <timestamp> <seq_num> 12530 WARN EAP: EAP-TLS failed SSL/TLS handshake because of the client certificate is not yet valid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12530 WARN EAP: EAP-TLS failed SSL/TLS handshake because of the client certificate is not yet valid, <log details>

- **Message Code:** 12531

  Severity: WARN

  Message Text: Successfully updated EAP-TLS seed key

  Message Description: Successfully updated the EAP-TLS seed key, used for further generation of master keys.

Local Target Message Format: <timestamp> <seq_num> 12531 WARN EAP: Successfully updated EAP-TLS seed key, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12531 WARN EAP: Successfully updated EAP-TLS seed key, <log details>

- **Message Code:** 12532

  Severity: WARN

  Message Text: Failed to update seed key

  Message Description: Internal error: failed to update EAP-TLS seed key, needed for further generation of master keys, most likely because an internal configuration object could not be properly fetched.

  Local Target Message Format: <timestamp> <seq_num> 12532 WARN EAP: Failed to update seed key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12532 WARN EAP: Failed to update seed key, <log details>

- **Message Code:** 12533

  Severity: INFO

  Message Text: Updated EAP-TLS Master Key Generation period

  Message Description: Updated the EAP-TLS Master Key Generation period.

  Local Target Message Format: <timestamp> <seq_num> 12533 INFO EAP: Updated EAP-TLS Master Key Generation period, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12533 INFO EAP: Updated EAP-TLS Master Key Generation period, <log details>

- **Message Code:** 12534

  Severity: INFO

  Message Text: EAP-TLS session ticket received from supplicant

  Message Description: EAP-TLS session ticket received from supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12534 INFO EAP: EAP-TLS session ticket received from supplicant, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12534 INFO EAP: EAP-TLS session ticket received from supplicant, <log details>

- **Message Code:** 12535

  Severity: WARN

  Message Text: The EAP-TLS session ticket received from supplicant is expired

  Message Description: Received from the supplicant the session ticket that has expired. Rejecting it.

Local Target Message Format: <timestamp> <seq_num> 12535 WARN EAP: The EAP-TLS session ticket received from supplicant is expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12535 WARN EAP: The EAP-TLS session ticket received from supplicant is expired, <log details>

- **Message Code:** 12536

  Severity: WARN

  Message Text: Failed to verify the EAP-TLS session ticket received from supplicant.

  Message Description: Failed to verify the EAP-TLS session ticket received from supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12536 WARN EAP: Failed to verify the EAP-TLS session ticket received from supplicant., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12536 WARN EAP: Failed to verify the EAP-TLS session ticket received from supplicant., <log details>

- **Message Code:** 12537

  Severity: WARN

  Message Text: The EAP-TLS session ticket identity does not match the EAP identity

  Message Description: The EAP-TLS session ticket identity does not match the EAP identity.

  Local Target Message Format: <timestamp> <seq_num> 12537 WARN EAP: The EAP-TLS session ticket identity does not match the EAP identity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12537 WARN EAP: The EAP-TLS session ticket identity does not match the EAP identity, <log details>

- **Message Code:** 12538

  Severity: WARN

  Message Text: The EAP-TLS session ticket received from supplicant contains an invalid authentication code

  Message Description: The EAP-TLS session ticket received from supplicant contains an invalid authentication code.

  Local Target Message Format: <timestamp> <seq_num> 12538 WARN EAP: The EAP-TLS session ticket received from supplicant contains an invalid authentication code, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12538 WARN EAP: The EAP-TLS session ticket received from supplicant contains an invalid authentication code, <log details>

- **Message Code:** 12539

  Severity: WARN

  Message Text: Failed to decrypt the EAP-TLS session ticket received from supplicant

  Message Description: Failed to decrypt the EAP-TLS session ticket received from supplicant.

Local Target Message Format: <timestamp> <seq_num> 12539 WARN EAP: Failed to decrypt the EAP-TLS session ticket received from supplicant, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12539 WARN EAP: Failed to decrypt the EAP-TLS session ticket received from supplicant, <log details>

- **Message Code:** 12540

  Severity: INFO

  Message Text: Successfully finished EAP-TLS session ticket provisioning/update

  Message Description: Successfully finished EAP-TLS session ticket provisioning/update,

  Local Target Message Format: <timestamp> <seq_num> 12540 INFO EAP: Successfully finished EAP-TLS session ticket provisioning/update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12540 INFO EAP: Successfully finished EAP-TLS session ticket provisioning/update, <log details>

- **Message Code:** 12541

  Severity: INFO

  Message Text: EAP-TLS needs to proactively update session ticket that is about to expire

  Message Description: EAP-TLS needs to proactively update session ticket that is about to expire.

  Local Target Message Format: <timestamp> <seq_num> 12541 INFO EAP: EAP-TLS needs to proactively update session ticket that is about to expire, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12541 INFO EAP: EAP-TLS needs to proactively update session ticket that is about to expire, <log details>

- **Message Code:** 12542

  Severity: WARN

  Message Text: The EAP-TLS session ticket received from supplicant while the stateless session resume is disabled. Performing full authentication

  Message Description: The EAP-TLS session ticket received from supplicant while the stateless session resume is disabled. Performing full authentication.

  Local Target Message Format: <timestamp> <seq_num> 12542 WARN EAP: The EAP-TLS session ticket received from supplicant while the stateless session resume is disabled. Performing full authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12542 WARN EAP: The EAP-TLS session ticket received from supplicant while the stateless session resume is disabled. Performing full authentication, <log details>

- **Message Code:** 12543

  Severity: WARN

Message Text: Cannot generate a new session ticket

Message Description: Encountered an internal error while attempting to issue a new session ticket.

Local Target Message Format: <timestamp> <seq_num> 12543 WARN EAP: Cannot generate a new session ticket, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12543 WARN EAP: Cannot generate a new session ticket, <log details>

- **Message Code:** 12544

  Severity: WARN

  Message Text: The EAP-TLS session ticket contains invalid Authority ID

  Message Description: The Authority ID of the session ticket received from the client does not match that of the ISE deployment that processed the authentication request, probably because the session ticket of the client was created by another ISE deployment.

  Local Target Message Format: <timestamp> <seq_num> 12544 WARN EAP: The EAP-TLS session ticket contains invalid Authority ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12544 WARN EAP: The EAP-TLS session ticket contains invalid Authority ID, <log details>

- **Message Code:** 12545

  Severity: INFO

  Message Text: Client requested EAP-TLS session ticket

  Message Description: Client sent empty EAP-TLS session ticket client hello extension awaiting new EAP-TLS session ticket in reposnse from ISE.

  Local Target Message Format: <timestamp> <seq_num> 12545 INFO EAP: Client requested EAP-TLS session ticket, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12545 INFO EAP: Client requested EAP-TLS session ticket, <log details>

- **Message Code:** 12546

  Severity: WARN

  Message Text: The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless session resume. Performing full authentication

  Message Description: The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless session resume. Performing full authentication.

  Local Target Message Format: <timestamp> <seq_num> 12546 WARN EAP: The EAP-TLS session ticket received from supplicant. Inner EAP-TLS does not support stateless session resume. Performing full authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12546 WARN EAP: The EAP-TLS

session ticket received from supplicant. Inner EAP-TLS does not support stateless session resume. Performing full authentication, <log details>

- **Message Code:** 12550

  Severity: INFO

  Message Text: Sent an OCSP request to the primary OCSP server for the CA

  Message Description: Send an OCSP request to the primary OCSP server for the CA.

  Local Target Message Format: <timestamp> <seq_num> 12550 INFO EAP: Sent an OCSP request to the primary OCSP server for the CA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12550 INFO EAP: Sent an OCSP request to the primary OCSP server for the CA, <log details>

- **Message Code:** 12551

  Severity: INFO

  Message Text: Sent an OCSP request to the secondary OCSP server for the CA

  Message Description: Send an OCSP request to the secondary OCSP server for the CA.

  Local Target Message Format: <timestamp> <seq_num> 12551 INFO EAP: Sent an OCSP request to the secondary OCSP server for the CA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12551 INFO EAP: Sent an OCSP request to the secondary OCSP server for the CA, <log details>

- **Message Code:** 12552

  Severity: WARN

  Message Text: Conversation with OCSP server ended with failure

  Message Description: Conversation with OCSP server ended with failure.

  Local Target Message Format: <timestamp> <seq_num> 12552 WARN EAP: Conversation with OCSP server ended with failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12552 WARN EAP: Conversation with OCSP server ended with failure, <log details>

- **Message Code:** 12553

  Severity: INFO

  Message Text: Received OCSP response

  Message Description: Received OCSP response.

  Local Target Message Format: <timestamp> <seq_num> 12553 INFO EAP: Received OCSP response, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12553 INFO EAP: Received OCSP response, <log details>

- **Message Code:** 12554

  Severity: INFO

  Message Text: OCSP status of user certificate is good

  Message Description: The OCSP server reported that the user certificate status is good.

  Local Target Message Format: <timestamp> <seq_num> 12554 INFO EAP: OCSP status of user certificate is good, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12554 INFO EAP: OCSP status of user certificate is good, <log details>

- **Message Code:** 12555

  Severity: WARN

  Message Text: OCSP status of user certificate is revoked

  Message Description: The OCSP server reported that the user certificate status is revoked.

  Local Target Message Format: <timestamp> <seq_num> 12555 WARN EAP: OCSP status of user certificate is revoked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12555 WARN EAP: OCSP status of user certificate is revoked, <log details>

- **Message Code:** 12556

  Severity: INFO

  Message Text: OCSP status of user certificate is unknown

  Message Description: The OCSP server reported that the user certificate status is unknown or ISE was unable to connect to the OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 12556 INFO EAP: OCSP status of user certificate is unknown, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12556 INFO EAP: OCSP status of user certificate is unknown, <log details>

- **Message Code:** 12557

  Severity: WARN

  Message Text: User Auth failed because OCSP status is unknown

  Message Description: User Auth failed because OCSP status is unknown.

  Local Target Message Format: <timestamp> <seq_num> 12557 WARN EAP: User Auth failed because OCSP status is unknown, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12557 WARN EAP: User Auth failed because OCSP status is unknown, <log details>

- **Message Code:** 12558

  Severity: INFO

  Message Text: Performed fallback to secondary OCSP server

  Message Description: Performed fallback to secondary OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 12558 INFO EAP: Performed fallback to secondary OCSP server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12558 INFO EAP: Performed fallback to secondary OCSP server, <log details>

- **Message Code:** 12559

  Severity: WARN

  Message Text: Internal error occurred during communication with the OCSP server

  Message Description: Internal error during communication with the OCSP server. The configuration of the OCSP server doesn't match the ISE OCSP client.

  Local Target Message Format: <timestamp> <seq_num> 12559 WARN EAP: Internal error occurred during communication with the OCSP server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12559 WARN EAP: Internal error occurred during communication with the OCSP server, <log details>

- **Message Code:** 12560

  Severity: WARN

  Message Text: OCSP server URL is invalid

  Message Description: OCSP server URL is invalid and cannot be properly parsed.

  Local Target Message Format: <timestamp> <seq_num> 12560 WARN EAP: OCSP server URL is invalid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12560 WARN EAP: OCSP server URL is invalid, <log details>

- **Message Code:** 12561

  Severity: WARN

  Message Text: Connection to OCSP server failed

  Message Description: Connection attempt to OCSP server failed.

  Local Target Message Format: <timestamp> <seq_num> 12561 WARN EAP: Connection to OCSP server failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12561 WARN EAP: Connection to OCSP server failed, <log details>

- **Message Code:** 12562

  Severity: WARN

  Message Text: OCSP server response is invalid

  Message Description: OCSP server returned a response that cannot be parsed by ISE.

  Local Target Message Format: <timestamp> <seq_num> 12562 WARN EAP: OCSP server response is invalid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12562 WARN EAP: OCSP server response is invalid, <log details>

- **Message Code:** 12563

  Severity: WARN

  Message Text: OCSP server returned an error

  Message Description: OCSP server returned an error in response to the ISE OCSP request.

  Local Target Message Format: <timestamp> <seq_num> 12563 WARN EAP: OCSP server returned an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12563 WARN EAP: OCSP server returned an error, <log details>

- **Message Code:** 12564

  Severity: WARN

  Message Text: OCSP server did not provide the required nonce in response

  Message Description: Specific OCSP service in ISE is configured to use nonce for OCSP server verification but the OCSP server did not provide a nonce in response.

  Local Target Message Format: <timestamp> <seq_num> 12564 WARN EAP: OCSP server did not provide the required nonce in response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12564 WARN EAP: OCSP server did not provide the required nonce in response, <log details>

- **Message Code:** 12565

  Severity: WARN

  Message Text: OCSP server response nonce verification failed

  Message Description: Cryptographic verification of nonce returned in OCSP server response failed.

  Local Target Message Format: <timestamp> <seq_num> 12565 WARN EAP: OCSP server response nonce verification failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12565 WARN EAP: OCSP server response nonce verification failed, <log details>

- **Message Code:** 12566

  Severity: WARN

  Message Text: OCSP server response time verification failed

  Message Description: In the OCSP server response verification of 'This Update' or 'Next Update' fields failed.

  Local Target Message Format: <timestamp> <seq_num> 12566 WARN EAP: OCSP server response time verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12566 WARN EAP: OCSP server response time verification failed, <log details>

- **Message Code:** 12567

  Severity: WARN

  Message Text: OCSP server response signature verification failed

  Message Description: OCSP server response signature verification failed.

  Local Target Message Format: <timestamp> <seq_num> 12567 WARN EAP: OCSP server response signature verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12567 WARN EAP: OCSP server response signature verification failed, <log details>

- **Message Code:** 12568

  Severity: INFO

  Message Text: Lookup user certificate status in OCSP cache

  Message Description: Lookup user certificate status in OCSP cache.

  Local Target Message Format: <timestamp> <seq_num> 12568 INFO EAP: Lookup user certificate status in OCSP cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12568 INFO EAP: Lookup user certificate status in OCSP cache, <log details>

- **Message Code:** 12569

  Severity: INFO

  Message Text: User certificate status was not found in OCSP cache

  Message Description: User certificate status was not found in OCSP cache; ISE is going to perform OCSP request to the configured OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 12569 INFO EAP: User certificate status was not found in OCSP cache, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12569 INFO EAP: User certificate status was not found in OCSP cache, <log details>

- **Message Code:** 12570

  Severity: INFO

  Message Text: Lookup user certificate status in OCSP cache succeeded

  Message Description: Lookup user certificate status in OCSP cache succeeded; ISE is going to use this status without performing OCSP request to the configured OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 12570 INFO EAP: Lookup user certificate status in OCSP cache succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12570 INFO EAP: Lookup user certificate status in OCSP cache succeeded, <log details>

- **Message Code:** 12571

  Severity: INFO

  Message Text: ISE will continue to CRL verification if it is configured for specific CA

  Message Description: OCSP verification either failed or returned unknown certificate status. ISE will continue to CRL verification if it is configured for specific CA.

  Local Target Message Format: <timestamp> <seq_num> 12571 INFO EAP: ISE will continue to CRL verification if it is configured for specific CA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12571 INFO EAP: ISE will continue to CRL verification if it is configured for specific CA, <log details>

- **Message Code:** 12572

  Severity: DEBUG

  Message Text: OCSP response not cached

  Message Description: Response from OCSP server indicates that the contents of the response should not be cached

  Local Target Message Format: <timestamp> <seq_num> 12572 DEBUG EAP: OCSP response not cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12572 DEBUG EAP: OCSP response not cached, <log details>

- **Message Code:** 12573

  Severity: ERROR

  Message Text: A field in the handshake was incorrect or inconsistent with other fields

  Message Description: The curve group used to generate the key that signed the client certificate is not included in the clients supported groups list

Local Target Message Format: <timestamp> <seq_num>12573 ERROR EAP A field in the handshake was incorrect or inconsistent with other fields, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12573 ERROR EAP A field in the handshake was incorrect or inconsistent with other fields, <log details>

- **Message Code:** 12600

  Severity: INFO

  Message Text: Prepared EAP-Request proposing EAP-GTC with challenge

  Message Description: Created an EAP-Request packet to propose to use the EAP-GTC protocol, and also providing an GTC challenge, for attachment to a RADIUS message. The EAP-GTC protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12600 INFO EAP: Prepared EAP-Request proposing EAP-GTC with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12600 INFO EAP: Prepared EAP-Request proposing EAP-GTC with challenge, <log details>

- **Message Code:** 12601

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use EAP-GTC instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-GTC instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12601 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-GTC instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12601 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-GTC instead, <log details>

- **Message Code:** 12602

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-GTC challenge-response and accepting EAP-GTC as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing an EAP-GTC challenge-response, and accepting EAP-GTC as negotiated.

  Local Target Message Format: <timestamp> <seq_num> 12602 INFO EAP: Extracted EAP-Response containing EAP-GTC challenge-response and accepting EAP-GTC as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12602 INFO EAP: Extracted EAP-Response containing EAP-GTC challenge-response and accepting EAP-GTC as negotiated, <log details>

- **Message Code:** 12603

  Severity: WARN

  Message Text: Failed to negotiate EAP because EAP-GTC not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-GTC instead. However, EAP-GTC is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12603 WARN EAP: Failed to negotiate EAP because EAP-GTC not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12603 WARN EAP: Failed to negotiate EAP because EAP-GTC not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12604

  Severity: INFO

  Message Text: Extracted EAP-Response containing GTC challenge-response

  Message Description: Continuing the EAP-GTC protocol; processing the EAP-GTC challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12604 INFO EAP: Extracted EAP-Response containing GTC challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12604 INFO EAP: Extracted EAP-Response containing GTC challenge-response, <log details>

- **Message Code:** 12605

  Severity: INFO

  Message Text: Prepared EAP-Request with another EAP-GTC challenge

  Message Description: As part of the continuation of the EAP-GTC protocol, created an EAP-Request packet containing another EAP-GTC challenge, for attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12605 INFO EAP: Prepared EAP-Request with another EAP-GTC challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12605 INFO EAP: Prepared EAP-Request with another EAP-GTC challenge, <log details>

- **Message Code:** 12606

  Severity: INFO

  Message Text: Prepared EAP-Request for inner method proposing EAP-GTC with challenge

  Message Description: Created an EAP-Request packet to propose to use the EAP-GTC protocol for the inner method, and also providing an GTC challenge, for attachment to a RADIUS message. The EAP-GTC protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12606 INFO EAP: Prepared EAP-Request for inner method proposing EAP-GTC with challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12606 INFO EAP: Prepared EAP-Request for inner method proposing EAP-GTC with challenge, <log details>

- **Message Code:** 12607

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK for inner method requesting to use EAP-GTC instead

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/NAK packet, rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-GTC instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12607 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-GTC instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12607 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-GTC instead, <log details>

- **Message Code:** 12608

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-GTC challenge-response for inner method and accepting EAP-GTC as negotiated

  Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response packet containing an EAP-GTC challenge-response, and accepting EAP-GTC as negotiated for the inner method.

  Local Target Message Format: <timestamp> <seq_num> 12608 INFO EAP: Extracted EAP-Response containing EAP-GTC challenge-response for inner method and accepting EAP-GTC as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12608 INFO EAP: Extracted EAP-Response containing EAP-GTC challenge-response for inner method and accepting EAP-GTC as negotiated, <log details>

- **Message Code:** 12609

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-GTC not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-GTC instead. However, EAP-GTC is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12609 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12609 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12610

  Severity: INFO

  Message Text: Extracted EAP-Response for inner method containing GTC challenge-response

  Message Description: Continuing the inner EAP-GTC protocol; processing the EAP-GTC challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12610 INFO EAP: Extracted EAP-Response for inner method containing GTC challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12610 INFO EAP: Extracted EAP-Response for inner method containing GTC challenge-response, <log details>

- **Message Code:** 12611

  Severity: INFO

  Message Text: Prepared EAP-Request for inner method with another EAP-GTC challenge

  Message Description: As part of the continuation of the inner EAP-GTC protocol, created an EAP-Request packet containing another EAP-GTC challenge, for encapsulation within the outer EAP method's outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12611 INFO EAP: Prepared EAP-Request for inner method with another EAP-GTC challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12611 INFO EAP: Prepared EAP-Request for inner method with another EAP-GTC challenge, <log details>

- **Message Code:** 12612

  Severity: INFO

  Message Text: EAP-GTC authentication succeeded

  Message Description: EAP-GTC authentication has succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12612 INFO EAP: EAP-GTC authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12612 INFO EAP: EAP-GTC authentication succeeded, <log details>

- **Message Code:** 12613

  Severity: INFO

  Message Text: EAP-GTC authentication failed

  Message Description: EAP-GTC authentication has failed.

  Local Target Message Format: <timestamp> <seq_num> 12613 INFO EAP: EAP-GTC authentication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12613 INFO EAP: EAP-GTC authentication failed, <log details>

- **Message Code:** 12614

  Severity: INFO

  Message Text: Inner EAP-GTC authentication succeeded

  Message Description: EAP-GTC authentication for the inner EAP method has succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12614 INFO EAP: Inner EAP-GTC authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12614 INFO EAP: Inner EAP-GTC authentication succeeded, <log details>

- **Message Code:** 12615

  Severity: INFO

  Message Text: Inner EAP-GTC authentication failed

  Message Description: EAP-GTC authentication for the inner EAP method has failed.

  Local Target Message Format: <timestamp> <seq_num> 12615 INFO EAP: Inner EAP-GTC authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12615 INFO EAP: Inner EAP-GTC authentication failed, <log details>

- **Message Code:** 12616

  Severity: WARN

  Message Text: GTC username doesn't match inner method EAP-Response/Identity

  Message Description: The GTC username does not match the username received in the inner method EAP-Response/Identity packet. One possible reason might be that the client's supplicant is preconfigured with another username not matching that entered by the user.

  Local Target Message Format: <timestamp> <seq_num> 12616 WARN EAP: GTC username doesn't match inner method EAP-Response/Identity, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12616 WARN EAP: GTC username doesn't match inner method EAP-Response/Identity, <log details>

- **Message Code:** 12617

  Severity: WARN

  Message Text: Internal error: invalid EAP-GTC state

  Message Description: Internal error: invalid EAP-GTC state.

  Local Target Message Format: <timestamp> <seq_num> 12617 WARN EAP: Internal error: invalid EAP-GTC state, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12617 WARN EAP: Internal error: invalid EAP-GTC state, <log details>

- **Message Code:** 12618

  Severity: INFO

  Message Text: Failed to parse EAP-GTC packet

  Message Description: Failed to parse the EAP-GTC packet.

  Local Target Message Format: <timestamp> <seq_num> 12618 INFO EAP: Failed to parse EAP-GTC packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12618 INFO EAP: Failed to parse EAP-GTC packet, <log details>

- **Message Code:** 12619

  Severity: INFO

  Message Text: Received EAP-GTC packet with invalid argument

  Message Description: Received an EAP-GTC packet with an invalid argument.

  Local Target Message Format: <timestamp> <seq_num> 12619 INFO EAP: Received EAP-GTC packet with invalid argument, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12619 INFO EAP: Received EAP-GTC packet with invalid argument, <log details>

- **Message Code:** 12621

  Severity: INFO

  Message Text: EAP-GTC password change attempt failed

  Message Description: The attempt to change the password failed because the Allowed Protocols does not allow password change for the GTC inner method.

  Local Target Message Format: <timestamp> <seq_num> 12621 INFO EAP: EAP-GTC password change attempt failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12621 INFO EAP: EAP-GTC password change attempt failed, <log details>

- **Message Code:** 12622

  Severity: DEBUG

  Message Text: EAP-GTC password change attempt passed

  Message Description: The EAP-GTC password change attempt has passed.

