

About This Guide

The following topics explain how to use this guide.

- What's New in Each Release, on page i
- About Secure Firewall Threat Defense Syslog Messages, on page v
- Configure the System to Send Syslog Messages, on page x
- Communications, Services, and Additional Information, on page x

What's New in Each Release

Security Event Syslog Messages

Changes to syslog messages for the following event types are described in the History for Security Event Syslog Messages:

- Intrusion events
- Connection events
- Security Intelligence events
- File events
- Malware events

All Other Syslog Messages

This section provides the following new, changed, and deprecated syslog messages for the following Secure Firewall Threat Defense releases. For complete syslog message descriptions, see respective chapters.

- Version 10.1
- Version 10.0
- Version 7.7
- Version 7.6
- Version 7.4.1
- Version 7.4

- Version 7.3
- Version 7.2
- Version 7.1
- Version 7.0
- Version 6.7
- Version 6.6
- Version 6.5
- Version 6.4

For Version 10.1, there are no new, changed, or deprecated syslog messages.

Table 1: New, Changed, and Deprecated Syslog Message for Version 10.0

New Syslog Messages	716163, 716164, 717067, 717068, 717069, 717070
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	302014, 302016
Deprecated Syslog Messages	None

Table 2: New, Changed, and Deprecated Syslog Message for Version 7.7

New Syslog Messages	716166, 751031, 780005, 780006
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	None
Deprecated Syslog Messages	None

Table 3: New, Changed, and Deprecated Syslog Message for Version 7.6

New Syslog Messages	413009
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	None
Deprecated Syslog Messages	None

Table 4: New, Changed, and Deprecated Syslog Message for Version 7.4.1

New Syslog Messages	709015
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	None

Deprecated Syslog Messages	None

Table 5: New, Changed, and Deprecated Syslog Message for Version 7.4

New Syslog Messages	717071, 717072, 870001, 880001, 880002
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	302020, 302021
Deprecated Syslog Messages	None

Table 6: New, Changed, and Deprecated Syslog Message for Version 7.3

New Syslog Messages	No new syslog messages were added.
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	None
Deprecated Syslog Messages	None

Table 7: New, Changed, and Deprecated Syslog Message for Version 7.2

New Syslog Messages	No new syslog messages were added.
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	None
Deprecated Syslog Messages	None

Table 8: New, Changed, and Deprecated Syslog Message for Version 7.1

New Syslog Messages	709009, 709010, 709011, 709012, 709013
Changed Syslog Messages (Document)	None
Changed Syslog Messages (Code)	None
Deprecated Syslog Messages	None

Table 9: New, Changed, and Deprecated Syslog Message for Version 7.0

New Syslog Messages	302037, 302038, 305021, 305022, 324302, 324303, 717032, 722057, 733201
Changed Syslog Messages (Document)	717009
Changed Syslog Messages (Code)	None
Deprecated Syslog Messages	716055 and 716056

Table 10: New, Changed, and Deprecated Syslog Message for Version 6.7

New Syslog Messages	106029
Changed Syslog Messages (Document)	105042, 105003, 105004, 105043, 305006, 414004
Changed Syslog Messages (Code)	302013, 302014
Deprecated Syslog Messages	None

Table 11: New, Changed, and Deprecated Syslog Message for Version 6.6

New Syslog Messages	209006, 324012

Table 12: New, Changed, and Deprecated Syslog Message for Version 6.5

New Syslog Messages	748011, 748012, 302311, 747042, 747043, 747044, 769007, 769009, 852001, 852002
Changed Syslog Messages	302014
Deprecated Syslog Messages	

Table 13: New, Changed, and Deprecated Syslog Messages for Version 6.4

New Syslog Messages	Security events: 430004, 430005 Other: 305017, 408101, 408102, 409014, 409015, 409016, 409017, 419004, 419005, 419006, 503002, 503003, 503004, 503005, 737038, 737200-737206,737400-737407, 747042, 747043, 747044, 768003, 768004 815002, 815003, 815004
Changed Syslog Messages	737001-737019, 737031-737036
Deprecated Syslog Messages	

