

# Cisco Identity Services Engine Passive Identity Connector Administrator Guide, Release 3.4

**First Published:** 2024-08-05

**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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2024 Cisco Systems, Inc. All rights reserved.



# CONTENTS


CHAPTER 1 **Introduction to ISE-PIC** 1

Cisco ISE-PIC Terminology 1

ISE-PIC Overview 2

Cisco ISE-PIC Architecture, Deployments, and Nodes 3

Benefits of ISE-PIC 4

Comparing ISE-PIC with Cisco ISE and Cisco Context Directory Agent 5

CHAPTER 2 **Getting Started with ISE-PIC** 9

Administrator Access Console 9

Administrator Login Browser Support 9

Secure SSH Key Exchange Using Diffie-Hellman Algorithm 10

Initial Setup and Configuration 10

ISE-PIC Smart Licensing 10

ISE-PIC Licensing Packages 11

Register and Activate Smart Licenses 12

Specific License Reservation 13

DNS Server 13

Specify System Time and Network Time Protocol Server Settings 14

ISE-PIC Home Dashboard 15

CHAPTER 3 **Active Directory as a Probe and a Provider** 17

Work with Active Directory 17

Getting Started with the PassiveID Setup 18

Set Up an Active Directory (WMI) Probe Step-by-Step 20

Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point 20

Add Domain Controllers 22

Configure Active Directory User Groups 23
Manage the Active Directory Provider 23
Test Users for Active Directory Groups 24
View Active Directory Joins for a Node 24
Diagnose Active Directory Problems 25
Leave the Active Directory Domain 25
Delete Active Directory Configurations 26
Enable Active Directory Debug Logs 27
Active Directory Settings 27

CHAPTER 4 **Providers** 31
Active Directory Agents 34
Automatically Install and Deploy Active Directory Agents 35
Manually Install and Deploy Active Directory Agents 36
Uninstall the Agent 37
Active Directory Agent Settings 37
API Providers 38
Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services 39
Send API Calls to the ISE-PIC REST Service 40
API Provider Settings 40
API Calls 41
SPAN 43
Working with SPAN 43
SPAN Settings 44
Syslog Providers 44
Configure Syslog Clients 45
Syslog Settings 46
Customize Syslog Message Structures (Templates) 49
Customize the Syslog Message Body 50
Customize Syslog Headers 50
Syslog Customized Template Settings and Examples 52
Work with Syslog Predefined Message Templates 54
Syslog ASA VPN Pre-Defined Template 55
Syslog Bluecat Pre-Defined Template 58

Syslog F5 VPN Pre-Defined Template 58
Syslog Infoblox Pre-Defined Template 59
Syslog Linux DHCPd3 Pre-Defined Template 60
Syslog MS DHCP Pre-Defined Template 60
Syslog SafeConnect NAC Pre-Defined Template 61
Syslog Aerohive Pre-Defined Templates 62
Syslog Blue Coat Pre-Defined Templates—Main Proxy, Proxy SG, Squid Web Proxy 62
Syslog ISE and ACS Pre-Defined Templates 64
Syslog Lucent QIP Pre-Defined Template 65
Filter Passive Identity Services 66
Endpoint Probe 67
Work with the Endpoint Probe 68
Generate pxGrid Certificates for Subscribers 68
Enable Subscribers 70
View Subscriber Events from Live Logs 70
Configure Subscriber Settings 70

CHAPTER 5 **Certificate Management in Cisco ISE-PIC** 73
Certificate Matching in Cisco ISE-PIC 74
Wildcard Certificates 74
Advantages of Using Wildcard Certificates 75
Disadvantages of Using Wildcard Certificates 76
Wildcard Certificate Compatibility 76
Certificate Hierarchy in ISE-PIC 77
System Certificates 77
View System Certificates 78
Import a System Certificate 79
Generate a Self-Signed Certificate 79
Edit a System Certificate 80
Delete a System Certificate 80
Export a System Certificate 81
Trusted Certificates Store 81
Trusted Certificate Naming Constraints 82
View Trusted Certificates 83