  Local Target Message Format: <timestamp> <seq_num> 12622 DEBUG EAP: EAP-GTC password change attempt passed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12622 DEBUG EAP: EAP-GTC password change attempt passed, <log details>

- **Message Code:** 12623

  Severity: INFO

  Message Text: EAP-GTC authentication attempt failed

  Message Description: The EAP-GTC authentication attempt has failed.

  Local Target Message Format: <timestamp> <seq_num> 12623 INFO EAP: EAP-GTC authentication attempt failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12623 INFO EAP: EAP-GTC authentication attempt failed, <log details>

- **Message Code:** 12624

  Severity: DEBUG

  Message Text: EAP-GTC authentication attempt passed

  Message Description: The EAP-GTC authentication attempt has passed.

  Local Target Message Format: <timestamp> <seq_num> 12624 DEBUG EAP: EAP-GTC authentication attempt passed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12624 DEBUG EAP: EAP-GTC authentication attempt passed, <log details>

- **Message Code:** 12625

  Severity: DEBUG

  Message Text: Valid EAP-Key-Name attribute received

  Message Description: A valid EAP-Key-Name attribute was received. ISE will provide the EAP-Key-Name attribute filled with EAP-Session-ID on RADIUS Access-Accept message.

  Local Target Message Format: <timestamp> <seq_num> 12625 DEBUG EAP: Valid EAP-Key-Name attribute received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12625 DEBUG EAP: Valid EAP-Key-Name attribute received, <log details>

- **Message Code:** 12626

  Severity: WARN

  Message Text: Invalid EAP-Key-Name attribute received

  Message Description: An invalid EAP-Key-Name attribute was received. The attribute value must be empty.

  Local Target Message Format: <timestamp> <seq_num> 12626 WARN EAP: Invalid EAP-Key-Name attribute received, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12626 WARN EAP: Invalid EAP-Key-Name attribute received, <log details>

- **Message Code:** 12628

  Severity: WARN

  Message Text: Invalid operation performed

  Message Description: Internal error, invalid operation performed, cannot continue current conversation. Refer to debug log for detailed information and contact TAC engineer to report the problem

  Local Target Message Format: <timestamp> <seq_num> 12628 WARN EAP: Invalid operation performed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12628 WARN EAP: Invalid operation performed, <log details>

- **Message Code:** 12650

  Severity: WARN

  Message Text: Invalid operation performed

  Message Description: Internal error, invalid operation performed. Refer to debug log for detailed information and contact TAC engineer to report the problem

  Local Target Message Format: <timestamp> <seq_num> 12650 WARN EAP: Invalid operation performed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12650 WARN EAP: Invalid operation performed, <log details>

- **Message Code:** 12651

  Severity: INFO

  Message Text: Accept client on authenticated provisioning

  Message Description: Accept client on authenticated provisioning

  Local Target Message Format: <timestamp> <seq_num> 12651 INFO EAP: Accept client on authenticated provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12651 INFO EAP: Accept client on authenticated provisioning, <log details>

- **Message Code:** 12652

  Severity: INFO

  Message Text: Accept client on provisioning after invalid PAC fallback

  Message Description: Accept client on provisioning after invalid PAC fallback

  Local Target Message Format: <timestamp> <seq_num> 12652 INFO EAP: Accept client on provisioning after invalid PAC fallback, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12652 INFO EAP: Accept client on provisioning after invalid PAC fallback, <log details>

- **Message Code:** 12653

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-GTC denied for anonymous PAC provisioning

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-GTC instead. However, EAP-GTC cannot be used for anonymous PAC provisioning.

  Local Target Message Format: <timestamp> <seq_num> 12653 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC denied for anonymous PAC provisioning, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12653 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC denied for anonymous PAC provisioning, <log details>

- **Message Code:** 12700

  Severity: INFO

  Message Text: Prepared EAP-Request proposing LEAP with challenge

  Message Description: Created an EAP-Request packet to propose to use the LEAP protocol, and also providing a LEAP challenge, for attachment to a RADIUS message. The LEAP protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12700 INFO EAP: Prepared EAP-Request proposing LEAP with challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12700 INFO EAP: Prepared EAP-Request proposing LEAP with challenge, <log details>

- **Message Code:** 12701

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use LEAP instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use LEAP instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12701 INFO EAP: Extracted EAP-Response/NAK requesting to use LEAP instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12701 INFO EAP: Extracted EAP-Response/NAK requesting to use LEAP instead, <log details>

- **Message Code:** 12702

Severity: INFO

Message Text: Extracted EAP-Response containing LEAP challenge-response and accepting LEAP as negotiated

Message Description: Extracted from the RADIUS message an EAP-Response packet containing a LEAP challenge-response, and accepting LEAP as negotiated

Local Target Message Format: <timestamp> <seq_num> 12702 INFO EAP: Extracted EAP-Response containing LEAP challenge-response and accepting LEAP as negotiated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12702 INFO EAP: Extracted EAP-Response containing LEAP challenge-response and accepting LEAP as negotiated, <log details>

- **Message Code:** 12703

  Severity: WARN

  Message Text: Failed to negotiate EAP because LEAP not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use LEAP instead. However, LEAP is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12703 WARN EAP: Failed to negotiate EAP because LEAP not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12703 WARN EAP: Failed to negotiate EAP because LEAP not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12704

  Severity: INFO

  Message Text: LEAP completed. Sent EAP-Response containing LEAP challenge-response and cisco-av-pair containing LEAP session-key

  Message Description: Completed the LEAP protocol. Sent the LEAP challenge-response in EAP-Response, and LEAP session-key in cisco-av-pair.

  Local Target Message Format: <timestamp> <seq_num> 12704 INFO EAP: LEAP completed. Sent EAP-Response containing LEAP challenge-response and cisco-av-pair containing LEAP session-key, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12704 INFO EAP: LEAP completed. Sent EAP-Response containing LEAP challenge-response and cisco-av-pair containing LEAP session-key, <log details>

- **Message Code:** 12705

  Severity: INFO

  Message Text: LEAP authentication passed; Continuing protocol

  Message Description: LEAP authentication passed. Continue LEAP protocol.

Local Target Message Format: <timestamp> <seq_num> 12705 INFO EAP: LEAP authentication passed; Continuing protocol, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12705 INFO EAP: LEAP authentication passed; Continuing protocol, <log details>

- **Message Code:** 12706

  Severity: INFO

  Message Text: LEAP authentication failed; Finishing protocol

  Message Description: LEAP authentication has failed. Protocol finished with a failure.

  Local Target Message Format: <timestamp> <seq_num> 12706 INFO EAP: LEAP authentication failed; Finishing protocol, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12706 INFO EAP: LEAP authentication failed; Finishing protocol, <log details>

- **Message Code:** 12707

  Severity: INFO

  Message Text: LEAP authentication error; Finishing protocol

  Message Description: A LEAP authentication error has occurred. Protocol finished with an error.

  Local Target Message Format: <timestamp> <seq_num> 12707 INFO EAP: LEAP authentication error; Finishing protocol, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12707 INFO EAP: LEAP authentication error; Finishing protocol, <log details>

- **Message Code:** 12708

  Severity: WARN

  Message Text: LEAP packet validation failed

  Message Description: Failed to validate LEAP packet.

  Local Target Message Format: <timestamp> <seq_num> 12708 WARN EAP: LEAP packet validation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12708 WARN EAP: LEAP packet validation failed, <log details>

- **Message Code:** 12709

  Severity: WARN

  Message Text: LEAP packet parsing failed

  Message Description: Failed to parse LEAP packet.

Local Target Message Format: <timestamp> <seq_num> 12709 WARN EAP: LEAP packet parsing failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12709 WARN EAP: LEAP packet parsing failed, <log details>

- **Message Code:** 12710

  Severity: WARN

  Message Text: LEAP internal error: Invalid state

  Message Description: LEAP internal error: Invalid state.

  Local Target Message Format: <timestamp> <seq_num> 12710 WARN EAP: LEAP internal error: Invalid state, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12710 WARN EAP: LEAP internal error: Invalid state, <log details>

- **Message Code:** 12711

  Severity: WARN

  Message Text: LEAP internal error: LEAP challenge not created

  Message Description: LEAP internal error: LEAP challenge was not created.

  Local Target Message Format: <timestamp> <seq_num> 12711 WARN EAP: LEAP internal error: LEAP challenge not created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12711 WARN EAP: LEAP internal error: LEAP challenge not created, <log details>

- **Message Code:** 12712

  Severity: WARN

  Message Text: LEAP internal error: LEAP challenge-response and session-key not created

  Message Description: LEAP internal error: LEAP challenge-response and session-key were not created.

  Local Target Message Format: <timestamp> <seq_num> 12712 WARN EAP: LEAP internal error: LEAP challenge-response and session-key not created, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12712 WARN EAP: LEAP internal error: LEAP challenge-response and session-key not created, <log details>

- **Message Code:** 12750

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under PEAP configuration in the Allowed Protocols

Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-MSCHAP instead. However, EAP-MSCHAP is not allowed under PEAP configuration in Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num> 12750 WARN EAP: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under PEAP configuration in the Allowed Protocols, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12750 WARN EAP: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under PEAP configuration in the Allowed Protocols, <log details>

- **Message Code:** 12751

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under EAP-FAST configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-MSCHAP instead. However, EAP-MSCHAP is not allowed under EAP-FAST configuration in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12751 WARN EAP: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under EAP-FAST configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12751 WARN EAP: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under EAP-FAST configuration in the Allowed Protocols, <log details>

- **Message Code:** 12752

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-TLS not allowed under PEAP configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol that was previously proposed for the inner method, and requested to use EAP-TLS instead. However, ISE does not allow EAP-TLS under PEAP configuration in the Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12752 WARN EAP: Failed to negotiate EAP for inner method because EAP-TLS not allowed under PEAP configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12752 WARN EAP: Failed to negotiate EAP for inner method because EAP-TLS not allowed under PEAP configuration in the Allowed Protocols, <log details>

- **Message Code:** 12753

  Severity: WARN

Message Text: Failed to negotiate EAP for inner method because EAP-TLS not allowed under EAP-FAST configuration in the Allowed Protocols

Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol that was previously proposed for the inner method, and requested to use EAP-TLS instead. However, ISE does not allow EAP-TLS under EAP-FAST configuration in the Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num> 12753 WARN EAP: Failed to negotiate EAP for inner method because EAP-TLS not allowed under EAP-FAST configuration in the Allowed Protocols, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12753 WARN EAP: Failed to negotiate EAP for inner method because EAP-TLS not allowed under EAP-FAST configuration in the Allowed Protocols, <log details>

- **Message Code:** 12754

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-GTC not allowed under PEAP configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-GTC instead. However, EAP-GTC is not allowed under PEAP configuration in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12754 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC not allowed under PEAP configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12754 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC not allowed under PEAP configuration in the Allowed Protocols, <log details>

- **Message Code:** 12755

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-GTC not allowed under EAP-FAST configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol that was previously proposed for the inner method, and requested to use EAP-GTC instead. However, ISE does not allow EAP-GTC under EAP-FAST configuration in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12755 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC not allowed under EAP-FAST configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12755 WARN EAP: Failed to negotiate EAP for inner method because EAP-GTC not allowed under EAP-FAST configuration in the Allowed Protocols, <log details>

- **Message Code:** 12756

Severity: INFO

Message Text: Prepared EAP-Request proposing TEAP with challenge

Message Description: Created an EAP-Request packet proposing to use the TEAP protocol, and also providing an TEAP challenge, for attachment to a RADIUS message. The TEAP protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num>12756 INFO EAP Prepared EAP-Request proposing TEAP with challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12756 INFO EAP Prepared EAP-Request proposing TEAP with challenge, <log details>

- **Message Code:** 12757

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use TEAP instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use TEAP instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num>12757 INFO EAP Extracted EAP-Response/NAK requesting to use TEAP instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12757 INFO EAP Extracted EAP-Response/NAK requesting to use TEAP instead, <log details>

- **Message Code:** 12758

  Severity: INFO

  Message Text: Extracted EAP-Response containing TEAP challenge-response and accepting TEAP as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing an TEAP challenge-response, and accepting TEAP as negotiated

  Local Target Message Format: <timestamp> <seq_num>12758 INFO EAP Extracted EAP-Response containing TEAP challenge-response and accepting TEAP as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12758 INFO EAP Extracted EAP-Response containing TEAP challenge-response and accepting TEAP as negotiated, <log details>

- **Message Code:** 12759

  Severity: WARN

  Message Text: Failed to negotiate EAP because TEAP not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use TEAP instead. However, TEAP is not allowed in Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num>12759 WARN EAP Failed to negotiate EAP because TEAP not allowed in the Allowed Protocols, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12759 WARN EAP Failed to negotiate EAP because TEAP not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12760

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under TEAP configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-MSCHAP instead. However, EAP-MSCHAP is not allowed under TEAP configuration in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num>12760 WARN EAP Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under TEAP configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12760 WARN EAP Failed to negotiate EAP for inner method because EAP-MSCHAP not allowed under TEAP configuration in the Allowed Protocols, <log details>

- **Message Code:** 12761

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-TLS not allowed under TEAP configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol that was previously proposed for the inner method, and requested to use EAP-TLS instead. However, ISE does not allow EAP-TLS under TEAP configuration in the Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num>12761 WARN EAP Failed to negotiate EAP for inner method because EAP-TLS not allowed under TEAP configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12761 WARN EAP Failed to negotiate EAP for inner method because EAP-TLS not allowed under TEAP configuration in the Allowed Protocols, <log details>

- **Message Code:** 12762

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-GTC not allowed under TEAP configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol that was previously proposed for the inner method, and requested to use EAP-GTC instead. However, ISE does not allow EAP-GTC under TEAP configuration in Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num>12762 WARN EAP Failed to negotiate EAP for inner method because EAP-GTC not allowed under TEAP configuration in the Allowed Protocols, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12762 WARN EAP Failed to negotiate EAP for inner method because EAP-GTC not allowed under TEAP configuration in the Allowed Protocols, <log details>

- **Message Code:** 12763

  Severity: INFO

  Message Text: Encrypted extentions server write

  Message Description: Encrypted extentions server write

  Local Target Message Format: <timestamp> <seq_num>EAP Encrypted extentions server write INFO Encrypted extentions server write, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Encrypted extentions server write INFO Encrypted extentions server write, <log details>

- **Message Code:** 12764

  Severity: INFO

  Message Text: Encrypted extentions server read

  Message Description: Encrypted extentions server read

  Local Target Message Format: <timestamp> <seq_num>EAP Encrypted extentions server read INFO Encrypted extentions server read, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Encrypted extentions server read INFO Encrypted extentions server read, <log details>

- **Message Code:** 12765

  Severity: INFO

  Message Text: Server certificate verify write

  Message Description: Server certificate verify write

  Local Target Message Format: <timestamp> <seq_num>EAP Server certificate verify write INFO Server certificate verify write, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server certificate verify write INFO Server certificate verify write, <log details>

- **Message Code:** 12766

  Severity: INFO

  Message Text: Server read certificate yerify

  Message Description: Server read certificate yerify

Local Target Message Format: <timestamp> <seq_num>EAP Server read certificate yerify INFO Server read certificate yerify, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server read certificate yerify INFO Server read certificate yerify, <log details>

- **Message Code:** 12767

  Severity: INFO

  Message Text: Server write key update

  Message Description: Server write key update

  Local Target Message Format: <timestamp> <seq_num>EAP Server write key update INFO Server write key update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server write key update INFO Server write key update, <log details>

- **Message Code:** 12768

  Severity: INFO

  Message Text: Client write key update

  Message Description: Client write key update

  Local Target Message Format: <timestamp> <seq_num>EAP Client write key update INFO Client write key update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client write key update INFO Client write key update, <log details>

- **Message Code:** 12769

  Severity: INFO

  Message Text: Client read key update

  Message Description: Client read key update

  Local Target Message Format: <timestamp> <seq_num>EAP Client read key update INFO Client read key update, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client read key update INFO Client read key update, <log details>

- **Message Code:** 12770

  Severity: INFO

  Message Text: Server read key update

  Message Description: Server read key update

Local Target Message Format: <timestamp> <seq_num>EAP Server read key update INFO Server read key update, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server read key update INFO Server read key update, <log details>

- **Message Code:** 12771

  Severity: INFO

  Message Text: Early data

  Message Description: Early data

  Local Target Message Format: <timestamp> <seq_num>EAP Early data INFO Early data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Early data INFO Early data, <log details>

- **Message Code:** 12772

  Severity: INFO

  Message Text: Pending early data end

  Message Description: Pending early data end

  Local Target Message Format: <timestamp> <seq_num>EAP Pending early data end INFO Pending early data end, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Pending early data end INFO Pending early data end, <log details>

- **Message Code:** 12773

  Severity: INFO

  Message Text: Write end of early data

  Message Description: Write end of early data

  Local Target Message Format: <timestamp> <seq_num>EAP Write end of early data INFO Write end of early data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Write end of early data INFO Write end of early data, <log details>

- **Message Code:** 12774

  Severity: INFO

  Message Text: Server read end of early data

  Message Description: Server read end of early data

  Local Target Message Format: <timestamp> <seq_num>EAP Server read end of early data INFO Server read end of early data, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server read end of early data INFO Server read end of early data, <log details>

- **Message Code:** 12775

  Severity: INFO

  Message Text: Client read end of early data

  Message Description: Client read end of early data

  Local Target Message Format: <timestamp> <seq_num>EAP Client read end of early data INFO Client read end of early data, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client read end of early data INFO Client read end of early data, <log details>

- **Message Code:** 12776

  Severity: INFO

  Message Text: Unknown state

  Message Description: Unknown state

  Local Target Message Format: <timestamp> <seq_num>EAP Unknown state INFO Unknown state, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Unknown state INFO Unknown state, <log details>

- **Message Code:** 12777

  Severity: INFO

  Message Text: Write client session ticket

  Message Description: Write client session ticket

  Local Target Message Format: <timestamp> <seq_num>EAP Write client session ticket INFO Write client session ticket, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Write client session ticket INFO Write client session ticket, <log details>

- **Message Code:** 12800

  Severity: INFO

  Message Text: Extracted first TLS record; TLS handshake started

  Message Description: For the first time in the current EAP conversation, extracted from the EAP-Response packet a TLS record, presumably containing in turn a TLS ClientHello message. ISE recognizes this as an attempt by the client's supplicant to initiate a TLS handshake.

  Local Target Message Format: <timestamp> <seq_num> 12800 INFO EAP: Extracted first TLS record; TLS handshake started, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12800 INFO EAP: Extracted first TLS record; TLS handshake started, <log details>

- **Message Code:** 12801

  Severity: INFO

  Message Text: Prepared TLS ChangeCipherSpec message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS ChangeCipherSpec message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12801 INFO EAP: Prepared TLS ChangeCipherSpec message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12801 INFO EAP: Prepared TLS ChangeCipherSpec message, <log details>

- **Message Code:** 12802

  Severity: INFO

  Message Text: Prepared TLS Finished message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS Finished message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message. ISE is indicating that it is ready to finish the TLS handshake.

  Local Target Message Format: <timestamp> <seq_num> 12802 INFO EAP: Prepared TLS Finished message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12802 INFO EAP: Prepared TLS Finished message, <log details>

- **Message Code:** 12803

  Severity: INFO

  Message Text: Extracted TLS ChangeCipherSpec message

  Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS ChangeCipherSpec message.

  Local Target Message Format: <timestamp> <seq_num> 12803 INFO EAP: Extracted TLS ChangeCipherSpec message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12803 INFO EAP: Extracted TLS ChangeCipherSpec message, <log details>

- **Message Code:** 12804

  Severity: INFO

  Message Text: Extracted TLS Finished message

Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS Finished message. The client's supplicant is indicating that it is ready to finish the TLS handshake.

Local Target Message Format: <timestamp> <seq_num> 12804 INFO EAP: Extracted TLS Finished message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12804 INFO EAP: Extracted TLS Finished message, <log details>

- **Message Code:** 12805

  Severity: INFO

  Message Text: Extracted TLS ClientHello message

  Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS ClientHello message.

  Local Target Message Format: <timestamp> <seq_num> 12805 INFO EAP: Extracted TLS ClientHello message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12805 INFO EAP: Extracted TLS ClientHello message, <log details>

- **Message Code:** 12806

  Severity: INFO

  Message Text: Prepared TLS ServerHello message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS ServerHello message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12806 INFO EAP: Prepared TLS ServerHello message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12806 INFO EAP: Prepared TLS ServerHello message, <log details>

- **Message Code:** 12807

  Severity: INFO

  Message Text: Prepared TLS Certificate message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS Certificate message, in turn containing the ISE local server certificate, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12807 INFO EAP: Prepared TLS Certificate message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12807 INFO EAP: Prepared TLS Certificate message, <log details>

- **Message Code:** 12808

  Severity: INFO

  Message Text: Prepared TLS ServerKeyExchange message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS ServerKeyExchange message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12808 INFO EAP: Prepared TLS ServerKeyExchange message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12808 INFO EAP: Prepared TLS ServerKeyExchange message, <log details>

- **Message Code:** 12809

  Severity: INFO

  Message Text: Prepared TLS CertificateRequest message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS CertificateRequest message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12809 INFO EAP: Prepared TLS CertificateRequest message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12809 INFO EAP: Prepared TLS CertificateRequest message, <log details>

- **Message Code:** 12810

  Severity: INFO

  Message Text: Prepared TLS ServerDone message

  Message Description: As part of the TLS handshake currently in progress, prepared a TLS record containing a TLS ServerDone message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12810 INFO EAP: Prepared TLS ServerDone message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12810 INFO EAP: Prepared TLS ServerDone message, <log details>

- **Message Code:** 12811

  Severity: INFO

  Message Text: Extracted TLS Certificate message containing client certificate

  Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS Certificate message, in turn containing the client's certificate.

Local Target Message Format: <timestamp> <seq_num> 12811 INFO EAP: Extracted TLS Certificate message containing client certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12811 INFO EAP: Extracted TLS Certificate message containing client certificate, <log details>

- **Message Code:** 12812

  Severity: INFO

  Message Text: Extracted TLS ClientKeyExchange message

  Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS ClientKeyExchange message.

  Local Target Message Format: <timestamp> <seq_num> 12812 INFO EAP: Extracted TLS ClientKeyExchange message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12812 INFO EAP: Extracted TLS ClientKeyExchange message, <log details>

- **Message Code:** 12813

  Severity: INFO

  Message Text: Extracted TLS CertificateVerify message

  Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS CertificateVerify message.

  Local Target Message Format: <timestamp> <seq_num> 12813 INFO EAP: Extracted TLS CertificateVerify message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12813 INFO EAP: Extracted TLS CertificateVerify message, <log details>

- **Message Code:** 12814

  Severity: INFO

  Message Text: Prepared TLS Alert message

  Message Description: ISE has detected a problem with the TLS handshake currently in progress. Prepared a TLS record containing a TLS Alert message, for encapsulation within the outgoing EAP-Request packet, and for ultimate attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12814 INFO EAP: Prepared TLS Alert message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12814 INFO EAP: Prepared TLS Alert message, <log details>

- **Message Code:** 12815

  Severity: INFO

Message Text: Extracted TLS Alert message

Message Description: As part of the TLS handshake currently in progress, extracted from the EAP-Response packet a TLS record containing a TLS Alert message, indicating that the client has detected a problem with the handshake.

Local Target Message Format: <timestamp> <seq_num> 12815 INFO EAP: Extracted TLS Alert message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12815 INFO EAP: Extracted TLS Alert message, <log details>

- **Message Code:** 12816

  Severity: INFO

  Message Text: TLS handshake succeeded

  Message Description: The TLS handshake initiated by the client's supplicant has completed successfully.