All Syslog Messages

Table 14: Changes to Syslog Messages for Version 6.3

Timestamp Logging	Beginning with version 6.3, Secure Firewall Threat Defense provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. Following is a sample output with RFC 5424 format: `<166>2018-06-27T12:17:46Z firepower : %FTD-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port` **Note** The PRI value, <166> in the above example, is the priority value that represents both Facility and Severity of the alert. Syslog messages in RFC5424 format, typically displays PRI. However, in case of Firewall Management Center managed Firewall Threat Defense, PRI value appears in the syslog messages only when you enable logging in EMBLEM format using Firewall Management Center platform settings. For information on how to enable the EMBLEM format, see *Cisco Secure Firewall Management Center Administration Guide*. For information on PRI, see RFC5424.
Syslog Prefix Format	The Firewall Threat Defenseoperating system was using parts of the ASA operating system, including the syslog utility. Therefore, Firewall Threat Defense syslog messages were starting with "%ASA" due to this shared utility. Beginning with release 6.3, the Firewall Threat Defense syslog messages will be starting with "%FTD"

About Secure Firewall Threat Defense Syslog Messages

Note Information in this topic does not apply to messages related to security events.

The following table lists the message classes and the ranges of message IDs that are associated with each class. The valid range for message IDs is between 100000 and 999999.

Note When a number is missing in a sequence, the message may no longer in the Firewall Threat Defense device code.

Most of the ISAKMP messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a message when available. If the object is not known at the time the message is generated, the specific **heading = value** combination will not be displayed.

The objects will be prepended as follows:

Group = **groupname**, Username = **user**, IP = **IP_address**,...

Where the Group identifies the tunnel group, the Username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

Typically, a traffic session displays the connection numbers/IDs sequentially for each flow in the syslog messages. However, for some of the connections, though the connection ID is incremented, the syslog messages does not display the ID. Thus, you may find missing sequence numbers in the connection IDs of the subsequent messages. For example, during a TCP traffic flow, the syslog messages display the connection IDs as 201, 202, 203, and 204 for each flow. When an ICMP flow begins, though the connection ID is internally incremented to 205 and 206, the syslog messages does not display the numbers. When another TCP flow follows, its connection numbers are now displayed as 207, 208, and so on, giving an impression of skipping sequence.



Remember Connection ID is by itself not an unique identifier of a specific event. Use the connection ID only in conjunction with the device name/ID, the Instance ID, and the FirstPacketSecond to identify a specific event. For instance, when pivoting from an intrusion event to the associated connection event.

Table 15: Syslog message classes and associated message ID numbers

Class	Definition	Syslog Message ID Numbers
access-list*	Access Lists	106
application-firewall*	Application Firewall	415
auth	User Authentication	109, 113
botnet-traffic-filtering*	Botnet Traffic Filtering	338
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
card-management*	Card Management	323
citrix	Citrix Client	723
clustering*	Clustering	747
config	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policies	734
EAP, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
EIGRP	EIGRP Routing	336
email	E-mail Proxy	719
environment-monitoring*	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709

Class	Definition	Syslog Message ID Numbers
identity-based-firewall*	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733
ikev2-toolkit*	IKEv2 Toolkit	750, 751, 752
IP	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	400, 401, 420
ipv6*	IPv6	325
licensing*	Licensing	444
MDM-proxy	MDM Proxy	802
NAC	Network Admission Control	731, 732
nacpolicy	NAC Policy	731
nacsettings	NAC Settings to apply NAC Policy	732
NAT-and-PAT*	NAT and PAT	305
network-access-point*	Network Access Point	713
NP	Network Processor	319
NP-SSL*	NP SSL	725
OSPF	OSPF Routing	318, 409, 503, 613
password-encryption*	Password Encryption	742
phone-proxy*	Phone Proxy	337
RIP	RIP Routing	107, 312
rm	Resource Manager	321
scansafe*	ScanSafe	775
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
smart-call-home*	Smart Call Home	120
SNMP	SNMP proxy	212
SSL	SSL Stack	725

Class	Definition	Syslog Message ID Numbers
svc	SSL VPN Client	722
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
tag-switching	Service Tag Switching	779
threat-detection*	Threat Detection	733
transactional-rule-engine-tre*	Transactional Rule Engine	780
uc-IMS*	UC-IMS	339
vm	VLAN Mapping	730
vpdn	PPTP and L2TP Sessions	213, 403, 603
VPN	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
VXLAN*	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and Secure Client	716

Syslog Message Format

Syslog messages are structured as follows:

`[<PRI>]: [Timestamp] [Device-ID] : %FTD-Class-Level-Message_number: Message_text`

Field descriptions are as follows:

<PRI>	Priority value. When the logging EMBLEM is enabled, this value is displayed in the syslog message. Logging EMBLEM is compatible with UDP and not with TCP.
Timestamp	Date and time of the event is displayed. When logging of timestamps is enabled, and if the timestamp is configured to be in the RFC 5424 format, all timestamp in syslog messages display the time in UTC, as indicated by the RFC 5424 standard. By default, the data plane syslogs that are generated by the Lina engine on the Secure Firewall Threat Defense are in the UTC timezone and not of the local time zone.
Device-ID	The device identifier string that was configured while enabling the logging device-id option through the user interface. If enabled, the device ID does not appear in EMBLEM-formatted syslog messages.