  Local Target Message Format: <timestamp> <seq_num> 12816 INFO EAP: TLS handshake succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12816 INFO EAP: TLS handshake succeeded, <log details>

- **Message Code:** 12817

  Severity: INFO

  Message Text: TLS handshake failed

  Message Description: The TLS handshake initiated by the client's supplicant has failed.

  Local Target Message Format: <timestamp> <seq_num> 12817 INFO EAP: TLS handshake failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12817 INFO EAP: TLS handshake failed, <log details>

- **Message Code:** 12818

  Severity: WARN

  Message Text: Expected TLS acknowledge for last alert but received another message

  Message Description: ISE recently sent TLS alert to supplicant and expected TLS acknowledge from supplicant for the alert but received another message. This could be due to a possible incomformity in the implementation of the protocol between ISE and the supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12818 WARN EAP: Expected TLS acknowledge for last alert but received another message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12818 WARN EAP: Expected TLS acknowledge for last alert but received another message, <log details>

- **Message Code:** 12819

  Severity: WARN

  Message Text: Expected TLS acknowledge for handshake succeeded but received another message

  Message Description: ISE recently has successfully finished TLS handshake with the supplicant and expected TLS acknowledge from supplicant to confirm the handshake but received another message. This could be due to improper supplicant configuration or a possible incomformity in the implementation of the protocol between ISE and the supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12819 WARN EAP: Expected TLS acknowledge for handshake succeeded but received another message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12819 WARN EAP: Expected TLS acknowledge for handshake succeeded but received another message, <log details>

- **Message Code:** 12820

  Severity: WARN

  Message Text: The identity was locked due to previous failed attempts

  Message Description: Lock Identity feature is enabled and the identity was locked due to previous failed attempts

  Local Target Message Format: <timestamp> <seq_num>Failed-Attempt The identity was locked due to previous failed attempts WARN Lock Identity feature is enabled and the identity was locked due to previous failed attempts, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>Failed-Attempt The identity was locked due to previous failed attempts WARN Lock Identity feature is enabled and the identity was locked due to previous failed attempts, <log details>

- **Message Code:** 12830

  Severity: WARN

  Message Text: CRL verification bypassed

  Message Description: ISE was unable to download CRL; CRL verification bypassed

  Local Target Message Format: <timestamp> <seq_num> 12830 WARN CRL: CRL verification bypassed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12830 WARN CRL: CRL verification bypassed, <log details>

- **Message Code:** 12831

  Severity: WARN

  Message Text: Unable to download CRL

  Message Description: ISE was unable to download CRL; corresponding authentication has failed

  Local Target Message Format: <timestamp> <seq_num> 12831 WARN CRL: Unable to download CRL, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12831 WARN CRL: Unable to download CRL, <log details>

- **Message Code:** 12832

  Severity: WARN

  Message Text: Tunnel build with local server certificate is not yet active or it has already expired

  Message Description: Local server certificate has a specific period of time when it is active and can be used. The certificate cannot be used now because of either its 'Valid From' field is greater then the current date and time or its 'Valid To' field is less then the current date and time.

  Local Target Message Format: <timestamp> <seq_num> 12832 WARN EAP: Tunnel build with local server certificate is not yet active or it has already expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12832 WARN EAP: Tunnel build with local server certificate is not yet active or it has already expired, <log details>

- **Message Code:** 12833

  Severity: WARN

  Message Text: EAP-FAST provisioning mode is restricted to anonymous

  Message Description: Local server certificate is invalid because it is not yet active or it has already expired. Thus, the EAP-FAST provisioning mode is restricted to anonymous (if anonymous provisioning is allowed in configuration). Authenticated provisioning is prohibited even if it is allowed in configuration

  Local Target Message Format: <timestamp> <seq_num> 12833 WARN EAP: EAP-FAST provisioning mode is restricted to anonymous, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12833 WARN EAP: EAP-FAST provisioning mode is restricted to anonymous, <log details>

- **Message Code:** 12834

  Severity: WARN

  Message Text: ISE used a CRL that is not active yet or has expired

  Message Description: ISE used a CRL even though it is not yet active or has expired

  Local Target Message Format: <timestamp> <seq_num> 12834 WARN CRL: ISE used a CRL that is not active yet or has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12834 WARN CRL: ISE used a CRL that is not active yet or has expired, <log details>

- **Message Code:** 12835

  Severity: WARN

  Message Text: Expired certificate was accepted from the client

  Message Description: ISE accepted expired user or machine certificate per configuration

Local Target Message Format: <timestamp> <seq_num> 12835 WARN EAP: Expired certificate was accepted from the client, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12835 WARN EAP: Expired certificate was accepted from the client, <log details>

- **Message Code:** 12850

  Severity: WARN

  Message Text: Received NAK TLV. Client rejected the conversation

  Message Description: ISE expects for regular conversation continuation but client sent NAK TLV inside the tunnel. It means that client rejected conversation for some reason that is unknown to ISE. Known issue: CSSC 5.1.1.10 sends NAK TLV during EAP-FAST/EAP-GTC conversation to reject the conversation according to user's input.

  Local Target Message Format: <timestamp> <seq_num> 12850 WARN EAP: Received NAK TLV. Client rejected the conversation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12850 WARN EAP: Received NAK TLV. Client rejected the conversation, <log details>

- **Message Code:** 12851

  Severity: WARN

  Message Text: Received unexpected EAP NAK message. Client rejected the conversation

  Message Description: ISE expects for regular conversation continuation but client sent outer EAP method NAK message. It means that client rejected conversation for some reason that is unknown to ISE. Known issue: CSSC 5.1.1.10 sends outer EAP method NAK during EAP-FAST/EAP-GTC conversation to reject the conversation according to user's input.

  Local Target Message Format: <timestamp> <seq_num> 12851 WARN EAP: Received unexpected EAP NAK message. Client rejected the conversation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12851 WARN EAP: Received unexpected EAP NAK message. Client rejected the conversation, <log details>

- **Message Code:** 12852

  Severity: WARN

  Message Text: Cryptographic processing of received buffer failed

  Message Description: ISE received invalid encrypted buffer from client. Cryptographic processing of this buffer failed.

  Local Target Message Format: <timestamp> <seq_num> 12852 WARN EAP: Cryptographic processing of received buffer failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12852 WARN EAP: Cryptographic processing of received buffer failed, <log details>

- **Message Code:** 12853

  Severity: WARN

  Message Text: Empty EAP-GTC message received

  Message Description: ISE received empty EAP-GTC message inside the tunnel during EAP-FAST conversation. Known issue: CSSC 5.1.1.10 sends empty EaP-GTC message after it prompts user to retry entering passcode.

  Local Target Message Format: <timestamp> <seq_num> 12853 WARN EAP: Empty EAP-GTC message received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12853 WARN EAP: Empty EAP-GTC message received, <log details>

- **Message Code:** 12854

  Severity: WARN

  Message Text: Cannot authenticate because password was not present or was empty

  Message Description: ISE did not receive user password or received empty password. Plain password authentication cannot be performed with no password or empty password

  Local Target Message Format: <timestamp> <seq_num> 12854 WARN EAP: Cannot authenticate because password was not present or was empty, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12854 WARN EAP: Cannot authenticate because password was not present or was empty, <log details>

- **Message Code:** 12855

  Severity: INFO

  Message Text: PAC was not sent due to authorization failure

  Message Description: ISE did not send a PAC to the supplicant because authorization failed and thus the whole conversation is considered failed

  Local Target Message Format: <timestamp> <seq_num> 12855 INFO EAP: PAC was not sent due to authorization failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12855 INFO EAP: PAC was not sent due to authorization failure, <log details>

- **Message Code:** 12856

  Severity: INFO

  Message Text: User certificate was revoked by CRL verification

  Message Description: CRL verification returned revoked certificate status.

  Local Target Message Format: <timestamp> <seq_num> 12856 INFO EAP: User certificate was revoked by CRL verification, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12856 INFO EAP: User certificate was revoked by CRL verification, <log details>

- **Message Code:** 12857

  Severity: WARN

  Message Text: Client certificate authentication failed

  Message Description: Client certificate authentication failed

  Local Target Message Format: <timestamp> <seq_num> 12857 WARN EAP: Client certificate authentication failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12857 WARN EAP: Client certificate authentication failed, <log details>

- **Message Code:** 12858

  Severity: WARN

  Message Text: Server indicates that it will not send any more messages on this connection

  Message Description: Server indicates that it will not send any more messages on this connection

  Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that it will not send any more messages on this connection WARN Server indicates that it will not send any more messages on this connection, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that it will not send any more messages on this connection WARN Server indicates that it will not send any more messages on this connection, <log details>

- **Message Code:** 12859

  Severity: WARN

  Message Text: Server indicates that a field in the handshake was incorrect or inconsistent with other fields

  Message Description: Server indicates that a field in the handshake was incorrect or inconsistent with other fields

  Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that a field in the handshake was incorrect or inconsistent with other fields WARN Server indicates that a field in the handshake was incorrect or inconsistent with other fields, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that a field in the handshake was incorrect or inconsistent with other fields WARN Server indicates that a field in the handshake was incorrect or inconsistent with other fields, <log details>

- **Message Code:** 12860

  Severity: WARN

  Message Text: Invalid connection retry attempt from a client

Message Description: Invalid connection retry attempt from a client

Local Target Message Format: <timestamp> <seq_num>EAP Invalid connection retry attempt from a client WARN Invalid connection retry attempt from a client, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Invalid connection retry attempt from a client WARN Invalid connection retry attempt from a client, <log details>

- **Message Code:** 12861

  Severity: WARN

  Message Text: Server is canceling the handshake for some reason unrelated to a protocol failure

  Message Description: User is canceling the handshake for some reason unrelated to a protocol failure

  Local Target Message Format: <timestamp> <seq_num>EAP Server is canceling the handshake for some reason unrelated to a protocol failure WARN User is canceling the handshake for some reason unrelated to a protocol failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server is canceling the handshake for some reason unrelated to a protocol failure WARN User is canceling the handshake for some reason unrelated to a protocol failure, <log details>

- **Message Code:** 12862

  Severity: WARN

  Message Text: Client receives a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters

  Message Description: Client receive a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters

  Local Target Message Format: <timestamp> <seq_num>EAP Client receives a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters WARN Client receive a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client receives a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters WARN Client receive a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters, <log details>

- **Message Code:** 12863

  Severity: WARN

  Message Text: Server indicates that there is no server with the name provided by the client via the server_name extension

  Message Description: Server indicates that there is no server with the name provided by the client via the server_name extension

Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that there is no server with the name provided by the client via the server_name extension WARN Server indicates that there is no server with the name provided by the client via the server_name extension, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that there is no server with the name provided by the client via the server_name extension WARN Server indicates that there is no server with the name provided by the client via the server_name extension, <log details>

- **Message Code:** 12864

  Severity: WARN

  Message Text: Client indicates that an invalid or unacceptable OCSP response is provided by the server via the status_request extension

  Message Description: Client indicates that an invalid or unacceptable OCSP response is provided by the server via the status_request extension

  Local Target Message Format: <timestamp> <seq_num>EAP Client indicates that an invalid or unacceptable OCSP response is provided by the server via the status_request extension WARN Client indicates that an invalid or unacceptable OCSP response is provided by the server via the status_request extension, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client indicates that an invalid or unacceptable OCSP response is provided by the server via the status_request extension WARN Client indicates that an invalid or unacceptable OCSP response is provided by the server via the status_request extension, <log details>

- **Message Code:** 12865

  Severity: WARN

  Message Text: Server indicates that there is no acceptable PSK identity was provided by the client

  Message Description: Sent by servers when PSK key establishment is desired but no acceptable PSK identity is provided by the client. Sending this alert is OPTIONAL; servers MAY instead choose to send a decrypt_error alert to merely indicate an invalid PSK

  Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that there is no acceptable PSK identity was provided by the client WARN Sent by servers when PSK key establishment is desired but no acceptable PSK identity is provided by the client. Sending this alert is OPTIONAL; servers MAY instead choose to send a decrypt_error alert to merely indicate an invalid PSK, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that there is no acceptable PSK identity was provided by the client WARN Sent by servers when PSK key establishment is desired but no acceptable PSK identity is provided by the client. Sending this alert is OPTIONAL; servers MAY instead choose to send a decrypt_error alert to merely indicate an invalid PSK, <log details>

- **Message Code:** 12866

  Severity: WARN

  Message Text: Server indicates that a client certificate is desired but none was provided by the client

Message Description: Server indicates that a client certificate is desired but none was provided by the client

Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that a client certificate is desired but none was provided by the client WARN Server indicates that a client certificate is desired but none was provided by the client, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that a client certificate is desired but none was provided by the client WARN Server indicates that a client certificate is desired but none was provided by the client, <log details>

- **Message Code:** 12867

  Severity: WARN

  Message Text: Server indicates that a client application_layer_protocol_negotiation extension advertises only protocols that the server does not support

  Message Description: Server indicates that a client application_layer_protocol_negotiation extension advertises only protocols that the server does not support

  Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that a client application_layer_protocol_negotiation extension advertises only protocols that the server does not support WARN Server indicates that a client application_layer_protocol_negotiation extension advertises only protocols that the server does not support, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that a client application_layer_protocol_negotiation extension advertises only protocols that the server does not support WARN Server indicates that a client application_layer_protocol_negotiation extension advertises only protocols that the server does not support, <log details>

- **Message Code:** 12868

  Severity: WARN

  Message Text: Client indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in Certificate not first offered in the corresponding ClientHello or CertificateRequest

  Message Description: Client indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in a ServerHello or Certificate not first offered in the corresponding CertificateRequest

  Local Target Message Format: <timestamp> <seq_num>EAP Client indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in Certificate not first offered in the corresponding ClientHello or CertificateRequest WARN Client indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in a ServerHello or Certificate not first offered in the corresponding CertificateRequest, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in Certificate not first offered in the corresponding ClientHello or CertificateRequest WARN Client indicates that handshake message containing an extension known to

be prohibited for inclusion in the given handshake message, or including any extensions in a ServerHello or Certificate not first offered in the corresponding CertificateRequest, <log details>

- **Message Code:** 12869

  Severity: WARN

  Message Text: Client indicates that it will not send any more messages on this connection

  Message Description: Client indicates that it will not send any more messages on this connection

  Local Target Message Format: <timestamp> <seq_num>EAP Client indicates that it will not send any more messages on this connection WARN Client indicates that it will not send any more messages on this connection, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client indicates that it will not send any more messages on this connection WARN Client indicates that it will not send any more messages on this connection, <log details>

- **Message Code:** 12870

  Severity: WARN

  Message Text: Client is canceling the handshake for some reason unrelated to a protocol failure

  Message Description: Client is canceling the handshake for some reason unrelated to a protocol failure

  Local Target Message Format: <timestamp> <seq_num>EAP Client is canceling the handshake for some reason unrelated to a protocol failure WARN Client is canceling the handshake for some reason unrelated to a protocol failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Client is canceling the handshake for some reason unrelated to a protocol failure WARN Client is canceling the handshake for some reason unrelated to a protocol failure, <log details>

- **Message Code:** 12871

  Severity: WARN

  Message Text: Server receives a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters

  Message Description: Server receive a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters

  Local Target Message Format: <timestamp> <seq_num>EAP Server receives a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters WARN Server receive a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server receives a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters WARN Server receive a handshake message not containing an extension that is mandatory to send for the offered TLS version or other negotiated parameters, <log details>

- **Message Code:** 12872

Severity: WARN

Message Text: Server indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in Certificate not first offered in the corresponding ClientHello or CertificateRequest

Message Description: Server indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in a ServerHello or Certificate not first offered in the corresponding ClientHello or CertificateRequest

Local Target Message Format: <timestamp> <seq_num>EAP Server indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in Certificate not first offered in the corresponding ClientHello or CertificateRequest WARN Server indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in a ServerHello or Certificate not first offered in the corresponding ClientHello or CertificateRequest, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>EAP Server indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in Certificate not first offered in the corresponding ClientHello or CertificateRequest WARN Server indicates that handshake message containing an extension known to be prohibited for inclusion in the given handshake message, or including any extensions in a ServerHello or Certificate not first offered in the corresponding ClientHello or CertificateRequest, <log details>

- **Message Code:** 12902

  Severity: WARN

  Message Text: NAS sends RADIUS accounting modem start messages too frequently

  Message Description: NAS sends RADIUS accounting modem start messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting modem start messages too frequently WARN NAS sends RADIUS accounting modem start messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting modem start messages too frequently WARN NAS sends RADIUS accounting modem start messages too frequently, <log details>

- **Message Code:** 12903

  Severity: WARN

  Message Text: NAS sends RADIUS accounting modem stop messages too frequently

  Message Description: NAS sends RADIUS accounting modem stop messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting modem stop messages too frequently WARN NAS sends RADIUS accounting modem stop messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting modem stop messages too frequently WARN NAS sends RADIUS accounting modem stop messages too frequently, <log details>

- **Message Code:** 12904

  Severity: WARN

  Message Text: NAS sends RADIUS accounting cancel messages too frequently

  Message Description: NAS sends RADIUS accounting cancel messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting cancel messages too frequently WARN NAS sends RADIUS accounting cancel messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting cancel messages too frequently WARN NAS sends RADIUS accounting cancel messages too frequently, <log details>

- **Message Code:** 12905

  Severity: WARN

  Message Text: NAS sends RADIUS accounting on messages too frequently

  Message Description: NAS sends RADIUS accounting on messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting on messages too frequently WARN NAS sends RADIUS accounting on messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting on messages too frequently WARN NAS sends RADIUS accounting on messages too frequently, <log details>

- **Message Code:** 12906

  Severity: WARN

  Message Text: NAS sends RADIUS accounting off messages too frequently

  Message Description: NAS sends RADIUS accounting off messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting off messages too frequently WARN NAS sends RADIUS accounting off messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting off messages too frequently WARN NAS sends RADIUS accounting off messages too frequently, <log details>

- **Message Code:** 12907

  Severity: WARN

  Message Text: NAS sends RADIUS accounting tunnel start messages too frequently

  Message Description: NAS sends RADIUS accounting tunnel start messages too frequently

Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel start messages too frequently WARN NAS sends RADIUS accounting tunnel start messages too frequently, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel start messages too frequently WARN NAS sends RADIUS accounting tunnel start messages too frequently, <log details>

- **Message Code:** 12908

  Severity: WARN

  Message Text: NAS sends RADIUS accounting tunnel stop messages too frequently

  Message Description: NAS sends RADIUS accounting tunnel stop messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel stop messages too frequently WARN NAS sends RADIUS accounting tunnel stop messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel stop messages too frequently WARN NAS sends RADIUS accounting tunnel stop messages too frequently, <log details>

- **Message Code:** 12909

  Severity: WARN

  Message Text: NAS sends RADIUS accounting tunnel reject messages too frequently

  Message Description: NAS sends RADIUS accounting tunnel reject messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel reject messages too frequently WARN NAS sends RADIUS accounting tunnel reject messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel reject messages too frequently WARN NAS sends RADIUS accounting tunnel reject messages too frequently, <log details>

- **Message Code:** 12910

  Severity: WARN

  Message Text: NAS sends RADIUS accounting tunnel link start messages too frequently

  Message Description: NAS sends RADIUS accounting tunnel link start messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel link start messages too frequently WARN NAS sends RADIUS accounting tunnel link start messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel link start messages too frequently WARN NAS sends RADIUS accounting tunnel link start messages too frequently, <log details>

- **Message Code:** 12911

  Severity: WARN

  Message Text: NAS sends RADIUS accounting tunnel link stop messages too frequently

  Message Description: NAS sends RADIUS accounting tunnel link stop messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel link stop messages too frequently WARN NAS sends RADIUS accounting tunnel link stop messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel link stop messages too frequently WARN NAS sends RADIUS accounting tunnel link stop messages too frequently, <log details>

- **Message Code:** 12912

  Severity: WARN

  Message Text: NAS sends RADIUS accounting tunnel link reject messages too frequently

  Message Description: NAS sends RADIUS accounting tunnel link reject messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel link reject messages too frequently WARN NAS sends RADIUS accounting tunnel link reject messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting tunnel link reject messages too frequently WARN NAS sends RADIUS accounting tunnel link reject messages too frequently, <log details>

- **Message Code:** 12913

  Severity: WARN

  Message Text: NAS sends RADIUS accounting reserved for failed messages too frequently

  Message Description: NAS sends RADIUS accounting reserved for failed messages too frequently

  Local Target Message Format: <timestamp> <seq_num>RADIUS NAS sends RADIUS accounting reserved for failed messages too frequently WARN NAS sends RADIUS accounting reserved for failed messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>RADIUS NAS sends RADIUS accounting reserved for failed messages too frequently WARN NAS sends RADIUS accounting reserved for failed messages too frequently, <log details>

- **Message Code:** 12914

  Severity: INFO

  Message Text: Using weak TLS cipher

  Message Description: Using weak TLS cipher

  Local Target Message Format: <timestamp> <seq_num> 12914 INFO EAP: Using weak TLS cipher, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12914 INFO EAP: Using weak TLS cipher, <log details>

- **Message Code:** 12915

  Severity: WARN

  Message Text: PEAP version negotiation failed

  Message Description: PEAP version negotiation failed because supplicant proposed version 1 while the option 'Allow PEAPv 0 Only' is turned on.

  Local Target Message Format: <timestamp> <seq_num> 12915 WARN EAP: PEAP version negotiation failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12915 WARN EAP: PEAP version negotiation failed, <log details>

- **Message Code:** 12916

  Severity: WARN

  Message Text: Expected TLS acknowledge for TLS fragment but received another message

  Message Description: ISE recently has sent another TLS fragment to the supplicant and expected TLS acknowledge from supplicant to confirm the fragment before sending it the next one but received another message. This could be due to improper supplicant configuration or a possible incomformity in the implementation of the protocol between ISE and the supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12916 WARN EAP: Expected TLS acknowledge for TLS fragment but received another message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12916 WARN EAP: Expected TLS acknowledge for TLS fragment but received another message, <log details>

- **Message Code:** 12917

  Severity: WARN

  Message Text: Expected TLS acknowledge for PEAPv1 protected termination but received another message

  Message Description: ISE recently has sent PEAPv1 protected termination EAP Success message to the supplicant and expected TLS acknowledge from supplicant to confirm that but received another message. This could be due to improper supplicant configuration or a possible incomformity in the implementation of the protocol between ISE and the supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12917 WARN EAP: Expected TLS acknowledge for PEAPv1 protected termination but received another message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12917 WARN EAP: Expected TLS acknowledge for PEAPv1 protected termination but received another message, <log details>

- **Message Code:** 12918

Severity: WARN

Message Text: Supplicant sent unmatched EAP Response packet identifier

Message Description: ISE sent EAP Request to the supplicant with a certain identifier. According to EAP specification supplicant must respond to this request with EAP Response packet with the same identifier. However the EAP identifier in the response was different from the request.

Local Target Message Format: <timestamp> <seq_num> 12918 WARN EAP: Supplicant sent unmatched EAP Response packet identifier, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12918 WARN EAP: Supplicant sent unmatched EAP Response packet identifier, <log details>

- **Message Code:** 12919

  Severity: WARN

  Message Text: Supplicant sent unmatched inner EAP Response packet identifier

  Message Description: ISE sent inner EAP Request to the supplicant with a certain identifier. According to EAP specification supplicant must respond to this request with EAP Response packet with the same identifier. However the EAP identifier in the response was different from the request.

  Local Target Message Format: <timestamp> <seq_num> 12919 WARN EAP: Supplicant sent unmatched inner EAP Response packet identifier, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12919 WARN EAP: Supplicant sent unmatched inner EAP Response packet identifier, <log details>

- **Message Code:** 12921

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during TEAP tunnel establishment

  Message Description: Supplicant stopped responding to ISE during TEAP tunnel establishment

  Local Target Message Format: <timestamp> <seq_num>12921 WARN Failed-Attempt Supplicant stopped responding to ISE during TEAP tunnel establishment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12921 WARN Failed-Attempt Supplicant stopped responding to ISE during TEAP tunnel establishment, <log details>

- **Message Code:** 12928

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during TEAP protected termination

  Message Description: Supplicant stopped responding to ISE during TEAP protected termination

  Local Target Message Format: <timestamp> <seq_num>12928 WARN Failed-Attempt Supplicant stopped responding to ISE during TEAP protected termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12928 WARN Failed-Attempt Supplicant stopped responding to ISE during TEAP protected termination, <log details>

- **Message Code:** 12929

  Severity: WARN

  Message Text: NAS sends RADIUS accounting update messages too frequently

  Message Description: NAS sends RADIUS accounting update messages too frequently

  Local Target Message Format: <timestamp> <seq_num> 12929 WARN RADIUS: NAS sends RADIUS accounting update messages too frequently, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12929 WARN RADIUS: NAS sends RADIUS accounting update messages too frequently, <log details>

- **Message Code:** 12930

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE after sending it the first PEAP message

  Message Description: Supplicant stopped responding to ISE after sending it the first PEAP message

  Local Target Message Format: <timestamp> <seq_num> 12930 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first PEAP message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12930 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first PEAP message, <log details>

- **Message Code:** 12931

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE after sending it the first EAP-TLS message

  Message Description: Supplicant stopped responding to ISE after sending it the first EAP-TLS message

  Local Target Message Format: <timestamp> <seq_num> 12931 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first EAP-TLS message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12931 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first EAP-TLS message, <log details>

- **Message Code:** 12932

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE after sending it the first EAP-FAST message

  Message Description: Supplicant stopped responding to ISE after sending it the first EAP-FAST message

  Local Target Message Format: <timestamp> <seq_num> 12932 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first EAP-FAST message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12932 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first EAP-FAST message, <log details>

- **Message Code:** 12933

Severity: WARN

Message Text: Supplicant stopped responding to ISE during EAP-FAST tunnel establishment

Message Description: Supplicant stopped responding to ISE during EAP-FAST tunnel establishment

Local Target Message Format: <timestamp> <seq_num> 12933 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-FAST tunnel establishment, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12933 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-FAST tunnel establishment, <log details>

- **Message Code:** 12934

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during PEAP tunnel establishment

  Message Description: Supplicant stopped responding to ISE during PEAP tunnel establishment

  Local Target Message Format: <timestamp> <seq_num> 12934 WARN Failed-Attempt: Supplicant stopped responding to ISE during PEAP tunnel establishment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12934 WARN Failed-Attempt: Supplicant stopped responding to ISE during PEAP tunnel establishment, <log details>

- **Message Code:** 12935

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during EAP-TLS certificate exchange

  Message Description: Supplicant stopped responding to ISE during EAP-TLS certificate exchange

  Local Target Message Format: <timestamp> <seq_num> 12935 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-TLS certificate exchange, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12935 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-TLS certificate exchange, <log details>

- **Message Code:** 12936

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE after sending it inner EAP Identity Request

  Message Description: Supplicant stopped responding to ISE after sending it inner EAP Identity Request

  Local Target Message Format: <timestamp> <seq_num> 12936 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it inner EAP Identity Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12936 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it inner EAP Identity Request, <log details>

- **Message Code:** 12937

  Severity: WARN

Message Text: Supplicant stopped responding to ISE after sending it the first inner EAP-MSCHAPv2 message

Message Description: Supplicant stopped responding to ISE after sending it the first inner EAP-MSCHAPv2 message

Local Target Message Format: <timestamp> <seq_num> 12937 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first inner EAP-MSCHAPv2 message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12937 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first inner EAP-MSCHAPv2 message, <log details>

- **Message Code:** 12938

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE after sending it the first inner EAP-GTC message

  Message Description: Supplicant stopped responding to ISE after sending it the first inner EAP-GTC message

  Local Target Message Format: <timestamp> <seq_num> 12938 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first inner EAP-GTC message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12938 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first inner EAP-GTC message, <log details>

- **Message Code:** 12939

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE after sending it the first inner EAP-TLS message

  Message Description: Supplicant stopped responding to ISE after sending it the first inner EAP-TLS message

  Local Target Message Format: <timestamp> <seq_num> 12939 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first inner EAP-TLS message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12939 WARN Failed-Attempt: Supplicant stopped responding to ISE after sending it the first inner EAP-TLS message, <log details>

- **Message Code:** 12940

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during conducting inner EAP-MSCHAPv2 method

  Message Description: Supplicant stopped responding to ISE during conducting inner EAP-MSCHAPv2 method

  Local Target Message Format: <timestamp> <seq_num> 12940 WARN Failed-Attempt: Supplicant stopped responding to ISE during conducting inner EAP-MSCHAPv2 method, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12940 WARN Failed-Attempt: Supplicant stopped responding to ISE during conducting inner EAP-MSCHAPv2 method, <log details>

- **Message Code:** 12941

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during conducting inner EAP-GTC method

  Message Description: Supplicant stopped responding to ISE during conducting inner EAP-GTC method

  Local Target Message Format: <timestamp> <seq_num> 12941 WARN Failed-Attempt: Supplicant stopped responding to ISE during conducting inner EAP-GTC method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12941 WARN Failed-Attempt: Supplicant stopped responding to ISE during conducting inner EAP-GTC method, <log details>

- **Message Code:** 12942

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during conducting inner EAP-TLS method

  Message Description: Supplicant stopped responding to ISE during conducting inner EAP-TLS method

  Local Target Message Format: <timestamp> <seq_num> 12942 WARN Failed-Attempt: Supplicant stopped responding to ISE during conducting inner EAP-TLS method, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12942 WARN Failed-Attempt: Supplicant stopped responding to ISE during conducting inner EAP-TLS method, <log details>

- **Message Code:** 12943

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during PEAPv0 protected termination

  Message Description: Supplicant stopped responding to ISE during PEAPv0 protected termination

  Local Target Message Format: <timestamp> <seq_num> 12943 WARN Failed-Attempt: Supplicant stopped responding to ISE during PEAPv0 protected termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12943 WARN Failed-Attempt: Supplicant stopped responding to ISE during PEAPv0 protected termination, <log details>

- **Message Code:** 12944

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during PEAPv1 protected termination

  Message Description: Supplicant stopped responding to ISE during PEAPv1 protected termination

  Local Target Message Format: <timestamp> <seq_num> 12944 WARN Failed-Attempt: Supplicant stopped responding to ISE during PEAPv1 protected termination, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12944 WARN Failed-Attempt: Supplicant stopped responding to ISE during PEAPv1 protected termination, <log details>

- **Message Code:** 12945

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during EAP-FAST protected termination

  Message Description: Supplicant stopped responding to ISE during EAP-FAST protected termination

  Local Target Message Format: <timestamp> <seq_num> 12945 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-FAST protected termination, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12945 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-FAST protected termination, <log details>

- **Message Code:** 12946

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during LEAP

  Message Description: Supplicant stopped responding to ISE during LEAP

  Local Target Message Format: <timestamp> <seq_num> 12946 WARN Failed-Attempt: Supplicant stopped responding to ISE during LEAP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12946 WARN Failed-Attempt: Supplicant stopped responding to ISE during LEAP, <log details>

- **Message Code:** 12947

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during EAP-MD5

  Message Description: Supplicant stopped responding to ISE during EAP-MD5

  Local Target Message Format: <timestamp> <seq_num> 12947 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-MD5, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12947 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-MD5, <log details>

- **Message Code:** 12948

  Severity: WARN

  Message Text: Supplicant sent unexpected unencrypted TLS handshake message instead of TLS application data in PEAP protocol

  Message Description: Supplicant sent unexpected unencrypted TLS handshake message instead of TLS application data in PEAP protocol

Local Target Message Format: <timestamp> <seq_num> 12948 WARN Failed-Attempt: Supplicant sent unexpected unencrypted TLS handshake message instead of TLS application data in PEAP protocol, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12948 WARN Failed-Attempt: Supplicant sent unexpected unencrypted TLS handshake message instead of TLS application data in PEAP protocol, <log details>

- **Message Code:** 12949

  Severity: WARN

  Message Text: Supplicant sent malformed PEAP message - wrong block cioher padding

  Message Description: Supplicant sent malformed PEAP message - wrong block cioher padding

  Local Target Message Format: <timestamp> <seq_num> 12949 WARN Failed-Attempt: Supplicant sent malformed PEAP message - wrong block cioher padding, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12949 WARN Failed-Attempt: Supplicant sent malformed PEAP message - wrong block cioher padding, <log details>

- **Message Code:** 12950

  Severity: WARN

  Message Text: Supplicant sent malformed PEAP message - bad record MAC

  Message Description: Supplicant sent malformed PEAP message - bad record MAC

  Local Target Message Format: <timestamp> <seq_num> 12950 WARN Failed-Attempt: Supplicant sent malformed PEAP message - bad record MAC, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12950 WARN Failed-Attempt: Supplicant sent malformed PEAP message - bad record MAC, <log details>

- **Message Code:** 12951

  Severity: WARN

  Message Text: Unexpected renegotiation received. Renegotiation is not supported in PEAP

  Message Description: Unexpected renegotiation received. Renegotiation is not supported in PEAP

  Local Target Message Format: <timestamp> <seq_num> 12951 WARN Failed-Attempt: Unexpected renegotiation received. Renegotiation is not supported in PEAP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12951 WARN Failed-Attempt: Unexpected renegotiation received. Renegotiation is not supported in PEAP, <log details>

- **Message Code:** 12952

  Severity: WARN

  Message Text: Received EAP packet from the middle of conversation but the conversation was not started on this PSN

Message Description: Session does not belong to this PSN according to hostname. Possible unexpected NAD behavior. Maybe NAD sent a packet from the middle of the conversation with another PSN.

Local Target Message Format: <timestamp> <seq_num> 12952 WARN EAP: Received EAP packet from the middle of conversation but the conversation was not started on this PSN, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12952 WARN EAP: Received EAP packet from the middle of conversation but the conversation was not started on this PSN, <log details>

- **Message Code:** 12953

  Severity: WARN

  Message Text: Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist

  Message Description: Session was not found on this PSN. Possible unexpected NAD behavior. Session belongs to this PSN according to hostname but may has already been reaped by timeout. This packet arrived too late.

  Local Target Message Format: <timestamp> <seq_num> 12953 WARN EAP: Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12953 WARN EAP: Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist, <log details>

- **Message Code:** 12954

  Severity: WARN

  Message Text: CRL signature check failed

  Message Description: The CRL found for specific CA does not fit the CA. Possible usage of more than one CA with the same name and CRL with no AKI for one of them. So ISE cannot determine to which CA the CRL belongs.

  Local Target Message Format: <timestamp> <seq_num> 12954 WARN EAP: CRL signature check failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12954 WARN EAP: CRL signature check failed, <log details>

- **Message Code:** 12955

  Severity: WARN

  Message Text: RADIUS request that contains EAP message must contain MessageAuthenticator attribute

  Message Description: RADIUS request that contains EAP message must contain MessageAuthenticator attribute

  Local Target Message Format: <timestamp> <seq_num> 12955 WARN RADIUS: RADIUS request that contains EAP message must contain MessageAuthenticator attribute, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12955 WARN RADIUS: RADIUS request that contains EAP message must contain MessageAuthenticator attribute, <log details>

- **Message Code:** 12956

  Severity: WARN

  Message Text: Client certificate validation failed due to name constraints permitted subtree violation

  Message Description: Client certificate validation failed due to name constraints permitted subtree violation

  Local Target Message Format: <timestamp> <seq_num> 12956 WARN RADIUS: Client certificate validation failed due to name constraints permitted subtree violation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12956 WARN RADIUS: Client certificate validation failed due to name constraints permitted subtree violation, <log details>

- **Message Code:** 12957

  Severity: WARN

  Message Text: Client certificate validation failed due to name constraints excluded subtree violation

  Message Description: Client certificate validation failed due to name constraints excluded subtree violation

  Local Target Message Format: <timestamp> <seq_num> 12957 WARN RADIUS: Client certificate validation failed due to name constraints excluded subtree violation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12957 WARN RADIUS: Client certificate validation failed due to name constraints excluded subtree violation, <log details>

- **Message Code:** 12958

  Severity: WARN

  Message Text: Client certificate validation failed due to min or max name constraints values violation

  Message Description: Client certificate validation failed due to min or max name constraints values violation

  Local Target Message Format: <timestamp> <seq_num> 12958 WARN RADIUS: Client certificate validation failed due to min or max name constraints values violation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12958 WARN RADIUS: Client certificate validation failed due to min or max name constraints values violation, <log details>

- **Message Code:** 12959

  Severity: WARN

  Message Text: Client certificate validation failed due to unsupported name constraint type

  Message Description: Client certificate validation failed due to unsupported name constraint type

Local Target Message Format: <timestamp> <seq_num> 12959 WARN RADIUS: Client certificate validation failed due to unsupported name constraint type, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12959 WARN RADIUS: Client certificate validation failed due to unsupported name constraint type, <log details>

- **Message Code:** 12960

  Severity: WARN

  Message Text: Client certificate validation failed due to bad or unsupported name constraint syntax

  Message Description: Client certificate validation failed due to bad or unsupported name constraint syntax

  Local Target Message Format: <timestamp> <seq_num> 12960 WARN RADIUS: Client certificate validation failed due to bad or unsupported name constraint syntax, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12960 WARN RADIUS: Client certificate validation failed due to bad or unsupported name constraint syntax, <log details>

- **Message Code:** 12961

  Severity: WARN

  Message Text: Client certificate validation failed due to bad or unsupported name syntax of the constraint

  Message Description: Client certificate validation failed due to bad or unsupported name syntax of the constraint

  Local Target Message Format: <timestamp> <seq_num> 12961 WARN RADIUS: Client certificate validation failed due to bad or unsupported name syntax of the constraint, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12961 WARN RADIUS: Client certificate validation failed due to bad or unsupported name syntax of the constraint, <log details>

- **Message Code:** 12962

  Severity: WARN

  Message Text: Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID

  Message Description: Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID

  Local Target Message Format: <timestamp> <seq_num> 12962 WARN RADIUS: Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12962 WARN RADIUS: Reject User Authorization PAC since its Initiator-ID does not match the Tunnel PAC Initiator-ID, <log details>

- **Message Code:** 12963

  Severity: WARN

Message Text: Received malformed EAP Payload TLV

Message Description: ISE received malformed EAP Payload TLV from the supplicat

Local Target Message Format: <timestamp> <seq_num> 12963 WARN RADIUS: Received malformed EAP Payload TLV, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12963 WARN RADIUS: Received malformed EAP Payload TLV, <log details>

- **Message Code:** 12964

  Severity: DEBUG

  Message Text: Sent EAP Result TLV indicating success

  Message Description: ISE sent EAP Result TLV indicating success

  Local Target Message Format: <timestamp> <seq_num> 12964 DEBUG RADIUS: Sent EAP Result TLV indicating success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12964 DEBUG RADIUS: Sent EAP Result TLV indicating success, <log details>

- **Message Code:** 12965

  Severity: DEBUG

  Message Text: Sent EAP Result TLV indicating failure

  Message Description: ISE sent EAP Result TLV indicating failure

  Local Target Message Format: <timestamp> <seq_num> 12965 DEBUG RADIUS: Sent EAP Result TLV indicating failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12965 DEBUG RADIUS: Sent EAP Result TLV indicating failure, <log details>

- **Message Code:** 12966

  Severity: DEBUG

  Message Text: Sent EAP Intermediate Result TLV indicating success

  Message Description: ISE sent EAP Intermediate Result TLV indicating success

  Local Target Message Format: <timestamp> <seq_num> 12966 DEBUG RADIUS: Sent EAP Intermediate Result TLV indicating success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12966 DEBUG RADIUS: Sent EAP Intermediate Result TLV indicating success, <log details>

- **Message Code:** 12967

  Severity: DEBUG

  Message Text: Sent EAP Intermediate Result TLV indicating failure

Message Description: ISE sent EAP Intermediate Result TLV indicating failure

Local Target Message Format: <timestamp> <seq_num> 12967 DEBUG RADIUS: Sent EAP Intermediate Result TLV indicating failure, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12967 DEBUG RADIUS: Sent EAP Intermediate Result TLV indicating failure, <log details>

- **Message Code:** 12968

  Severity: WARN

  Message Text: Client didn't provide suitable ciphers

  Message Description: Client didn't provide suitable ciphers that are allowed on ISE

  Local Target Message Format: <timestamp> <seq_num>12968 WARN EAP Client didn't provide suitable ciphers, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>12968 WARN EAP Client didn't provide suitable ciphers, <log details>

- **Message Code:** 12970

  Severity: INFO

  Message Text: EAP-TTLS inner method finished with failure

  Message Description: EAP-TTLS inner method finished with failure.

  Local Target Message Format: <timestamp> <seq_num> 12970 INFO EAP: EAP-TTLS inner method finished with failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12970 INFO EAP: EAP-TTLS inner method finished with failure, <log details>

- **Message Code:** 12971

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-TTLS challenge-response

  Message Description: Continuing the EAP-TTLS protocol; processing the EAP-TTLS challenge-response in the extracted EAP-Response.

  Local Target Message Format: <timestamp> <seq_num> 12971 INFO EAP: Extracted EAP-Response containing EAP-TTLS challenge-response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12971 INFO EAP: Extracted EAP-Response containing EAP-TTLS challenge-response, <log details>

- **Message Code:** 12972

  Severity: WARN

  Message Text: EAP-TTLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

Message Description: EAP-TTLS failed SSL/TLS handshake because the client rejected the ISE local-certificate

Local Target Message Format: <timestamp> <seq_num> 12972 WARN EAP: EAP-TTLS failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12972 WARN EAP: EAP-TTLS failed SSL/TLS handshake because the client rejected the ISE local-certificate, <log details>

- **Message Code:** 12973

  Severity: WARN

  Message Text: EAP-TTLS failed SSL/TLS handshake after a client alert

  Message Description: EAP-TTLS failed SSL/TLS handshake after a client alert

  Local Target Message Format: <timestamp> <seq_num> 12973 WARN EAP: EAP-TTLS failed SSL/TLS handshake after a client alert, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12973 WARN EAP: EAP-TTLS failed SSL/TLS handshake after a client alert, <log details>

- **Message Code:** 12974

  Severity: WARN

  Message Text: EAP-TTLS handshake failed

  Message Description: EAP-TTLS handshake failed.

  Local Target Message Format: <timestamp> <seq_num> 12974 WARN EAP: EAP-TTLS handshake failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12974 WARN EAP: EAP-TTLS handshake failed, <log details>

- **Message Code:** 12975

  Severity: INFO

  Message Text: EAP-TTLS authentication succeeded

  Message Description: EAP-TTLS authentication succeeded.

  Local Target Message Format: <timestamp> <seq_num> 12975 INFO EAP: EAP-TTLS authentication succeeded, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12975 INFO EAP: EAP-TTLS authentication succeeded, <log details>

- **Message Code:** 12976

  Severity: INFO

  Message Text: EAP-TTLS authentication failed

Message Description: EAP-TTLS authentication failed.

Local Target Message Format: <timestamp> <seq_num> 12976 INFO EAP: EAP-TTLS authentication failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12976 INFO EAP: EAP-TTLS authentication failed, <log details>

- **Message Code:** 12977

  Severity: INFO

  Message Text: EAP-TTLS built tunnel based on earlier generated keys, this will imply authentication

  Message Description: EAP-TTLS short handshake finished successfully - built tunnel for purpose of authentication.

  Local Target Message Format: <timestamp> <seq_num> 12977 INFO EAP: EAP-TTLS built tunnel based on earlier generated keys, this will imply authentication, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12977 INFO EAP: EAP-TTLS built tunnel based on earlier generated keys, this will imply authentication, <log details>

- **Message Code:** 12978

  Severity: INFO

  Message Text: Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated

  Message Description: Extracted from the RADIUS message an EAP-Response packet containing a EAP-TTLS challenge-response, and accepting EAP-TTLS as negotiated.

  Local Target Message Format: <timestamp> <seq_num> 12978 INFO EAP: Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12978 INFO EAP: Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated, <log details>

- **Message Code:** 12979

  Severity: INFO

  Message Text: Extracted EAP-Response/NAK requesting to use EAP-TTLS instead

  Message Description: Extracted from the RADIUS message an EAP-Response/NAK packet, rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-TTLS instead, per the configuration of the client's supplicant.

  Local Target Message Format: <timestamp> <seq_num> 12979 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-TTLS instead, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12979 INFO EAP: Extracted EAP-Response/NAK requesting to use EAP-TTLS instead, <log details>

- **Message Code:** 12980

  Severity: WARN

  Message Text: Failed to negotiate EAP because EAP-TTLS not allowed in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use EAP-TTLS instead. However, EAP-TTLS is not allowed in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12980 WARN EAP: Failed to negotiate EAP because EAP-TTLS not allowed in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12980 WARN EAP: Failed to negotiate EAP because EAP-TTLS not allowed in the Allowed Protocols, <log details>

- **Message Code:** 12981

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during EAP-TTLS tunnel establishment

  Message Description: Supplicant stopped responding to ISE during EAP-TTLS tunnel establishment

  Local Target Message Format: <timestamp> <seq_num> 12981 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-TTLS tunnel establishment, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12981 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-TTLS tunnel establishment, <log details>

- **Message Code:** 12982

  Severity: WARN

  Message Text: Supplicant stopped responding to ISE during EAP-TTLS plain inner MSCHAPv2 authentication flow

  Message Description: Supplicant stopped responding to ISE during EAP-TTLS plain inner MSCHAPv2 authentication flow

  Local Target Message Format: <timestamp> <seq_num> 12982 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-TTLS plain inner MSCHAPv2 authentication flow, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12982 WARN Failed-Attempt: Supplicant stopped responding to ISE during EAP-TTLS plain inner MSCHAPv2 authentication flow, <log details>

- **Message Code:** 12983

  Severity: INFO

  Message Text: Prepared EAP-Request proposing EAP-TTLS with challenge

  Message Description: Created an EAP-Request packet proposing to use the EAP-TTLS protocol, and also providing a EAP-TTLS challenge, for attachment to a RADIUS message. The EAP-TTLS protocol was proposed because it was one of the EAP-based protocols allowed in Allowed Protocols.

Local Target Message Format: <timestamp> <seq_num> 12983 INFO EAP: Prepared EAP-Request proposing EAP-TTLS with challenge, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12983 INFO EAP: Prepared EAP-Request proposing EAP-TTLS with challenge, <log details>

- **Message Code:** 12984

  Severity: WARN

  Message Text: Unexpected renegotiation received. Renegotiation is not supported in EAP_TTLS

  Message Description: Unexpected renegotiation received. Renegotiation is not supported in EAP_TTLS

  Local Target Message Format: <timestamp> <seq_num> 12984 WARN Failed-Attempt: Unexpected renegotiation received. Renegotiation is not supported in EAP_TTLS, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12984 WARN Failed-Attempt: Unexpected renegotiation received. Renegotiation is not supported in EAP_TTLS, <log details>

- **Message Code:** 12985

  Severity: INFO

  Message Text: Prepared EAP-Request with another EAP-TTLS challenge

  Message Description: As part of the continuation of the EAP-TTLS protocol, created an EAP-Request packet containing another EAP-TTLS challenge, for attachment to a RADIUS message.