Class	The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the device. For example, the vpnc class denotes VPN Client. Message class appears only in EMBLEM-formatted syslog messages.
FTD	The syslog message facility code for messages that are generated by the FTD. This value is always `FTD`.
Level	0 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition.
Message_number	A unique six-digit number that identifies the syslog message.
Message_text	A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.

All syslog messages that are generated by the device in non-EMBLEM format are documented in this guide.

The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. Hence, when EMBLEM is enabled, the syslog message prints colon (:) after <PRI> field.

Example of a syslog message with logging EMBLEM, logging timestamp rfc5424, and device-id enabled. Note the colon (:) after the <PRI> field (<*166*>) and the message class before *Level*.

```
<166>:2018-06-27T12:17:46Z: %FTD-bridge-6-110002: Failed to locate egress interface for
protocol from src interface :src IP/src port to dest IP/dest port
```

Example of a syslog message without logging EMBLEM, but with logging timestamp rfc5424 and device-id enabled. No colon (:) is present before the timestamp, and the configured device-id (example, *ftd1*) is included after the timestamp.

```
2018-06-27T12:17:46Z ftd1: %FTD-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

Handling Connection Event Syslog Alerting

The Secure Firewall Threat Defense (formerly known as, Firepower Threat Defense (FTD)) versions 7.0.5 and later, and 7.2.x and later, generate syslog messages with a colon (:) between the *Timestamp* or *Device-ID* (if present) and the *%FTD-Level-Message_number* string. The other Secure Firewall Threat Defense versions do not include such colon (:) character. Therefore, if you use filtering rules on the syslog server or the SIEM application to identify syslog messages from devices running the Secure Firewall Threat Defense software, make sure that the match criteria accounts for the presence (versions 7.0.5 and later, and 7.2.x and later) or absence (earlier versions) of the colon (:) character, so that messages are not missed.

For example, in the following syslog message from the Firewall Threat Defense Virtual device, a space and colon is used to separate the hostname from the rest of the message:

```
Apr 10 18:52:47 labuser-ftdv : %FTD-6-305012: Teardown dynamic UDP translation from
inside:10.51.100.1/54453 to outside:10.0.2.3/54453 duration 0:00:00
```

If your regular expression to match syslog messages from the Firewall Threat Defense devices look like this (in this example, only the colon character portion of the regular expression is displayed):

```
^... .. ..:..:.. [-[:alpha:]]+[[:space:]]*%FTD
```

Change your regular expression to have the colon character (:) after the hostname as optional in the messages, like this:

```
^... .. ..:..:.. [-[:alpha:]]+[[:space:]](:?[[:space:]])%FTD
```

With this recommended regular expression, regardless of the presence or absence of colon (:) in the syslog messages, the filtering rules will work as expected.

Note

- The `(:?[[:space:]]*)` addition to the regular expression would make the regular expression match 0 or 1 colon (:) character followed by zero or more spaces.
- The recommended workaround must be implemented on the syslog server or the SIEM that the Firewall Threat Defense devices are sending syslog messages to.
- Alternatively, you can simplify the regular expression to only match `%FTD-[[:digit:]]`. This will also match regardless of the presence or absence of a colon (:) after the *Timestamp* or *Device-ID* (if present).

Configure the System to Send Syslog Messages

A syslog is generated as soon as a triggering event occurs. The maximum rate at which the Firewall Threat Defense can send the syslog messages depends on the level of syslog and the available CPU resources. The number of events the Firewall Management Center can store depends on its model. To improve system performance, you can configure the event generation limits, threshold limits, and you can even disable storage for some event types.

You can also log events to an external syslog, or SNMP trap server, or other external tools. However, configure the system with external servers or tools to use the syslog-ng process of the firewall system. Do not initiate external configuration files, like the *scwx.conf* file from SecureWorks. Such files are not compatible with the device. Using them will lead to parsing error and eventually the syslog-ng process will fail. For more information about these system logging configurations, see the *Cisco Secure Firewall Management Center Device Configuration Guide* or *Cisco Secure Firewall Device Manager Configuration Guide* for your release.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.