  Local Target Message Format: <timestamp> <seq_num> 12985 INFO EAP: Prepared EAP-Request with another EAP-TTLS challenge, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12985 INFO EAP: Prepared EAP-Request with another EAP-TTLS challenge, <log details>

- **Message Code:** 12986

  Severity: WARN

  Message Text: Client requested TLSv1.0 or TLSv1.1 that is not allowed

  Message Description: Client requested TLSv1.0 or TLSv1.1 as the highest version but it is not allowed in the security settings

  Local Target Message Format: <timestamp> <seq_num> 12986 WARN EAP: Client requested TLSv1.0 or TLSv1.1 that is not allowed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12986 WARN EAP: Client requested TLSv1.0 or TLSv1.1 that is not allowed, <log details>

- **Message Code:** 12987

  Severity: INFO

  Message Text: Take OCSP servers list from AIA extension of client certificate

  Message Description: Take OCSP servers list from AIA extension of client certificate

Local Target Message Format: <timestamp> <seq_num> 12987 INFO EAP: Take OCSP servers list from AIA extension of client certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12987 INFO EAP: Take OCSP servers list from AIA extension of client certificate, <log details>

- **Message Code:** 12988

  Severity: INFO

  Message Text: Take OCSP servers list from OCSP service configuration

  Message Description: Take OCSP servers list from OCSP service configuration

  Local Target Message Format: <timestamp> <seq_num> 12988 INFO EAP: Take OCSP servers list from OCSP service configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12988 INFO EAP: Take OCSP servers list from OCSP service configuration, <log details>

- **Message Code:** 12989

  Severity: INFO

  Message Text: Sent an OCSP request to the next OCSP server in the list

  Message Description: Sent an OCSP request to the next OCSP server in the list

  Local Target Message Format: <timestamp> <seq_num> 12989 INFO EAP: Sent an OCSP request to the next OCSP server in the list, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12989 INFO EAP: Sent an OCSP request to the next OCSP server in the list, <log details>

- **Message Code:** 12990

  Severity: WARN

  Message Text: No valid OCSP server URLs found in the AIA extension of client certificate

  Message Description: If the OCSP service was configured to take OCSP servers list from the AIA extension of client certificate then at least one valid OCSP server URL must be present.

  Local Target Message Format: <timestamp> <seq_num> 12990 WARN EAP: No valid OCSP server URLs found in the AIA extension of client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12990 WARN EAP: No valid OCSP server URLs found in the AIA extension of client certificate, <log details>

- **Message Code:** 12991

  Severity: INFO

  Message Text: No more OCSP servers in AIA estension of client certificate

  Message Description: No more OCSP servers in AIA estension of client certificate

Local Target Message Format: <timestamp> <seq_num> 12991 INFO EAP: No more OCSP servers in AIA estension of client certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12991 INFO EAP: No more OCSP servers in AIA estension of client certificate, <log details>

- **Message Code:** 12992

  Severity: INFO

  Message Text: No AIA extension in client certificate

  Message Description: No AIA extension in client certificate

  Local Target Message Format: <timestamp> <seq_num> 12992 INFO EAP: No AIA extension in client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12992 INFO EAP: No AIA extension in client certificate, <log details>

- **Message Code:** 12993

  Severity: WARN

  Message Text: User Auth failed because OCSP is unreachable

  Message Description: User Auth failed because OCSP is unreachable

  Local Target Message Format: <timestamp> <seq_num> 12993 WARN EAP: User Auth failed because OCSP is unreachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12993 WARN EAP: User Auth failed because OCSP is unreachable, <log details>

- **Message Code:** 12994

  Severity: WARN

  Message Text: EAP-TTLS inner method CHAP is not allowed in Allowed Protocols

  Message Description: EAP-TTLS inner method CHAP is not allowed in Allowed Protocols

  Local Target Message Format: <timestamp> <seq_num> 12994 WARN EAP: EAP-TTLS inner method CHAP is not allowed in Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12994 WARN EAP: EAP-TTLS inner method CHAP is not allowed in Allowed Protocols, <log details>

- **Message Code:** 12995

  Severity: WARN

  Message Text: EAP-TTLS inner method MSCHAPv1 is not allowed in Allowed Protocols

  Message Description: EAP-TTLS inner method MSCHAPv1 is not allowed in Allowed Protocols

Local Target Message Format: <timestamp> <seq_num> 12995 WARN EAP: EAP-TTLS inner method MSCHAPv1 is not allowed in Allowed Protocols, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12995 WARN EAP: EAP-TTLS inner method MSCHAPv1 is not allowed in Allowed Protocols, <log details>

- **Message Code:** 12996

  Severity: WARN

  Message Text: EAP-TTLS inner method MSCHAPv2 is not allowed in Allowed Protocols

  Message Description: EAP-TTLS inner method MSCHAPv2 is not allowed in Allowed Protocols

  Local Target Message Format: <timestamp> <seq_num> 12996 WARN EAP: EAP-TTLS inner method MSCHAPv2 is not allowed in Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12996 WARN EAP: EAP-TTLS inner method MSCHAPv2 is not allowed in Allowed Protocols, <log details>

- **Message Code:** 12997

  Severity: WARN

  Message Text: EAP-TTLS inner method PAP is not allowed in Allowed Protocols

  Message Description: EAP-TTLS inner method PAP is not allowed in Allowed Protocols

  Local Target Message Format: <timestamp> <seq_num> 12997 WARN EAP: EAP-TTLS inner method PAP is not allowed in Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12997 WARN EAP: EAP-TTLS inner method PAP is not allowed in Allowed Protocols, <log details>

- **Message Code:** 12998

  Severity: WARN

  Message Text: Failed to negotiate EAP for inner method because EAP-MD5 not allowed under EAP-TTLS configuration in the Allowed Protocols

  Message Description: The client's supplicant sent an EAP-Response/NAK packet rejecting the EAP-based protocol that was previously proposed for the inner method, and requested to use EAP-MD5 instead. However, ISE does not allow EAP-MD5 under EAP-TTLS configuration in Allowed Protocols.

  Local Target Message Format: <timestamp> <seq_num> 12998 WARN EAP: Failed to negotiate EAP for inner method because EAP-MD5 not allowed under EAP-TTLS configuration in the Allowed Protocols, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12998 WARN EAP: Failed to negotiate EAP for inner method because EAP-MD5 not allowed under EAP-TTLS configuration in the Allowed Protocols, <log details>

- **Message Code:** 12999

  Severity: INFO

Message Text: Extracted EAP-Response/NAK for inner method requesting to use EAP-MD5 instead

Message Description: From the EAP-Response packet encountered in the outer EAP method, extracted an EAP-Response/NAK packet, rejecting the EAP-based protocol previously proposed for the inner method, and requesting to use EAP-MD5 instead, per the configuration of the client's supplicant.

Local Target Message Format: <timestamp> <seq_num> 12999 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-MD5 instead, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 12999 INFO EAP: Extracted EAP-Response/NAK for inner method requesting to use EAP-MD5 instead, <log details>

- **Message Code:** 13079

  Severity: WARN

  Message Text: TLS handshake failed because of an unknown CA in the certificates chain

  Message Description: TLS handshake failed because of an unknown CA in the certificates chain

  Local Target Message Format: <timestamp> <seq_num>13079 WARN TACACS TLS handshake failed because of an unknown CA in the certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13079 WARN TACACS TLS handshake failed because of an unknown CA in the certificates chain, <log details>

- **Message Code:** 13080

  Severity: WARN

  Message Text: TLS handshake failed because of a bad certificate in the certificate chain

  Message Description: TLS handshake failed because of a bad certificate in the certificate chain

  Local Target Message Format: <timestamp> <seq_num>13080 WARN TACACS TLS handshake failed because of a bad certificate in the certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13080 WARN TACACS TLS handshake failed because of a bad certificate in the certificate chain, <log details>

- **Message Code:** 13081

  Severity: WARN

  Message Text: TLS handshake failed because decryption error

  Message Description: TLS handshake failed because decryption error

  Local Target Message Format: <timestamp> <seq_num>13081 WARN TACACS TLS handshake failed because decryption error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13081 WARN TACACS TLS handshake failed because decryption error, <log details>

- **Message Code:** 13082

  Severity: WARN

Message Text: TLS handshake failed because certificate has expired

Message Description: TLS handshake failed because certificate has expired

Local Target Message Format: <timestamp> <seq_num>13082 WARN TACACS TLS handshake failed because certificate has expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13082 WARN TACACS TLS handshake failed because certificate has expired, <log details>

- **Message Code:** 13083

  Severity: WARN

  Message Text: TLS handshake failed because unknown certificate

  Message Description: TLS handshake failed because unknown certificate

  Local Target Message Format: <timestamp> <seq_num>13083 WARN TACACS TLS handshake failed because unknown certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13083 WARN TACACS TLS handshake failed because unknown certificate, <log details>

- **Message Code:** 13084

  Severity: WARN

  Message Text: TLS handshake failed because of unsupported protocol version

  Message Description: TLS handshake failed because of unsupported protocol version

  Local Target Message Format: <timestamp> <seq_num>13084 WARN TACACS TLS handshake failed because of unsupported protocol version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13084 WARN TACACS TLS handshake failed because of unsupported protocol version, <log details>

- **Message Code:** 13085

  Severity: WARN

  Message Text: received client hello message

  Message Description: received client hello message

  Local Target Message Format: <timestamp> <seq_num>13085 WARN TACACS received client hello message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13085 WARN TACACS received client hello message, <log details>

- **Message Code:** 13086

  Severity: WARN

  Message Text: TLS handshake failed because of client hello verification failed

Message Description: TLS handshake failed because of client hello verification failed

Local Target Message Format: <timestamp> <seq_num>13086 WARN TACACS TLS handshake failed because of client hello verification failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13086 WARN TACACS TLS handshake failed because of client hello verification failed, <log details>

- **Message Code:** 13087

  Severity: INFO

  Message Text: sent client hello verify request

  Message Description: sent client hello verify request

  Local Target Message Format: <timestamp> <seq_num>13087 INFO TACACS sent client hello verify request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13087 INFO TACACS sent client hello verify request, <log details>

- **Message Code:** 13088

  Severity: WARN

  Message Text: client Identity check failed

  Message Description: client Identity check failed

  Local Target Message Format: <timestamp> <seq_num>13088 WARN TACACS client Identity check failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13088 WARN TACACS client Identity check failed, <log details>

- **Message Code:** 13089

  Severity: WARN

  Message Text: Unencrypted flag in the TACACS header is set to FALSE

  Message Description: Unencrypted flag in the TACACS header is set to FALSE

  Local Target Message Format: <timestamp> <seq_num>13089 WARN TACACS Unencrypted flag in the TACACS header is set to FALSE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13089 WARN TACACS Unencrypted flag in the TACACS header is set to FALSE, <log details>

- **Message Code:** 13090

  Severity: INFO

  Message Text: TCP connection was established successfully

  Message Description: TCP connection was established successfully

Local Target Message Format: <timestamp> <seq_num>13090 INFO TACACS TCP connection was established successfully, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13090 INFO TACACS TCP connection was established successfully, <log details>

- **Message Code:** 13091

  Severity: INFO

  Message Text: TLS encrypted packet was received

  Message Description: TLS encrypted packet was received

  Local Target Message Format: <timestamp> <seq_num>13091 INFO TACACS TLS encrypted packet was received, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13091 INFO TACACS TLS encrypted packet was received, <log details>

- **Message Code:** 13092

  Severity: INFO

  Message Text: TLS encrypted packet was sent

  Message Description: TLS encrypted packet was sent

  Local Target Message Format: <timestamp> <seq_num>13092 INFO TACACS TLS encrypted packet was sent, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13092 INFO TACACS TLS encrypted packet was sent, <log details>

- **Message Code:** 13093

  Severity: WARN

  Message Text: Failed to send the TACACS+ encrypted packet

  Message Description: Failed to send the TACACS+ encrypted packet

  Local Target Message Format: <timestamp> <seq_num>13093 WARN TACACS Failed to send the TACACS+ encrypted packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13093 WARN TACACS Failed to send the TACACS+ encrypted packet, <log details>

- **Message Code:** 13094

  Severity: INFO

  Message Text: Identity Check SAN is not configured

  Message Description: Identity Check SAN is not configured

Local Target Message Format: <timestamp> <seq_num>13094 INFO TACACS Identity Check SAN is not configured, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13094 INFO TACACS Identity Check SAN is not configured, <log details>

- **Message Code:** 13095

  Severity: INFO

  Message Text: Identity Check: SAN IP validation

  Message Description: Identity Check: SAN IP validation

  Local Target Message Format: <timestamp> <seq_num>13095 INFO TACACS Identity Check: SAN IP validation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13095 INFO TACACS Identity Check: SAN IP validation, <log details>

- **Message Code:** 13096

  Severity: INFO

  Message Text: Identity Check: SAN IP matched

  Message Description: Identity Check: SAN IP matched

  Local Target Message Format: <timestamp> <seq_num>13096 INFO TACACS Identity Check: SAN IP matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13096 INFO TACACS Identity Check: SAN IP matched, <log details>

- **Message Code:** 13097

  Severity: INFO

  Message Text: Identity Check: SAN IP did not match

  Message Description: Identity Check: SAN IP did not match

  Local Target Message Format: <timestamp> <seq_num>13097 INFO TACACS Identity Check: SAN IP did not match, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13097 INFO TACACS Identity Check: SAN IP did not match, <log details>

- **Message Code:** 13098

  Severity: INFO

  Message Text: Identity Check: SAN DNS hostname validation

  Message Description: Identity Check: SAN DNS hostname validation

Local Target Message Format: <timestamp> <seq_num>13098 INFO TACACS Identity Check: SAN DNS hostname validation, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13098 INFO TACACS Identity Check: SAN DNS hostname validation, <log details>

- **Message Code:** 13099

  Severity: INFO

  Message Text: Identity Check: SAN DNS hostname matched

  Message Description: Identity Check: SAN DNS hostname matched

  Local Target Message Format: <timestamp> <seq_num>13099 INFO TACACS Identity Check: SAN DNS hostname matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13099 INFO TACACS Identity Check: SAN DNS hostname matched, <log details>

- **Message Code:** 13100

  Severity: INFO

  Message Text: Identity Check: SAN DNS hostname did not match

  Message Description: Identity Check: SAN DNS hostname did not match

  Local Target Message Format: <timestamp> <seq_num>13100 INFO TACACS Identity Check: SAN DNS hostname did not match, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13100 INFO TACACS Identity Check: SAN DNS hostname did not match, <log details>

- **Message Code:** 13101

  Severity: INFO

  Message Text: Identity Check: SAN DirName validation

  Message Description: Identity Check: SAN DirName validation

  Local Target Message Format: <timestamp> <seq_num>13101 INFO TACACS Identity Check: SAN DirName validation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13101 INFO TACACS Identity Check: SAN DirName validation, <log details>

- **Message Code:** 13102

  Severity: INFO

  Message Text: Identity Check: SAN DirName matched

  Message Description: Identity Check: SAN DirName matched

Local Target Message Format: <timestamp> <seq_num>13102 INFO TACACS Identity Check: SAN DirName matched, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13102 INFO TACACS Identity Check: SAN DirName matched, <log details>

- **Message Code:** 13103

  Severity: INFO

  Message Text: Identity Check: SAN DirName did not match

  Message Description: Identity Check: SAN DirName did not match

  Local Target Message Format: <timestamp> <seq_num>13103 INFO TACACS Identity Check: SAN DirName did not match, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13103 INFO TACACS Identity Check: SAN DirName did not match, <log details>

- **Message Code:** 13104

  Severity: WARN

  Message Text: NAD requested TLS version less then TLSv1.3

  Message Description: NAD requested TLS version less then TLSv1.3

  Local Target Message Format: <timestamp> <seq_num>13104 WARN TACACS NAD requested TLS version less then TLSv1.3, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13104 WARN TACACS NAD requested TLS version less then TLSv1.3, <log details>

System Statistics

- **Message Code:** 70000

  Severity: NOTICE

  Message Text: ISE Utilization

  Message Description: ISE Utilization

  Local Target Message Format: <timestamp> <seq_num> 70000 NOTICE System-Stats: ISE Utilization, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 70000 NOTICE System-Stats: ISE Utilization, <log details>

- **Message Code:** 70001

  Severity: NOTICE

Message Text: ISE Process Health

Message Description: ISE Process Health

Local Target Message Format: <timestamp> <seq_num> 70001 NOTICE System-Stats: ISE Process Health, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 70001 NOTICE System-Stats: ISE Process Health, <log details>

- **Message Code:** 70002

  Severity: NOTICE

  Message Text: ISE Process Health Unavailable

  Message Description: ISE Process Health Unavailable

  Local Target Message Format: <timestamp> <seq_num> 70002 NOTICE System-Stats: ISE Process Health Unavailable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 70002 NOTICE System-Stats: ISE Process Health Unavailable, <log details>

- **Message Code:** 70010

  Severity: INFO

  Message Text: OCSP Statistics

  Message Description: OCSP Statistics

  Local Target Message Format: <timestamp> <seq_num> 70010 INFO System-Stats: OCSP Statistics, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 70010 INFO System-Stats: OCSP Statistics, <log details>

- **Message Code:** 70011

  Severity: INFO

  Message Text: ISE Counters

  Message Description: ISE Counters

  Local Target Message Format: <timestamp> <seq_num> 70011 INFO System-Stats: ISE Counters, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 70011 INFO System-Stats: ISE Counters, <log details>

TACACS Accounting

- **Message Code:** 3300

  Severity: NOTICE

  Message Text: TACACS+ Accounting with Command

  Message Description: Received a TACACS+ Accounting request containing a command

  Local Target Message Format: <timestamp> <seq_num> 3300 NOTICE Tacacs-Accounting: TACACS+ Accounting with Command, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3300 NOTICE Tacacs-Accounting: TACACS+ Accounting with Command, <log details>

- **Message Code:** 3301

  Severity: NOTICE

  Message Text: TACACS+ Accounting START

  Message Description: Received a TACACS+ Accounting START request

  Local Target Message Format: <timestamp> <seq_num> 3301 NOTICE Tacacs-Accounting: TACACS+ Accounting START, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3301 NOTICE Tacacs-Accounting: TACACS+ Accounting START, <log details>

- **Message Code:** 3302

  Severity: NOTICE

  Message Text: TACACS+ Accounting STOP

  Message Description: Received a TACACS+ Accounting STOP request

  Local Target Message Format: <timestamp> <seq_num> 3302 NOTICE Tacacs-Accounting: TACACS+ Accounting STOP, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3302 NOTICE Tacacs-Accounting: TACACS+ Accounting STOP, <log details>

- **Message Code:** 3303

  Severity: NOTICE

  Message Text: TACACS+ Accounting WATCHDOG

  Message Description: Received a TACACS+ Accounting WATCHDOG request

  Local Target Message Format: <timestamp> <seq_num> 3303 NOTICE Tacacs-Accounting: TACACS+ Accounting WATCHDOG, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3303 NOTICE Tacacs-Accounting: TACACS+ Accounting WATCHDOG, <log details>

- **Message Code:** 3304

  Severity: NOTICE

  Message Text: TACACS+ Accounting request rejected

  Message Description: Received a TACACS+ Accounting request but it has been rejected. See FailureReason for more information

  Local Target Message Format: <timestamp> <seq_num> 3304 NOTICE Tacacs-Accounting: TACACS+ Accounting request rejected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 3304 NOTICE Tacacs-Accounting: TACACS+ Accounting request rejected, <log details>

TACACS Diagnostics

- **Message Code:** 13000

  Severity: WARN

  Message Text: Invalid TACACS+ authorization request

  Message Description: The TACACS+ authorization request was not one that ISE supports

  Local Target Message Format: <timestamp> <seq_num> 13000 WARN TACACS: Invalid TACACS+ authorization request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13000 WARN TACACS: Invalid TACACS+ authorization request, <log details>

- **Message Code:** 13001

  Severity: WARN

  Message Text: Invalid TACACS+ accounting request

  Message Description: The TACACS+ accounting request was not one that ISE supports

  Local Target Message Format: <timestamp> <seq_num> 13001 WARN TACACS: Invalid TACACS+ accounting request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13001 WARN TACACS: Invalid TACACS+ accounting request, <log details>

- **Message Code:** 13002

  Severity: INFO

  Message Text: Started TACACS+ listener

Message Description: Started TACACS+ listener

Local Target Message Format: <timestamp> <seq_num> 13002 INFO TACACS: Started TACACS+ listener, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13002 INFO TACACS: Started TACACS+ listener, <log details>

- **Message Code:** 13003

  Severity: INFO

  Message Text: Stopped TACACS+ listener

  Message Description: Stopped TACACS+ listener

  Local Target Message Format: <timestamp> <seq_num> 13003 INFO TACACS: Stopped TACACS+ listener, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13003 INFO TACACS: Stopped TACACS+ listener, <log details>

- **Message Code:** 13004

  Severity: ERROR

  Message Text: TACACS+ listener failed

  Message Description: TACACS+ listener failed

  Local Target Message Format: <timestamp> <seq_num> 13004 ERROR TACACS: TACACS+ listener failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13004 ERROR TACACS: TACACS+ listener failed, <log details>

- **Message Code:** 13005

  Severity: DEBUG

  Message Text: Received TACACS+ Authorization Request

  Message Description: Received TACACS+ Authorization Request

  Local Target Message Format: <timestamp> <seq_num> 13005 DEBUG TACACS: Received TACACS+ Authorization Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13005 DEBUG TACACS: Received TACACS+ Authorization Request, <log details>

- **Message Code:** 13006

  Severity: DEBUG

  Message Text: Received TACACS+ Accounting Request

  Message Description: Received TACACS+ Accounting Request

Local Target Message Format: <timestamp> <seq_num> 13006 DEBUG TACACS: Received TACACS+ Accounting Request, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13006 DEBUG TACACS: Received TACACS+ Accounting Request, <log details>

- **Message Code:** 13007

  Severity: WARN

  Message Text: Invalid TACACS+ packet header

  Message Description: The header of the TACACS+ packet failed to parse correctly

  Local Target Message Format: <timestamp> <seq_num> 13007 WARN TACACS: Invalid TACACS+ packet header, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13007 WARN TACACS: Invalid TACACS+ packet header, <log details>

- **Message Code:** 13008

  Severity: WARN

  Message Text: Reached TACACS+ maximum client limit

  Message Description: Check the Network Device or AAA Client and/or the network in between that device and ISE for hardware problems

  Local Target Message Format: <timestamp> <seq_num> 13008 WARN TACACS: Reached TACACS+ maximum client limit, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13008 WARN TACACS: Reached TACACS+ maximum client limit, <log details>

- **Message Code:** 13009

  Severity: WARN

  Message Text: Failed to accept TACACS+ client connection

  Message Description: The attempt to accept a connection request from a TACACS+ client failed. This could occur if the client, after initiating the request 'hangs up' before ISE is able to accept the connection. If this happens frequently it could indicate a faulty device or a potential DOS attack

  Local Target Message Format: <timestamp> <seq_num> 13009 WARN TACACS: Failed to accept TACACS+ client connection, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13009 WARN TACACS: Failed to accept TACACS+ client connection, <log details>

- **Message Code:** 13010

  Severity: WARN

  Message Text: Received TACACS+ packet with invalid length

Message Description: Received TACACS+ packet with less then 12 bytes or more than the defined maximum length

Local Target Message Format: <timestamp> <seq_num> 13010 WARN TACACS: Received TACACS+ packet with invalid length, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13010 WARN TACACS: Received TACACS+ packet with invalid length, <log details>

- **Message Code:** 13011

  Severity: WARN

  Message Text: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

  Message Description: The TACACS+ request packet was invalid. A likely reason is that the Shared Secret configured in the device and the Shared Secret configured for the Network Device or AAA Client in ISE do not match

  Local Target Message Format: <timestamp> <seq_num> 13011 WARN TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13011 WARN TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets, <log details>

- **Message Code:** 13013

  Severity: DEBUG

  Message Text: Received TACACS+ Authentication START Request

  Message Description: Received TACACS+ Authentication START Request

  Local Target Message Format: <timestamp> <seq_num> 13013 DEBUG TACACS: Received TACACS+ Authentication START Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13013 DEBUG TACACS: Received TACACS+ Authentication START Request, <log details>

- **Message Code:** 13014

  Severity: DEBUG

  Message Text: Received TACACS+ Authentication CONTINUE Request

  Message Description: Received TACACS+ Authentication CONTINUE Request

  Local Target Message Format: <timestamp> <seq_num> 13014 DEBUG TACACS: Received TACACS+ Authentication CONTINUE Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13014 DEBUG TACACS: Received TACACS+ Authentication CONTINUE Request, <log details>

- **Message Code:** 13015

  Severity: DEBUG

Message Text: Returned TACACS+ Authentication Reply

Message Description: Returned TACACS+ Authentication Reply

Local Target Message Format: <timestamp> <seq_num> 13015 DEBUG TACACS: Returned TACACS+ Authentication Reply, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13015 DEBUG TACACS: Returned TACACS+ Authentication Reply, <log details>

- **Message Code:** 13017

  Severity: DEBUG

  Message Text: Received TACACS+ packet from unknown Network Device or AAA Client

  Message Description: A TACACS+ packet was received with a source IP Address that did not match any configured Network Device or AAA Client

  Local Target Message Format: <timestamp> <seq_num> 13017 DEBUG TACACS: Received TACACS+ packet from unknown Network Device or AAA Client, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13017 DEBUG TACACS: Received TACACS+ packet from unknown Network Device or AAA Client, <log details>

- **Message Code:** 13019

  Severity: ERROR

  Message Text: Failed to obtain TACACS+ Settings

  Message Description: Internal Error: Failed to obtain TACACS+ settings from the configuration database

  Local Target Message Format: <timestamp> <seq_num> 13019 ERROR TACACS: Failed to obtain TACACS+ Settings, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13019 ERROR TACACS: Failed to obtain TACACS+ Settings, <log details>

- **Message Code:** 13020

  Severity: INFO

  Message Text: Get TACACS+ default network device setting

  Message Description: Obtain TACACS+ default network device setting.

  Local Target Message Format: <timestamp> <seq_num> 13020 INFO TACACS: Get TACACS+ default network device setting, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13020 INFO TACACS: Get TACACS+ default network device setting, <log details>

- **Message Code:** 13021

  Severity: WARN

Message Text: TACACS+ request was dropped because of system overload

Message Description: TACACS+ request was dropped because of system overload.

Local Target Message Format: <timestamp> <seq_num> 13021 WARN TACACS: TACACS+ request was dropped because of system overload, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13021 WARN TACACS: TACACS+ request was dropped because of system overload, <log details>

- **Message Code:** 13023

  Severity: DEBUG

  Message Text: Command matched a Deny-Always rule

  Message Description: The requested Command matched a Deny-Always rule in one of the Command Sets

  Local Target Message Format: <timestamp> <seq_num> 13023 DEBUG Device-administration: Command matched a Deny-Always rule, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13023 DEBUG Device-administration: Command matched a Deny-Always rule, <log details>

- **Message Code:** 13024

  Severity: DEBUG

  Message Text: Command matched a Permit rule

  Message Description: Command matched a Permit rule

  Local Target Message Format: <timestamp> <seq_num> 13024 DEBUG Device-administration: Command matched a Permit rule, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13024 DEBUG Device-administration: Command matched a Permit rule, <log details>

- **Message Code:** 13025

  Severity: DEBUG

  Message Text: Command failed to match a Permit rule

  Message Description: The requested command failed to match a Permit rule in any of the Command Sets

  Local Target Message Format: <timestamp> <seq_num> 13025 DEBUG Device-administration: Command failed to match a Permit rule, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13025 DEBUG Device-administration: Command failed to match a Permit rule, <log details>

- **Message Code:** 13027

  Severity: WARN

Message Text: TACACS+ authorization request missing both User and Remote-Address attributes

Message Description: The TACACS+ authorization request is missing both the User and Remote-Address attributes

Local Target Message Format: <timestamp> <seq_num> 13027 WARN TACACS: TACACS+ authorization request missing both User and Remote-Address attributes, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13027 WARN TACACS: TACACS+ authorization request missing both User and Remote-Address attributes, <log details>

- **Message Code:** 13029

  Severity: ERROR

  Message Text: Requested privilege level too high

  Message Description: The TACACS+ user requested a higher privilege level than the Maximum Privilege Level configured in the Shell Profile

  Local Target Message Format: <timestamp> <seq_num> 13029 ERROR TACACS: Requested privilege level too high, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13029 ERROR TACACS: Requested privilege level too high, <log details>

- **Message Code:** 13030

  Severity: WARN

  Message Text: TACACS+ authentication request missing a User name

  Message Description: The TACACS+ authentication request did not provide a User name

  Local Target Message Format: <timestamp> <seq_num> 13030 WARN TACACS: TACACS+ authentication request missing a User name, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13030 WARN TACACS: TACACS+ authentication request missing a User name, <log details>

- **Message Code:** 13031

  Severity: WARN

  Message Text: TACACS+ authentication request missing user Password

  Message Description: The TACACS+ authentication request did not provide a user Password

  Local Target Message Format: <timestamp> <seq_num> 13031 WARN TACACS: TACACS+ authentication request missing user Password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13031 WARN TACACS: TACACS+ authentication request missing user Password, <log details>

- **Message Code:** 13032

  Severity: ERROR

Message Text: Fatal error accessing TACACS+ configuration

Message Description: Internal Error: Unable to access Access Service configuration in the database

Local Target Message Format: <timestamp> <seq_num> 13032 ERROR TACACS: Fatal error accessing TACACS+ configuration, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13032 ERROR TACACS: Fatal error accessing TACACS+ configuration, <log details>

- **Message Code:** 13034

  Severity: DEBUG

  Message Text: Returned TACACS+ Authorization Reply

  Message Description: Returned TACACS+ Authorization Reply

  Local Target Message Format: <timestamp> <seq_num> 13034 DEBUG TACACS: Returned TACACS+ Authorization Reply, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13034 DEBUG TACACS: Returned TACACS+ Authorization Reply, <log details>

- **Message Code:** 13035

  Severity: DEBUG

  Message Text: Returned TACACS+ Accounting Reply

  Message Description: Returned TACACS+ Accounting Reply

  Local Target Message Format: <timestamp> <seq_num> 13035 DEBUG TACACS: Returned TACACS+ Accounting Reply, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13035 DEBUG TACACS: Returned TACACS+ Accounting Reply, <log details>

- **Message Code:** 13036

  Severity: INFO

  Message Text: Selected Shell Profile is DenyAccess

  Message Description: Selected Shell Profile fails for thsi request

  Local Target Message Format: <timestamp> <seq_num> 13036 INFO TACACS: Selected Shell Profile is DenyAccess, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13036 INFO TACACS: Selected Shell Profile is DenyAccess, <log details>

- **Message Code:** 13037

  Severity: INFO

  Message Text: Shell Profile Privilege Level not configured correctly

Message Description: Shell Profile Privilege Level not configured correctly

Local Target Message Format: <timestamp> <seq_num> 13037 INFO TACACS: Shell Profile Privilege Level not configured correctly, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13037 INFO TACACS: Shell Profile Privilege Level not configured correctly, <log details>

- **Message Code:** 13038

  Severity: INFO

  Message Text: TACACS+ request failed because of a critical logging error

  Message Description: The TACACS+ request failed because of a critical logging error.

  Local Target Message Format: <timestamp> <seq_num> 13038 INFO TACACS: TACACS+ request failed because of a critical logging error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13038 INFO TACACS: TACACS+ request failed because of a critical logging error, <log details>

- **Message Code:** 13039

  Severity: WARN

  Message Text: TACACS+ authentication request does not contain the user's new password

  Message Description: The TACACS+ authentication request does not contain the user's new password.

  Local Target Message Format: <timestamp> <seq_num> 13039 WARN TACACS: TACACS+ authentication request does not contain the user's new password, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13039 WARN TACACS: TACACS+ authentication request does not contain the user's new password, <log details>

- **Message Code:** 13040

  Severity: WARN

  Message Text: TACACS+ authentication request contains an empty string in the Confirm New User Password field

  Message Description: The TACACS+ authentication request does not contain the user's new password to confirm the change password request.

  Local Target Message Format: <timestamp> <seq_num> 13040 WARN TACACS: TACACS+ authentication request contains an empty string in the Confirm New User Password field, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13040 WARN TACACS: TACACS+ authentication request contains an empty string in the Confirm New User Password field, <log details>

- **Message Code:** 13041

  Severity: WARN

Message Text: TACACS+ authentication request switches from Login to Change Password functionality

Message Description: The TACACS+ authentication request switches from Login to Change Password functionality.

Local Target Message Format: <timestamp> <seq_num> 13041 WARN TACACS: TACACS+ authentication request switches from Login to Change Password functionality, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13041 WARN TACACS: TACACS+ authentication request switches from Login to Change Password functionality, <log details>

- **Message Code:** 13042

  Severity: WARN

  Message Text: TACACS+ authentication request to confirm a user's new password has failed

  Message Description: The TACACS+ authentication request to change a user's password does not contain a confirmation password.

  Local Target Message Format: <timestamp> <seq_num> 13042 WARN TACACS: TACACS+ authentication request to confirm a user's new password has failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13042 WARN TACACS: TACACS+ authentication request to confirm a user's new password has failed, <log details>

- **Message Code:** 13043

  Severity: WARN

  Message Text: Challenge-response mechanism is not supported by the selected TACACS+ authentication type

  Message Description: Challenge-response mechanism is not supported by the selected TACACS+ authentication type.

  Local Target Message Format: <timestamp> <seq_num> 13043 WARN TACACS: Challenge-response mechanism is not supported by the selected TACACS+ authentication type, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13043 WARN TACACS: Challenge-response mechanism is not supported by the selected TACACS+ authentication type, <log details>

- **Message Code:** 13044

  Severity: INFO

  Message Text: TACACS+ will use the password prompt returned by the identity store

  Message Description: TACACS+ will use the password prompt returned by the identity store.

  Local Target Message Format: <timestamp> <seq_num> 13044 INFO TACACS: TACACS+ will use the password prompt returned by the identity store, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13044 INFO TACACS: TACACS+ will use the password prompt returned by the identity store, <log details>

- **Message Code:** 13045

  Severity: INFO

  Message Text: TACACS+ will use the password prompt from global TACACS+ configuration

  Message Description: TACACS+ will use the password prompt from global TACACS+ configuration.

  Local Target Message Format: <timestamp> <seq_num> 13045 INFO TACACS: TACACS+ will use the password prompt from global TACACS+ configuration, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13045 INFO TACACS: TACACS+ will use the password prompt from global TACACS+ configuration, <log details>

- **Message Code:** 13046

  Severity: INFO

  Message Text: TACACS+ ASCII change password request

  Message Description: TACACS+ ASCII change password request.

  Local Target Message Format: <timestamp> <seq_num> 13046 INFO TACACS: TACACS+ ASCII change password request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13046 INFO TACACS: TACACS+ ASCII change password request, <log details>

- **Message Code:** 13050

  Severity: ERROR

  Message Text: Invalid TACACS+ MSCHAP flag value.

  Message Description: Invalid TACACS+ MSCHAP flag value.

  Local Target Message Format: <timestamp> <seq_num> 13050 ERROR TACACS : Invalid TACACS+ MSCHAP flag value. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13050 ERROR TACACS : Invalid TACACS+ MSCHAP flag value. , <log details>

- **Message Code:** 13051

  Severity: ERROR

  Message Text: Size of data fieid is small.

  Message Description: Size of data fieid is small.

  Local Target Message Format: <timestamp> <seq_num> 13051 ERROR TACACS : Size of data fieid is small. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13051 ERROR TACACS : Size of data fieid is small. , <log details>

- **Message Code:** 13052

Severity: ERROR

Message Text: Size of data fieid is small.

Message Description: Size of data fieid is small.

Local Target Message Format: <timestamp> <seq_num> 13052 ERROR TACACS : Size of data fieid is small. , <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13052 ERROR TACACS : Size of data fieid is small. , <log details>

- **Message Code:** 13060

  Severity: WARN

  Message Text: Failed to read TACACS proxy configuration.

  Message Description: ACS detected an error when trying to read the TACACS proxy configuration.

  Local Target Message Format: <timestamp> <seq_num> 13060 WARN TACACS-Proxy : Failed to read TACACS proxy configuration. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13060 WARN TACACS-Proxy : Failed to read TACACS proxy configuration. , <log details>

- **Message Code:** 13061

  Severity: WARN

  Message Text: Accounting request received but neither local nor remote accounting is configured.

  Message Description: An accounting request was received; however, neither local nor remote accounting is configured.

  Local Target Message Format: <timestamp> <seq_num> 13061 WARN TACACS-Proxy : Accounting request received but neither local nor remote accounting is configured. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13061 WARN TACACS-Proxy : Accounting request received but neither local nor remote accounting is configured. , <log details>

- **Message Code:** 13062

  Severity: WARN

  Message Text: No more external TACACS servers; canot perform failover.

  Message Description: Failover is not possible because no more external TACACS servers are configured.

  Local Target Message Format: <timestamp> <seq_num> 13062 WARN TACACS-Proxy : No more external TACACS servers; canot perform failover. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13062 WARN TACACS-Proxy : No more external TACACS servers; canot perform failover. , <log details>

- **Message Code:** 13063

Severity: INFO

Message Text: Start forwarding request to remote TACACS server.

Message Description: The request is being forwarded to the next remote TACACS server from the list configured for the selected ACS proxy service.

Local Target Message Format: <timestamp> <seq_num> 13063 INFO TACACS-Proxy : Start forwarding request to remote TACACS server. , <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13063 INFO TACACS-Proxy : Start forwarding request to remote TACACS server. , <log details>

- **Message Code:** 13064

  Severity: INFO

  Message Text: TACACS proxy received incoming request for forwarding.

  Message Description: The TACACS proxy has received an incoming request. Validating the request and preparing to forward it to a configured remote TACACS server.

  Local Target Message Format: <timestamp> <seq_num> 13064 INFO TACACS-Proxy : TACACS proxy received incoming request for forwarding. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13064 INFO TACACS-Proxy : TACACS proxy received incoming request for forwarding. , <log details>

- **Message Code:** 13065

  Severity: INFO

  Message Text: TACACS proxy received valid incoming authentication request.

  Message Description: The TACACS proxy has received a valid incoming authentication request.

  Local Target Message Format: <timestamp> <seq_num> 13065 INFO TACACS-Proxy : TACACS proxy received valid incoming authentication request. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13065 INFO TACACS-Proxy : TACACS proxy received valid incoming authentication request. , <log details>

- **Message Code:** 13066

  Severity: INFO

  Message Text: TACACS proxy received valid incoming authorization request.

  Message Description: The TACACS proxy has received a valid incoming authorization request.

  Local Target Message Format: <timestamp> <seq_num> 13066 INFO TACACS-Proxy : TACACS proxy received valid incoming authorization request. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13066 INFO TACACS-Proxy : TACACS proxy received valid incoming authorization request. , <log details>

- **Message Code:** 13067

Severity: INFO

Message Text: TACACS proxy received valid incoming accounting request.

Message Description: The TACACS proxy has received a valid incoming accounting request.

Local Target Message Format: <timestamp> <seq_num> 13067 INFO TACACS-Proxy : TACACS proxy received valid incoming accounting request. , <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13067 INFO TACACS-Proxy : TACACS proxy received valid incoming accounting request. , <log details>

- **Message Code:** 13068

  Severity: INFO

  Message Text: TACACS proxy performing local accounting.

  Message Description: The TACACS proxy is performing a local accounting based on the incoming accounting request received.

  Local Target Message Format: <timestamp> <seq_num> 13068 INFO TACACS-Proxy : TACACS proxy performing local accounting. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13068 INFO TACACS-Proxy : TACACS proxy performing local accounting. , <log details>

- **Message Code:** 13069

  Severity: INFO

  Message Text: TACACS proxy performing remote accounting.

  Message Description: The TACACS proxy is performing a remote accounting based on the incoming accounting request received.

  Local Target Message Format: <timestamp> <seq_num> 13069 INFO TACACS-Proxy : TACACS proxy performing remote accounting. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13069 INFO TACACS-Proxy : TACACS proxy performing remote accounting. , <log details>

- **Message Code:** 13070

  Severity: WARN

  Message Text: Failed to forward request to current remote TACACS server.

  Message Description: Current remote TACACS server has failed to process the forwarded request due to any of the following reasons: The remote TACACS server is down ; The remote TACACS server is not configured properly ; The remote TACACS server dropped the request.

  Local Target Message Format: <timestamp> <seq_num> 13070 WARN TACACS-Proxy : Failed to forward request to current remote TACACS server. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13070 WARN TACACS-Proxy : Failed to forward request to current remote TACACS server. , <log details>

- **Message Code:** 13071

  Severity: WARN

  Message Text: Continue flow (seq_no > 1).

  Message Description: Continue previous flow. Request will be send to server, what response to the previous request.

  Local Target Message Format: <timestamp> <seq_num> 13071 WARN TACACS-Proxy : Continue flow (seq_no > 1). , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13071 WARN TACACS-Proxy : Continue flow (seq_no > 1). , <log details>

- **Message Code:** 13072

  Severity: WARN

  Message Text: Failed to forward request to current remote TACACS server.

  Message Description: Failed to forward request to current remote TACACS server. Becouse flow is continue request can not be forward to the next TACACS server.

  Local Target Message Format: <timestamp> <seq_num> 13072 WARN TACACS-Proxy : Failed to forward request to current remote TACACS server. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13072 WARN TACACS-Proxy : Failed to forward request to current remote TACACS server. , <log details>

- **Message Code:** 13073

  Severity: INFO

  Message Text: TACACS+ Proxy request failed because of a critical logging error.

  Message Description: The TACACS+ Proxy request failed because of a critical logging error.

  Local Target Message Format: <timestamp> <seq_num> 13073 INFO TACACS : TACACS+ Proxy request failed because of a critical logging error. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13073 INFO TACACS : TACACS+ Proxy request failed because of a critical logging error. , <log details>

- **Message Code:** 13074

  Severity: INFO

  Message Text: Finished to process TACACS Proxy request.

  Message Description: Finished to process TACACS Proxy request.

  Local Target Message Format: <timestamp> <seq_num> 13074 INFO TACACS-Proxy : Finished to process TACACS Proxy request. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13074 INFO TACACS-Proxy : Finished to process TACACS Proxy request. , <log details>

- **Message Code:** 13075

  Severity: INFO

  Message Text: TACACS+ Proxy request won't continue.

  Message Description: TACACS+ Proxy request won't continue.

  Local Target Message Format: <timestamp> <seq_num> 13075 INFO TACACS-Proxy : TACACS+ Proxy request won't continue. , <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 13075 INFO TACACS-Proxy : TACACS+ Proxy request won't continue. , <log details>

- **Message Code:** 13076

  Severity: DEBUG

  Message Text: No command set for selected rule

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>13076 DEBUG Device-administration No command set for selected rule, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13076 DEBUG Device-administration No command set for selected rule, <log details>

- **Message Code:** 13077

  Severity: WARN

  Message Text: Invalid TACACS+ accouting request packet - possibly malformed packet

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>13077 WARN Tacacs-Accounting Invalid TACACS+ accouting request packet - possibly malformed packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13077 WARN Tacacs-Accounting Invalid TACACS+ accouting request packet - possibly malformed packet, <log details>

- **Message Code:** 13078

  Severity: WARN

  Message Text: Invalid TACACS+ authorization request packet - possibly malformed packet

  Message Description: nan

  Local Target Message Format: <timestamp> <seq_num>13078 WARN Device-administration Invalid TACACS+ authorization request packet - possibly malformed packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13078 WARN Device-administration Invalid TACACS+ authorization request packet - possibly malformed packet, <log details>

- **Message Code:** 13079

Severity: WARN

Message Text: TACACS+ TLS handshake failed due to an unknown Certificate Authority (CA) in the certificate chain.

Message Description: TACACS+ TLS handshake failed due to an unknown Certificate Authority (CA) in the certificate chain.

Local Target Message Format: <timestamp> <seq_num>13079 WARN TACACS TACACS+ TLS handshake failed due to an unknown Certificate Authority (CA) in the certificate chain., <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13079 WARN TACACS TACACS+ TLS handshake failed due to an unknown Certificate Authority (CA) in the certificate chain., <log details>

- **Message Code:** 13080

  Severity: WARN

  Message Text: TACACS+ TLS handshake failed due to a faulty certificate in the NAD certificate chain

  Message Description: TACACS+ TLS handshake failed due to a faulty certificate in the NAD certificate chain

  Local Target Message Format: <timestamp> <seq_num>13080 WARN TACACS TACACS+ TLS handshake failed due to a faulty certificate in the NAD certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13080 WARN TACACS TACACS+ TLS handshake failed due to a faulty certificate in the NAD certificate chain, <log details>

- **Message Code:** 13081

  Severity: WARN

  Message Text: TACACS+ TLS handshake failed due to a decryption error

  Message Description: TACACS+ TLS handshake failed due to a decryption error

  Local Target Message Format: <timestamp> <seq_num>13081 WARN TACACS TACACS+ TLS handshake failed due to a decryption error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13081 WARN TACACS TACACS+ TLS handshake failed due to a decryption error, <log details>

- **Message Code:** 13082

  Severity: WARN

  Message Text: TACACS+ TLS handshake failed because the NAD certificate has expired

  Message Description: TACACS+ TLS handshake failed because the NAD certificate has expired

  Local Target Message Format: <timestamp> <seq_num>13082 WARN TACACS TACACS+ TLS handshake failed because the NAD certificate has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13082 WARN TACACS TACACS+ TLS handshake failed because the NAD certificate has expired, <log details>

- **Message Code:** 13083

  Severity: WARN

  Message Text: TACACS+ TLS handshake failed due to an unknown certificate

  Message Description: TACACS+ TLS handshake failed due to an unknown certificate

  Local Target Message Format: <timestamp> <seq_num>13083 WARN TACACS TACACS+ TLS handshake failed due to an unknown certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13083 WARN TACACS TACACS+ TLS handshake failed due to an unknown certificate, <log details>

- **Message Code:** 13084

  Severity: WARN

  Message Text: TACACS+ TLS handshake failed due to an unsupported protocol version

  Message Description: TACACS+ TLS handshake failed due to an unsupported protocol version

  Local Target Message Format: <timestamp> <seq_num>13084 WARN TACACS TACACS+ TLS handshake failed due to an unsupported protocol version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13084 WARN TACACS TACACS+ TLS handshake failed due to an unsupported protocol version, <log details>

- **Message Code:** 13085

  Severity: INFO

  Message Text: TACACS+ TLS client hello message has been extracted

  Message Description: As part of the ongoing TLS handshake, a TLS record containing a TLS ClientHello message has been extracted from the TACACS+ Response packet

  Local Target Message Format: <timestamp> <seq_num>13085 INFO TACACS TACACS+ TLS client hello message has been extracted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13085 INFO TACACS TACACS+ TLS client hello message has been extracted, <log details>

- **Message Code:** 13086

  Severity: WARN

  Message Text: TACACS TLS: TLS handshake failed because of client hello verification failed

  Message Description: TACACS TLS: TLS handshake failed because of client hello verification failed.

  Local Target Message Format: <timestamp> <seq_num>13086 WARN TACACS TACACS TLS: TLS handshake failed because of client hello verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13086 WARN TACACS TACACS TLS: TLS handshake failed because of client hello verification failed, <log details>

- **Message Code:** 13087

  Severity: INFO

  Message Text: TACACS+ TLS sent a ClientHello Verify Request

  Message Description: TACACS+ TLS sent a ClientHello Verify Request

  Local Target Message Format: <timestamp> <seq_num>13087 INFO TACACS TACACS+ TLS sent a ClientHello Verify Request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13087 INFO TACACS TACACS+ TLS sent a ClientHello Verify Request, <log details>

- **Message Code:** 13088

  Severity: WARN

  Message Text: TACACS+ TLS NAD identity check failed

  Message Description: TACACS+ TLS NAD identity check failed

  Local Target Message Format: <timestamp> <seq_num>13088 WARN TACACS TACACS+ TLS NAD identity check failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13088 WARN TACACS TACACS+ TLS NAD identity check failed, <log details>

- **Message Code:** 13089

  Severity: WARN

  Message Text: TACACS+ TLS Unencrypted flag in the TACACS header is set to FALSE

  Message Description: TACACS+ TLS Unencrypted flag in the TACACS header is set to FALSE

  Local Target Message Format: <timestamp> <seq_num>13089 WARN TACACS TACACS+ TLS Unencrypted flag in the TACACS header is set to FALSE, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13089 WARN TACACS TACACS+ TLS Unencrypted flag in the TACACS header is set to FALSE, <log details>

- **Message Code:** 13090

  Severity: INFO

  Message Text: TACACS+ TLS TCP connection was established successfully

  Message Description: TACACS+ TLS TCP connection was established successfully.

  Local Target Message Format: <timestamp> <seq_num>13090 INFO TACACS TACACS+ TLS TCP connection was established successfully, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13090 INFO TACACS TACACS+ TLS TCP connection was established successfully, <log details>

- **Message Code:** 13091

Severity: INFO

Message Text: TACACS+ TLS encrypted packet was received

Message Description: TACACS+ TLS encrypted packet was received.

Local Target Message Format: <timestamp> <seq_num>13091 INFO TACACS TACACS+ TLS encrypted packet was received, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13091 INFO TACACS TACACS+ TLS encrypted packet was received, <log details>

- **Message Code:** 13092

  Severity: INFO

  Message Text: TACACS+ TLS encrypted packet was sent

  Message Description: TACACS+ TLS encrypted packet was sent.

  Local Target Message Format: <timestamp> <seq_num>13092 INFO TACACS TACACS+ TLS encrypted packet was sent, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13092 INFO TACACS TACACS+ TLS encrypted packet was sent, <log details>

- **Message Code:** 13093

  Severity: WARN

  Message Text: Failed to send the TACACS+ encrypted packet

  Message Description: Failed to send the TACACS+ encrypted packet.

  Local Target Message Format: <timestamp> <seq_num>13093 WARN TACACS Failed to send the TACACS+ encrypted packet, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13093 WARN TACACS Failed to send the TACACS+ encrypted packet, <log details>

- **Message Code:** 13094

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check SAN is not configured

  Message Description: TACACS+ TLS Identity Check SAN is not configured

  Local Target Message Format: <timestamp> <seq_num>13094 INFO TACACS TACACS+ TLS Identity Check SAN is not configured, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13094 INFO TACACS TACACS+ TLS Identity Check SAN is not configured, <log details>

- **Message Code:** 13095

  Severity: INFO

Message Text: TACACS+ TLS Identity Check: SAN IP validation

Message Description: TACACS+ TLS Identity Check: SAN IP validation.

Local Target Message Format: <timestamp> <seq_num>13095 INFO TACACS TACACS+ TLS Identity Check: SAN IP validation, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13095 INFO TACACS TACACS+ TLS Identity Check: SAN IP validation, <log details>

- **Message Code:** 13096

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN IP matched

  Message Description: TACACS+ TLS Identity Check: SAN IP matched.

  Local Target Message Format: <timestamp> <seq_num>13096 INFO TACACS TACACS+ TLS Identity Check: SAN IP matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13096 INFO TACACS TACACS+ TLS Identity Check: SAN IP matched, <log details>

- **Message Code:** 13097

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN IP did not match

  Message Description: TACACS+ TLS Identity Check: SAN IP did not match.

  Local Target Message Format: <timestamp> <seq_num>13097 INFO TACACS TACACS+ TLS Identity Check: SAN IP did not match, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13097 INFO TACACS TACACS+ TLS Identity Check: SAN IP did not match, <log details>

- **Message Code:** 13098

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN DNS hostname validation

  Message Description: TACACS+ TLS Identity Check: SAN DNS hostname validation.

  Local Target Message Format: <timestamp> <seq_num>13098 INFO TACACS TACACS+ TLS Identity Check: SAN DNS hostname validation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13098 INFO TACACS TACACS+ TLS Identity Check: SAN DNS hostname validation, <log details>

- **Message Code:** 13099

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN DNS hostname matched

Message Description: TACACS+ TLS Identity Check: SAN DNS hostname matched.

Local Target Message Format: <timestamp> <seq_num>13099 INFO TACACS TACACS+ TLS Identity Check: SAN DNS hostname matched, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13099 INFO TACACS TACACS+ TLS Identity Check: SAN DNS hostname matched, <log details>

- **Message Code:** 13100

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN DNS hostname did not match

  Message Description: TACACS+ TLS Identity Check: SAN DNS hostname did not match.

  Local Target Message Format: <timestamp> <seq_num>13100 INFO TACACS TACACS+ TLS Identity Check: SAN DNS hostname did not match, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13100 INFO TACACS TACACS+ TLS Identity Check: SAN DNS hostname did not match, <log details>

- **Message Code:** 13101

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN DirName validation

  Message Description: TACACS+ TLS Identity Check: SAN DirName validation.

  Local Target Message Format: <timestamp> <seq_num>13101 INFO TACACS TACACS+ TLS Identity Check: SAN DirName validation, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13101 INFO TACACS TACACS+ TLS Identity Check: SAN DirName validation, <log details>

- **Message Code:** 13102

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN DirName matched

  Message Description: TACACS+ TLS Identity Check: SAN DirName matched.

  Local Target Message Format: <timestamp> <seq_num>13102 INFO TACACS TACACS+ TLS Identity Check: SAN DirName matched, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13102 INFO TACACS TACACS+ TLS Identity Check: SAN DirName matched, <log details>

- **Message Code:** 13103

  Severity: INFO

  Message Text: TACACS+ TLS Identity Check: SAN DirName did not match

  Message Description: TACACS+ TLS Identity Check: SAN DirName did not match.

Local Target Message Format: <timestamp> <seq_num>13103 INFO TACACS TACACS+ TLS Identity Check: SAN DirName did not match, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13103 INFO TACACS TACACS+ TLS Identity Check: SAN DirName did not match, <log details>

- **Message Code:** 13104

  Severity: WARN

  Message Text: TACACS+ TLS: NAD requested a TLS version lower than TLSv1.3

  Message Description: TACACS+ TLS: NAD requested a TLS version lower than TLSv1.3.

  Local Target Message Format: <timestamp> <seq_num>13104 WARN TACACS TACACS+ TLS: NAD requested a TLS version lower than TLSv1.3, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>13104 WARN TACACS TACACS+ TLS: NAD requested a TLS version lower than TLSv1.3, <log details>

Threat Centric NAC

- **Message Code:** 91001

  Severity: ERROR

  Message Text: IRF Core Engine is not running

  Message Description: IRF Core Engine is not running

  Local Target Message Format: <timestamp> <seq_num> 91001 ERROR IRF: IRF Core Engine is not running, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91001 ERROR IRF: IRF Core Engine is not running, <log details>

- **Message Code:** 91002

  Severity: ERROR

  Message Text: Lost connection to adapter

  Message Description: Lost connection to adapter

  Local Target Message Format: <timestamp> <seq_num> 91002 ERROR IRF: Lost connection to adapter, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91002 ERROR IRF: Lost connection to adapter, <log details>

- **Message Code:** 91003

  Severity: INFO

Message Text: Stopped adapter instance

Message Description: Stopped adapter instance

Local Target Message Format: <timestamp> <seq_num> 91003 INFO IRF: Stopped adapter instance, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91003 INFO IRF: Stopped adapter instance, <log details>

- **Message Code:** 91004

  Severity: INFO

  Message Text: Started adapter instance

  Message Description: Started adapter instance

  Local Target Message Format: <timestamp> <seq_num> 91004 INFO IRF: Started adapter instance, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91004 INFO IRF: Started adapter instance, <log details>

- **Message Code:** 91005

  Severity: INFO

  Message Text: Configuration changed for adapter instance

  Message Description: Configuration changed for adapter instance

  Local Target Message Format: <timestamp> <seq_num> 91005 INFO IRF: Configuration changed for adapter instance, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91005 INFO IRF: Configuration changed for adapter instance, <log details>

- **Message Code:** 91006

  Severity: ERROR

  Message Text: An error occurred for adapter instance

  Message Description: An error occurred for adapter instance

  Local Target Message Format: <timestamp> <seq_num> 91006 ERROR IRF: An error occurred for adapter instance, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91006 ERROR IRF: An error occurred for adapter instance, <log details>

- **Message Code:** 91007

  Severity: INFO

  Message Text: Threat event received

Message Description: Threat event received

Local Target Message Format: <timestamp> <seq_num> 91007 INFO IRF: Threat event received, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91007 INFO IRF: Threat event received, <log details>

- **Message Code:** 91008

  Severity: FATAL

  Message Text: Vulnerability Scan failure

  Message Description: Vulnerability Scan failure

  Local Target Message Format: <timestamp> <seq_num> 91008 FATAL IRF: Vulnerability Scan failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91008 FATAL IRF: Vulnerability Scan failure, <log details>

- **Message Code:** 91009

  Severity: FATAL

  Message Text: Adapter had encountered a connection or configuration error

  Message Description: Adapter had encountered a connection or configuration error

  Local Target Message Format: <timestamp> <seq_num> 91009 FATAL IRF: Adapter had encountered a connection or configuration error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91009 FATAL IRF: Adapter had encountered a connection or configuration error, <log details>

- **Message Code:** 91010

  Severity: FATAL

  Message Text: An IRF Service component has reported some errors

  Message Description: An IRF Service component has reported some errors

  Local Target Message Format: <timestamp> <seq_num> 91010 FATAL IRF: An IRF Service component has reported some errors, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91010 FATAL IRF: An IRF Service component has reported some errors, <log details>

- **Message Code:** 91011

  Severity: INFO

  Message Text: An IRF Service component has send some notification

  Message Description: An IRF Service component has send some notification

Local Target Message Format: <timestamp> <seq_num> 91011 INFO IRF: An IRF Service component has send some notification, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91011 INFO IRF: An IRF Service component has send some notification, <log details>

- **Message Code:** 91012

  Severity: FATAL

  Message Text: An IRF Service component is down

  Message Description: An IRF Service component is down

  Local Target Message Format: <timestamp> <seq_num> 91012 FATAL IRF: An IRF Service component is down, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91012 FATAL IRF: An IRF Service component is down, <log details>

- **Message Code:** 91013

  Severity: INFO

  Message Text: COA initiated

  Message Description: Change of authority initiated

  Local Target Message Format: <timestamp> <seq_num> 91013 INFO IRF: COA initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91013 INFO IRF: COA initiated, <log details>

- **Message Code:** 91014

  Severity: INFO

  Message Text: COA successful

  Message Description: Change of authority successful

  Local Target Message Format: <timestamp> <seq_num> 91014 INFO IRF: COA successful, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91014 INFO IRF: COA successful, <log details>

- **Message Code:** 91015

  Severity: ERROR

  Message Text: COA initiated

  Message Description: Change of authority initiated

  Local Target Message Format: <timestamp> <seq_num> 91015 ERROR IRF: COA initiated, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91015 ERROR IRF: COA initiated, <log details>

- **Message Code:** 91016

  Severity: INFO

  Message Text: Adapter connection initiated

  Message Description: Adapter connection initiated

  Local Target Message Format: <timestamp> <seq_num> 91016 INFO IRF: Adapter connection initiated, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91016 INFO IRF: Adapter connection initiated, <log details>

- **Message Code:** 91017

  Severity: INFO

  Message Text: Adapter connection success

  Message Description: Adapter connection success

  Local Target Message Format: <timestamp> <seq_num> 91017 INFO IRF: Adapter connection success, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91017 INFO IRF: Adapter connection success, <log details>

- **Message Code:** 91018

  Severity: ERROR

  Message Text: Adapter connection failed

  Message Description: Adapter connection failed

  Local Target Message Format: <timestamp> <seq_num> 91018 ERROR IRF: Adapter connection failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91018 ERROR IRF: Adapter connection failed, <log details>

- **Message Code:** 91019

  Severity: INFO

  Message Text: Vulnerability Assessment Scan Status

  Message Description: Vulnerability Assessment Scan Status

  Local Target Message Format: <timestamp> <seq_num> 91019 INFO IRF: Vulnerability Assessment Scan Status, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91019 INFO IRF: Vulnerability Assessment Scan Status, <log details>

- **Message Code:** 91020

  Severity: ERROR

  Message Text: Active Directory dialin access denied for user.

  Message Description: Active Directory dialin access denied for user.

  Local Target Message Format: <timestamp> <seq_num> 91020 ERROR External-Active-Directory: Active Directory dialin access denied for user., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91020 ERROR External-Active-Directory: Active Directory dialin access denied for user., <log details>

- **Message Code:** 91030

  Severity: INFO

  Message Text: RADIUS DTLS handshake started

  Message Description: RADIUS DTLS handshake started

  Local Target Message Format: <timestamp> <seq_num> 91030 INFO RADIUS: RADIUS DTLS handshake started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91030 INFO RADIUS: RADIUS DTLS handshake started, <log details>

- **Message Code:** 91031

  Severity: INFO

  Message Text: RADIUS DTLS: received client hello message

  Message Description: RADIUS DTLS: received client hello message

  Local Target Message Format: <timestamp> <seq_num> 91031 INFO RADIUS: RADIUS DTLS: received client hello message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91031 INFO RADIUS: RADIUS DTLS: received client hello message, <log details>

- **Message Code:** 91032

  Severity: INFO

  Message Text: RADIUS DTLS: sent server hello message

  Message Description: RADIUS DTLS: sent server hello message

  Local Target Message Format: <timestamp> <seq_num> 91032 INFO RADIUS: RADIUS DTLS: sent server hello message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91032 INFO RADIUS: RADIUS DTLS: sent server hello message, <log details>

- **Message Code:** 91033

  Severity: INFO

  Message Text: RADIUS DTLS: sent server certificate

  Message Description: RADIUS DTLS: sent server certificate

  Local Target Message Format: <timestamp> <seq_num> 91033 INFO RADIUS: RADIUS DTLS: sent server certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91033 INFO RADIUS: RADIUS DTLS: sent server certificate, <log details>

- **Message Code:** 91034

  Severity: INFO

  Message Text: RADIUS DTLS: sent client certificate request

  Message Description: RADIUS DTLS: sent client certificate request

  Local Target Message Format: <timestamp> <seq_num> 91034 INFO RADIUS: RADIUS DTLS: sent client certificate request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91034 INFO RADIUS: RADIUS DTLS: sent client certificate request, <log details>

- **Message Code:** 91035

  Severity: INFO

  Message Text: RADIUS DTLS: sent server done message

  Message Description: RADIUS DTLS: sent server done message

  Local Target Message Format: <timestamp> <seq_num> 91035 INFO RADIUS: RADIUS DTLS: sent server done message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91035 INFO RADIUS: RADIUS DTLS: sent server done message, <log details>

- **Message Code:** 91036

  Severity: INFO

  Message Text: RADIUS DTLS: received client certificate

  Message Description: RADIUS DTLS: received client certificate

  Local Target Message Format: <timestamp> <seq_num> 91036 INFO RADIUS: RADIUS DTLS: received client certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91036 INFO RADIUS: RADIUS DTLS: received client certificate, <log details>

- **Message Code:** 91037

  Severity: INFO

  Message Text: RADIUS DTLS: received client key exchange message

  Message Description: RADIUS DTLS: received client key exchange message

  Local Target Message Format: <timestamp> <seq_num> 91037 INFO RADIUS: RADIUS DTLS: received client key exchange message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91037 INFO RADIUS: RADIUS DTLS: received client key exchange message, <log details>

- **Message Code:** 91038

  Severity: INFO

  Message Text: RADIUS DTLS: received certificate verify message

  Message Description: RADIUS DTLS: received certificate verify message

  Local Target Message Format: <timestamp> <seq_num> 91038 INFO RADIUS: RADIUS DTLS: received certificate verify message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91038 INFO RADIUS: RADIUS DTLS: received certificate verify message, <log details>

- **Message Code:** 91039

  Severity: INFO

  Message Text: RADIUS DTLS: received finished message

  Message Description: RADIUS DTLS: received finished message

  Local Target Message Format: <timestamp> <seq_num> 91039 INFO RADIUS: RADIUS DTLS: received finished message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91039 INFO RADIUS: RADIUS DTLS: received finished message, <log details>

- **Message Code:** 91040

  Severity: INFO

  Message Text: RADIUS DTLS: sent change cipher spec message

  Message Description: RADIUS DTLS: sent change cipher spec message

  Local Target Message Format: <timestamp> <seq_num> 91040 INFO RADIUS: RADIUS DTLS: sent change cipher spec message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91040 INFO RADIUS: RADIUS DTLS: sent change cipher spec message, <log details>

- **Message Code:** 91041

  Severity: INFO

  Message Text: RADIUS DTLS: sent finished message

  Message Description: RADIUS DTLS: sent finished message

  Local Target Message Format: <timestamp> <seq_num> 91041 INFO RADIUS: RADIUS DTLS: sent finished message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91041 INFO RADIUS: RADIUS DTLS: sent finished message, <log details>

- **Message Code:** 91042

  Severity: INFO

  Message Text: RADIUS DTLS: sent client hello message

  Message Description: RADIUS DTLS: sent client hello message

  Local Target Message Format: <timestamp> <seq_num> 91042 INFO RADIUS: RADIUS DTLS: sent client hello message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91042 INFO RADIUS: RADIUS DTLS: sent client hello message, <log details>

- **Message Code:** 91043

  Severity: INFO

  Message Text: RADIUS DTLS: received server hello message

  Message Description: RADIUS DTLS: received server hello message

  Local Target Message Format: <timestamp> <seq_num> 91043 INFO RADIUS: RADIUS DTLS: received server hello message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91043 INFO RADIUS: RADIUS DTLS: received server hello message, <log details>

- **Message Code:** 91044

  Severity: INFO

  Message Text: RADIUS DTLS: received server certificate

  Message Description: RADIUS DTLS: received server certificate

  Local Target Message Format: <timestamp> <seq_num> 91044 INFO RADIUS: RADIUS DTLS: received server certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91044 INFO RADIUS: RADIUS DTLS: received server certificate, <log details>

- **Message Code:** 91045

  Severity: INFO

  Message Text: RADIUS DTLS: received server certificate request

  Message Description: RADIUS DTLS: received server certificate request

  Local Target Message Format: <timestamp> <seq_num> 91045 INFO RADIUS: RADIUS DTLS: received server certificate request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91045 INFO RADIUS: RADIUS DTLS: received server certificate request, <log details>

- **Message Code:** 91046

  Severity: INFO

  Message Text: RADIUS DTLS: received server done message

  Message Description: RADIUS DTLS: received server done message

  Local Target Message Format: <timestamp> <seq_num> 91046 INFO RADIUS: RADIUS DTLS: received server done message, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91046 INFO RADIUS: RADIUS DTLS: received server done message, <log details>

- **Message Code:** 91047

  Severity: INFO

  Message Text: RADIUS DTLS: sent client certificate

  Message Description: RADIUS DTLS: sent client certificate

  Local Target Message Format: <timestamp> <seq_num> 91047 INFO RADIUS: RADIUS DTLS: sent client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91047 INFO RADIUS: RADIUS DTLS: sent client certificate, <log details>

- **Message Code:** 91048

  Severity: INFO

  Message Text: RADIUS DTLS: sent client key exchange message

  Message Description: RADIUS DTLS: sent client key exchange message

  Local Target Message Format: <timestamp> <seq_num> 91048 INFO RADIUS: RADIUS DTLS: sent client key exchange message, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91048 INFO RADIUS: RADIUS DTLS: sent client key exchange message, <log details>

- **Message Code:** 91049

  Severity: INFO

  Message Text: RADIUS DTLS: read server session ticket

  Message Description: RADIUS DTLS: read server session ticket

  Local Target Message Format: <timestamp> <seq_num> 91049 INFO RADIUS: RADIUS DTLS: read server session ticket, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91049 INFO RADIUS: RADIUS DTLS: read server session ticket, <log details>

- **Message Code:** 91050

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because of an unknown CA in the certificates chain

  Message Description: RADIUS DTLS: SSL handshake failed because of an unknown CA in the certificates chain

  Local Target Message Format: <timestamp> <seq_num> 91050 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of an unknown CA in the certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91050 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of an unknown CA in the certificates chain, <log details>

- **Message Code:** 91051

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because of a bad certificate in the certificate chain

  Message Description: RADIUS DTLS: TLS handshake failed because of a bad certificate in the certificate chain

  Local Target Message Format: <timestamp> <seq_num> 91051 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of a bad certificate in the certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91051 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of a bad certificate in the certificate chain, <log details>

- **Message Code:** 91052

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because decryption error

  Message Description: RADIUS DTLS: TLS handshake failed because decryption error

Local Target Message Format: <timestamp> <seq_num> 91052 WARN RADIUS: RADIUS DTLS: TLS handshake failed because decryption error, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91052 WARN RADIUS: RADIUS DTLS: TLS handshake failed because decryption error, <log details>

- **Message Code:** 91053

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because certificate has expired

  Message Description: RADIUS DTLS: TLS handshake failed because certificate has expired

  Local Target Message Format: <timestamp> <seq_num> 91053 WARN RADIUS: RADIUS DTLS: TLS handshake failed because certificate has expired, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91053 WARN RADIUS: RADIUS DTLS: TLS handshake failed because certificate has expired, <log details>

- **Message Code:** 91054

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because unknown certificate

  Message Description: RADIUS DTLS: TLS handshake failed because unknown certificate

  Local Target Message Format: <timestamp> <seq_num> 91054 WARN RADIUS: RADIUS DTLS: TLS handshake failed because unknown certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91054 WARN RADIUS: RADIUS DTLS: TLS handshake failed because unknown certificate, <log details>

- **Message Code:** 91055

  Severity: INFO

  Message Text: RADIUS packet is encrypted

  Message Description: RADIUS packet is encrypted

  Local Target Message Format: <timestamp> <seq_num> 91055 INFO RADIUS: RADIUS packet is encrypted, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91055 INFO RADIUS: RADIUS packet is encrypted, <log details>

- **Message Code:** 91056

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because of unsupported protocol version

  Message Description: RADIUS DTLS: TLS handshake failed because of unsupported protocol version

Local Target Message Format: <timestamp> <seq_num> 91056 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of unsupported protocol version, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91056 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of unsupported protocol version, <log details>

- **Message Code:** 91057

  Severity: WARN

  Message Text: RADIUS DTLS CoA: TLS handshake failed because of an unknown CA in the certificates chain

  Message Description: RADIUS DTLS CoA: SSL handshake failed because of an unknown CA in the certificates chain

  Local Target Message Format: <timestamp> <seq_num> 91057 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because of an unknown CA in the certificates chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91057 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because of an unknown CA in the certificates chain, <log details>

- **Message Code:** 91058

  Severity: WARN

  Message Text: RADIUS DTLS CoA: TLS handshake failed because of a bad certificate in the certificate chain

  Message Description: RADIUS DTLS CoA: TLS handshake failed because of a bad certificate in the certificate chain

  Local Target Message Format: <timestamp> <seq_num> 91058 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because of a bad certificate in the certificate chain, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91058 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because of a bad certificate in the certificate chain, <log details>

- **Message Code:** 91059

  Severity: WARN

  Message Text: RADIUS DTLS CoA: TLS handshake failed because decryption error

  Message Description: RADIUS DTLS CoA: TLS handshake failed because decryption error

  Local Target Message Format: <timestamp> <seq_num> 91059 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because decryption error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91059 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because decryption error, <log details>

- **Message Code:** 91060

  Severity: WARN

Message Text: RADIUS DTLS CoA: TLS handshake failed because certificate has expired

Message Description: RADIUS DTLS CoA: TLS handshake failed because certificate has expired

Local Target Message Format: <timestamp> <seq_num> 91060 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because certificate has expired, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91060 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because certificate has expired, <log details>

- **Message Code:** 91061

  Severity: WARN

  Message Text: RADIUS DTLS CoA: TLS handshake failed because unknown certificate

  Message Description: RADIUS DTLS CoA: TLS handshake failed because unknown certificate

  Local Target Message Format: <timestamp> <seq_num> 91061 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because unknown certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91061 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because unknown certificate, <log details>

- **Message Code:** 91062

  Severity: WARN

  Message Text: RADIUS DTLS CoA: TLS handshake failed because of unsupported protocol version

  Message Description: RADIUS DTLS CoA: TLS handshake failed because of unsupported protocol version

  Local Target Message Format: <timestamp> <seq_num> 91062 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because of unsupported protocol version, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91062 WARN RADIUS: RADIUS DTLS CoA: TLS handshake failed because of unsupported protocol version, <log details>

- **Message Code:** 91063

  Severity: WARN

  Message Text: RADIUS DTLS CoA: Client Certificate in not found in System certificates list

  Message Description: RADIUS DTLS CoA: Client Certificate in not found in System certificates list

  Local Target Message Format: <timestamp> <seq_num> 91063 WARN RADIUS: RADIUS DTLS CoA: Client Certificate in not found in System certificates list, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91063 WARN RADIUS: RADIUS DTLS CoA: Client Certificate in not found in System certificates list, <log details>

- **Message Code:** 91064

  Severity: WARN

Message Text: RADIUS DTLS connection disconnect due to OCSP found revoked certificate

Message Description: OCSP check result is that the certificate used for RADIUS DTLS connection is revoke

Local Target Message Format: <timestamp> <seq_num> 91064 WARN RADIUS: RADIUS DTLS connection disconnect due to OCSP found revoked certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91064 WARN RADIUS: RADIUS DTLS connection disconnect due to OCSP found revoked certificate, <log details>

- **Message Code:** 91065

  Severity: WARN

  Message Text: RADIUS DTLS connection disconnect due to CRL found revoked certificate

  Message Description: CRL check result is that the certificate used for RADIUS DTLS connection is revoke

  Local Target Message Format: <timestamp> <seq_num> 91065 WARN RADIUS: RADIUS DTLS connection disconnect due to CRL found revoked certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91065 WARN RADIUS: RADIUS DTLS connection disconnect due to CRL found revoked certificate, <log details>

- **Message Code:** 91066

  Severity: WARN

  Message Text: RADIUS DTLS connection disconnect because of the client certificate is not yet valid

  Message Description: OCSP check result is that the certificate used for RADIUS DTLS connection is not yet valid

  Local Target Message Format: <timestamp> <seq_num> 91066 WARN RADIUS: RADIUS DTLS connection disconnect because of the client certificate is not yet valid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91066 WARN RADIUS: RADIUS DTLS connection disconnect because of the client certificate is not yet valid, <log details>

- **Message Code:** 91067

  Severity: WARN

  Message Text: RADIUS DTLS CoA connection disconnect due to OCSP found revoked certificate

  Message Description: OCSP check result is that the certificate used for RADIUS DTLS CoA connection is revoke

  Local Target Message Format: <timestamp> <seq_num> 91067 WARN RADIUS: RADIUS DTLS CoA connection disconnect due to OCSP found revoked certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91067 WARN RADIUS: RADIUS DTLS CoA connection disconnect due to OCSP found revoked certificate, <log details>

- **Message Code:** 91068

  Severity: WARN

  Message Text: RADIUS DTLS CoA connection disconnect due to CRL found revoked certificate

  Message Description: CRL check result is that the certificate used for RADIUS DTLS CoA connection is revoke

  Local Target Message Format: <timestamp> <seq_num> 91068 WARN RADIUS: RADIUS DTLS CoA connection disconnect due to CRL found revoked certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91068 WARN RADIUS: RADIUS DTLS CoA connection disconnect due to CRL found revoked certificate, <log details>

- **Message Code:** 91069

  Severity: WARN

  Message Text: RADIUS DTLS CoA connection disconnect because of the server certificate is not yet valid

  Message Description: OCSP check result is that the certificate used for RADIUS DTLS CoA connection is not yet valid

  Local Target Message Format: <timestamp> <seq_num> 91069 WARN RADIUS: RADIUS DTLS CoA connection disconnect because of the server certificate is not yet valid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91069 WARN RADIUS: RADIUS DTLS CoA connection disconnect because of the server certificate is not yet valid, <log details>

- **Message Code:** 91070

  Severity: INFO

  Message Text: RADIUS DTLS CoA handshake started

  Message Description: RADIUS DTLS CoA handshake started

  Local Target Message Format: <timestamp> <seq_num> 91070 INFO RADIUS: RADIUS DTLS CoA handshake started, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91070 INFO RADIUS: RADIUS DTLS CoA handshake started, <log details>

- **Message Code:** 91071

  Severity: INFO

  Message Text: RADIUS DTLS: Sent an OCSP request to the primary OCSP server for the CA

  Message Description: RADIUS DTLS: Send an OCSP request to the primary OCSP server for the CA.

  Local Target Message Format: <timestamp> <seq_num> 91071 INFO RADIUS: RADIUS DTLS: Sent an OCSP request to the primary OCSP server for the CA, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91071 INFO RADIUS: RADIUS DTLS: Sent an OCSP request to the primary OCSP server for the CA, <log details>

- **Message Code:** 91072

  Severity: INFO

  Message Text: RADIUS DTLS: Sent an OCSP request to the secondary OCSP server for the CA

  Message Description: RADIUS DTLS: Send an OCSP request to the secondary OCSP server for the CA.

  Local Target Message Format: <timestamp> <seq_num> 91072 INFO RADIUS: RADIUS DTLS: Sent an OCSP request to the secondary OCSP server for the CA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91072 INFO RADIUS: RADIUS DTLS: Sent an OCSP request to the secondary OCSP server for the CA, <log details>

- **Message Code:** 91073

  Severity: WARN

  Message Text: RADIUS DTLS: Conversation with OCSP server ended with failure

  Message Description: RADIUS DTLS: Conversation with OCSP server ended with failure.

  Local Target Message Format: <timestamp> <seq_num> 91073 WARN RADIUS: RADIUS DTLS: Conversation with OCSP server ended with failure, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91073 WARN RADIUS: RADIUS DTLS: Conversation with OCSP server ended with failure, <log details>

- **Message Code:** 91074

  Severity: INFO

  Message Text: RADIUS DTLS: Received OCSP response

  Message Description: RADIUS DTLS: Received OCSP response.

  Local Target Message Format: <timestamp> <seq_num> 91074 INFO RADIUS: RADIUS DTLS: Received OCSP response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91074 INFO RADIUS: RADIUS DTLS: Received OCSP response, <log details>

- **Message Code:** 91075

  Severity: INFO

  Message Text: RADIUS DTLS: OCSP status of user certificate is good

  Message Description: RADIUS DTLS: The OCSP server reported that the user certificate status is good.

  Local Target Message Format: <timestamp> <seq_num> 91075 INFO RADIUS: RADIUS DTLS: OCSP status of user certificate is good, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91075 INFO RADIUS: RADIUS DTLS: OCSP status of user certificate is good, <log details>

- **Message Code:** 91076

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP status of user certificate is revoked

  Message Description: RADIUS DTLS: The OCSP server reported that the user certificate status is revoked.

  Local Target Message Format: <timestamp> <seq_num> 91076 WARN RADIUS: RADIUS DTLS: OCSP status of user certificate is revoked, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91076 WARN RADIUS: RADIUS DTLS: OCSP status of user certificate is revoked, <log details>

- **Message Code:** 91077

  Severity: INFO

  Message Text: RADIUS DTLS: OCSP status of user certificate is unknown

  Message Description: RADIUS DTLS: The OCSP server reported that the user certificate status is unknown or ISE was unable to connect to the OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 91077 INFO RADIUS: RADIUS DTLS: OCSP status of user certificate is unknown, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91077 INFO RADIUS: RADIUS DTLS: OCSP status of user certificate is unknown, <log details>

- **Message Code:** 91078

  Severity: WARN

  Message Text: RADIUS DTLS: Handshake failed because OCSP status is unknown

  Message Description: RADIUS DTLS: Handshake failed because OCSP status is unknown.

  Local Target Message Format: <timestamp> <seq_num> 91078 WARN RADIUS: RADIUS DTLS: Handshake failed because OCSP status is unknown, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91078 WARN RADIUS: RADIUS DTLS: Handshake failed because OCSP status is unknown, <log details>

- **Message Code:** 91079

  Severity: INFO

  Message Text: RADIUS DTLS: Performed fallback to secondary OCSP server

  Message Description: RADIUS DTLS: Performed fallback to secondary OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 91079 INFO RADIUS: RADIUS DTLS: Performed fallback to secondary OCSP server, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91079 INFO RADIUS: RADIUS DTLS: Performed fallback to secondary OCSP server, <log details>

- **Message Code:** 91080

  Severity: WARN

  Message Text: RADIUS DTLS: Internal error occurred during communication with the OCSP server

  Message Description: RADIUS DTLS: Internal error during communication with the OCSP server. The configuration of the OCSP server doesn't match the ISE OCSP client.

  Local Target Message Format: <timestamp> <seq_num> 91080 WARN RADIUS: RADIUS DTLS: Internal error occurred during communication with the OCSP server, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91080 WARN RADIUS: RADIUS DTLS: Internal error occurred during communication with the OCSP server, <log details>

- **Message Code:** 91081

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server URL is invalid

  Message Description: RADIUS DTLS: OCSP server URL is invalid and cannot be properly parsed.

  Local Target Message Format: <timestamp> <seq_num> 91081 WARN RADIUS: RADIUS DTLS: OCSP server URL is invalid, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91081 WARN RADIUS: RADIUS DTLS: OCSP server URL is invalid, <log details>

- **Message Code:** 91082

  Severity: WARN

  Message Text: RADIUS DTLS: Connection to OCSP server failed

  Message Description: RADIUS DTLS: Connection attempt to OCSP server failed.

  Local Target Message Format: <timestamp> <seq_num> 91082 WARN RADIUS: RADIUS DTLS: Connection to OCSP server failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91082 WARN RADIUS: RADIUS DTLS: Connection to OCSP server failed, <log details>

- **Message Code:** 91083

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server response is invalid

  Message Description: RADIUS DTLS: OCSP server returned a response that cannot be parsed by ISE.

  Local Target Message Format: <timestamp> <seq_num> 91083 WARN RADIUS: RADIUS DTLS: OCSP server response is invalid, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91083 WARN RADIUS: RADIUS DTLS: OCSP server response is invalid, <log details>

- **Message Code:** 91084

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server returned an error

  Message Description: RADIUS DTLS: OCSP server returned an error in response to the ISE OCSP request.

  Local Target Message Format: <timestamp> <seq_num> 91084 WARN RADIUS: RADIUS DTLS: OCSP server returned an error, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91084 WARN RADIUS: RADIUS DTLS: OCSP server returned an error, <log details>

- **Message Code:** 91085

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server did not provide the required nonce in response

  Message Description: RADIUS DTLS: Specific OCSP service in ISE is configured to use nonce for OCSP server verification but the OCSP server did not provide a nonce in response.

  Local Target Message Format: <timestamp> <seq_num> 91085 WARN RADIUS: RADIUS DTLS: OCSP server did not provide the required nonce in response, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91085 WARN RADIUS: RADIUS DTLS: OCSP server did not provide the required nonce in response, <log details>

- **Message Code:** 91086

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server response nonce verification failed

  Message Description: RADIUS DTLS: Cryptographic verification of nonce returned in OCSP server response failed.

  Local Target Message Format: <timestamp> <seq_num> 91086 WARN RADIUS: RADIUS DTLS: OCSP server response nonce verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91086 WARN RADIUS: RADIUS DTLS: OCSP server response nonce verification failed, <log details>

- **Message Code:** 91087

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server response time verification failed

  Message Description: RADIUS DTLS: In the OCSP server response verification of 'This Update' or 'Next Update' fields failed.

Local Target Message Format: <timestamp> <seq_num> 91087 WARN RADIUS: RADIUS DTLS: OCSP server response time verification failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91087 WARN RADIUS: RADIUS DTLS: OCSP server response time verification failed, <log details>

- **Message Code:** 91088

  Severity: WARN

  Message Text: RADIUS DTLS: OCSP server response signature verification failed

  Message Description: RADIUS DTLS: OCSP server response signature verification failed.

  Local Target Message Format: <timestamp> <seq_num> 91088 WARN RADIUS: RADIUS DTLS: OCSP server response signature verification failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91088 WARN RADIUS: RADIUS DTLS: OCSP server response signature verification failed, <log details>

- **Message Code:** 91089

  Severity: INFO

  Message Text: RADIUS DTLS: Lookup certificate status in OCSP cache

  Message Description: RADIUS DTLS: Lookup certificate status in OCSP cache.

  Local Target Message Format: <timestamp> <seq_num> 91089 INFO RADIUS: RADIUS DTLS: Lookup certificate status in OCSP cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91089 INFO RADIUS: RADIUS DTLS: Lookup certificate status in OCSP cache, <log details>

- **Message Code:** 91090

  Severity: INFO

  Message Text: RADIUS DTLS:Certificate status was not found in OCSP cache

  Message Description: RADIUS DTLS: Certificate status was not found in OCSP cache; ISE is going to perform OCSP request to the configured OCSP server.

  Local Target Message Format: <timestamp> <seq_num> 91090 INFO RADIUS: RADIUS DTLS:Certificate status was not found in OCSP cache, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91090 INFO RADIUS: RADIUS DTLS:Certificate status was not found in OCSP cache, <log details>

- **Message Code:** 91091

  Severity: INFO

  Message Text: RADIUS DTLS: Lookup Certificate status in OCSP cache succeeded

  Message Description: RADIUS DTLS: LookupCertificate status in OCSP cache succeeded; ISE is going to use this status without performing OCSP request to the configured OCSP server.

Local Target Message Format: <timestamp> <seq_num> 91091 INFO RADIUS: RADIUS DTLS: Lookup Certificate status in OCSP cache succeeded, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91091 INFO RADIUS: RADIUS DTLS: Lookup Certificate status in OCSP cache succeeded, <log details>

- **Message Code:** 91092

  Severity: INFO

  Message Text: RADIUS DTLS: ISE will continue to CRL verification if it is configured for specific CA

  Message Description: RADIUS DTLS: OCSP verification either failed or returned unknown certificate status. ISE will continue to CRL verification if it is configured for specific CA.

  Local Target Message Format: <timestamp> <seq_num> 91092 INFO RADIUS: RADIUS DTLS: ISE will continue to CRL verification if it is configured for specific CA, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91092 INFO RADIUS: RADIUS DTLS: ISE will continue to CRL verification if it is configured for specific CA, <log details>

- **Message Code:** 91093

  Severity: DEBUG

  Message Text: RADIUS DTLS: OCSP response not cached

  Message Description: RADIUS DTLS: Response from OCSP server indicates that the contents of the response should not be cached

  Local Target Message Format: <timestamp> <seq_num> 91093 DEBUG RADIUS: RADIUS DTLS: OCSP response not cached, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91093 DEBUG RADIUS: RADIUS DTLS: OCSP response not cached, <log details>

- **Message Code:** 91094

  Severity: INFO

  Message Text: RADIUS DTLS: Take OCSP servers list from AIA extension of client certificate

  Message Description: RADIUS DTLS: Take OCSP servers list from AIA extension of client certificate

  Local Target Message Format: <timestamp> <seq_num> 91094 INFO RADIUS: RADIUS DTLS: Take OCSP servers list from AIA extension of client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91094 INFO RADIUS: RADIUS DTLS: Take OCSP servers list from AIA extension of client certificate, <log details>

- **Message Code:** 91095

  Severity: INFO

  Message Text: RADIUS DTLS: Take OCSP servers list from OCSP service configuration

Message Description: RADIUS DTLS: Take OCSP servers list from OCSP service configuration

Local Target Message Format: <timestamp> <seq_num> 91095 INFO RADIUS: RADIUS DTLS: Take OCSP servers list from OCSP service configuration, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91095 INFO RADIUS: RADIUS DTLS: Take OCSP servers list from OCSP service configuration, <log details>

- **Message Code:** 91096

  Severity: INFO

  Message Text: RADIUS DTLS: Sent an OCSP request to the next OCSP server in the list

  Message Description: RADIUS DTLS: Sent an OCSP request to the next OCSP server in the list

  Local Target Message Format: <timestamp> <seq_num> 91096 INFO RADIUS: RADIUS DTLS: Sent an OCSP request to the next OCSP server in the list, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91096 INFO RADIUS: RADIUS DTLS: Sent an OCSP request to the next OCSP server in the list, <log details>

- **Message Code:** 91097

  Severity: WARN

  Message Text: RADIUS DTLS: No valid OCSP server URLs found in the AIA extension of client certificate

  Message Description: RADIUS DTLS: If the OCSP service was configured to take OCSP servers list from the AIA extension of client certificate then at least one valid OCSP server URL must be present.

  Local Target Message Format: <timestamp> <seq_num> 91097 WARN RADIUS: RADIUS DTLS: No valid OCSP server URLs found in the AIA extension of client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91097 WARN RADIUS: RADIUS DTLS: No valid OCSP server URLs found in the AIA extension of client certificate, <log details>

- **Message Code:** 91098

  Severity: INFO

  Message Text: RADIUS DTLS: No more OCSP servers in AIA estension of client certificate

  Message Description: RADIUS DTLS: No more OCSP servers in AIA estension of client certificate

  Local Target Message Format: <timestamp> <seq_num> 91098 INFO RADIUS: RADIUS DTLS: No more OCSP servers in AIA estension of client certificate, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91098 INFO RADIUS: RADIUS DTLS: No more OCSP servers in AIA estension of client certificate, <log details>

- **Message Code:** 91099

  Severity: INFO

  Message Text: RADIUS DTLS: No AIA extension in client certificate

Message Description: RADIUS DTLS: No AIA extension in client certificate

Local Target Message Format: <timestamp> <seq_num> 91099 INFO RADIUS: RADIUS DTLS: No AIA extension in client certificate, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91099 INFO RADIUS: RADIUS DTLS: No AIA extension in client certificate, <log details>

- **Message Code:** 91100

  Severity: WARN

  Message Text: RADIUS DTLS: Handshake failed because OCSP is unreachable

  Message Description: RADIUS DTLS: Handshake failed because OCSP is unreachable

  Local Target Message Format: <timestamp> <seq_num> 91100 WARN RADIUS: RADIUS DTLS: Handshake failed because OCSP is unreachable, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91100 WARN RADIUS: RADIUS DTLS: Handshake failed because OCSP is unreachable, <log details>

- **Message Code:** 91101

  Severity: INFO

  Message Text: RADIUS DTLS: User certificate was revoked by CRL verification

  Message Description: RADIUS DTLS: CRL verification returned revoked certificate status.

  Local Target Message Format: <timestamp> <seq_num> 91101 INFO RADIUS: RADIUS DTLS: User certificate was revoked by CRL verification, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91101 INFO RADIUS: RADIUS DTLS: User certificate was revoked by CRL verification, <log details>

- **Message Code:** 91102

  Severity: WARN

  Message Text: RADIUS DTLS: client Identity check failed

  Message Description: RADIUS DTLS: Client Identity check failed.

  Local Target Message Format: <timestamp> <seq_num> 91102 WARN RADIUS: RADIUS DTLS: client Identity check failed, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91102 WARN RADIUS: RADIUS DTLS: client Identity check failed, <log details>

- **Message Code:** 91103

  Severity: INFO

  Message Text: RADIUS DTLS: client Identity check needed

  Message Description: RADIUS DTLS: Client Identity check needed.

Local Target Message Format: <timestamp> <seq_num> 91103 INFO RADIUS: RADIUS DTLS: client Identity check needed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91103 INFO RADIUS: RADIUS DTLS: client Identity check needed, <log details>

- **Message Code:** 91104

  Severity: INFO

  Message Text: RADIUS DTLS: no need to run Client Identity check

  Message Description: RADIUS DTLS: No need to run Client Identity check.

  Local Target Message Format: <timestamp> <seq_num> 91104 INFO RADIUS: RADIUS DTLS: no need to run Client Identity check, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91104 INFO RADIUS: RADIUS DTLS: no need to run Client Identity check, <log details>

- **Message Code:** 91105

  Severity: INFO

  Message Text: RADIUS DTLS: sent client hello verify request

  Message Description: RADIUS DTLS: sent client hello verify request.

  Local Target Message Format: <timestamp> <seq_num> 91105 INFO RADIUS: RADIUS DTLS: sent client hello verify request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91105 INFO RADIUS: RADIUS DTLS: sent client hello verify request, <log details>

- **Message Code:** 91106

  Severity: INFO

  Message Text: RADIUS DTLS: received client hello verify request

  Message Description: RADIUS DTLS: received client hello verify request.

  Local Target Message Format: <timestamp> <seq_num> 91106 INFO RADIUS: RADIUS DTLS: received client hello verify request, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91106 INFO RADIUS: RADIUS DTLS: received client hello verify request, <log details>

- **Message Code:** 91107

  Severity: WARN

  Message Text: RADIUS DTLS: TLS handshake failed because of client hello verification failed

  Message Description: RADIUS DTLS: TLS handshake failed because of client hello verification failed.

Local Target Message Format: <timestamp> <seq_num> 91107 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of client hello verification failed, <log details>

Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num> 91107 WARN RADIUS: RADIUS DTLS: TLS handshake failed because of client hello verification failed, <log details>

- **Message Code:** 91110

  Severity: WARN

  Message Text: One or more Active Directory diagnostic tests failed during a scheduled run.

  Message Description: One or more Active Directory diagnostic tests failed during a scheduled run.

  Local Target Message Format: <timestamp> <seq_num>91110 WARN RADIUS One or more Active Directory diagnostic tests failed during a scheduled run., <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>91110 WARN RADIUS One or more Active Directory diagnostic tests failed during a scheduled run., <log details>

- **Message Code:** 91111

  Severity: WARN

  Message Text: High authentication load detected

  Message Description: High authentication load detected

  Local Target Message Format: <timestamp> <seq_num>91111 WARN RADIUS High authentication load detected, <log details>

  Remote Target Message Format: <pri_num> <timestamp> <IP address/hostname> <CISE_logging category> <msg_id> <total seg> <seg num><timestamp> <seq_num>91111 WARN RADIUS High authentication load detected, <log details>

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.