Change the Status of a Certificate in Trusted Certificates Store 84
Add a Certificate to Trusted Certificates Store 84
Edit a Trusted Certificate 85
Delete a Trusted Certificate 85
Export a Certificate from Trusted Certificates Store 86
Import a Root Certificate into the Trusted Certificate Store 86
Certificate Chain Import 87
Trusted Certificate Import Settings 87
Certificate-Signing Requests 88
Create a Certificate-Signing Request and Submit it to a Certificate Authority 88
Bind a CA-Signed Certificate to a Certificate Signing Request 89
Export a Certificate-Signing Request 90
Certificate-Signing Request Settings 90
Cisco ISE CA Service 94
Elliptical Curve Cryptography Certificates Support 95
Cisco ISE-PIC Certificate Authority Certificates 96
Edit a Cisco ISE-PIC CA Certificate 96
Export a Cisco ISE CA Certificate 96
Import a Cisco ISE-PIC CA Certificate 97
Trusted Certificate Settings 97
Backup and Restoration of Cisco ISE-PIC CA Certificates and Keys 99
Export Cisco ISE CA Certificates and Keys 100
Import Cisco ISE-PIC CA Certificates and Keys 100
Generate Root CA and Subordinate CAs 101
Configure Cisco ISE-PIC Root CA as Subordinate CA of an External PKI 102
OCSP Services 102
Cisco ISE CA Service Online Certificate Status Protocol Responder 102
OCSP Certificate Status Values 103
OCSP High Availability 103
OCSP Failures 104
Add OCSP Client Profiles 104
OCSP Statistics Counters 105

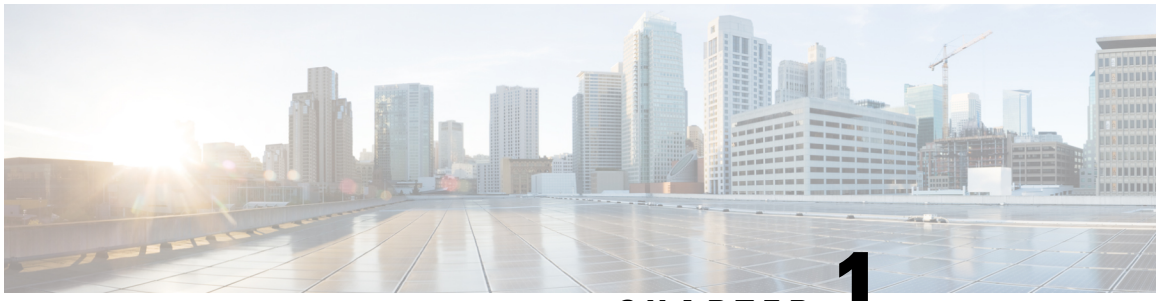
CHAPTER 6 **Administer ISE-PIC** 107

Manage ISE-PIC Nodes 107
Cisco ISE-PIC Deployment Setup 107
Data Replication from Primary to Secondary ISE-PIC Nodes 107
Effects of modifying nodes in Cisco ISE-PIC 108
Guidelines for Setting Up Two Nodes in a Deployment 108
View Nodes in a Deployment 109
Register a Secondary Cisco ISE-PIC Node 109
Synchronize Primary and Secondary Cisco ISE-PIC Nodes 110
Manually Promote Secondary PAN to Primary 110
Remove a Node from Deployment 111
Change the Hostname or IP Address of a Cisco ISE-PIC Node 111
Replace the Cisco ISE-PIC Appliance Hardware 112
Manage the ISE-PIC Installation 112
Install a software patch 113
Cisco ISE-PIC software patches 113
Software patch installation guidelines 114
Roll back software patches 114
Software patch rollback guidelines 115
Backup and Restore Data 115
Backup and Restore Repositories 115
Create Repositories 116
Repository Settings 117
Enable RSA Public Key Authentication in SFTP Repository 118
On-Demand and Scheduled Backups 119
Cisco ISE Restore Operation 123
Synchronize Primary and Secondary Nodes 127
Recovery of Lost Nodes in Standalone and Two-Node Deployments 127
Database Purge 130
Upgrading ISE-PIC to a Full ISE Installation 132
Upgrade to ISE by Registering Licenses 132
Manage Settings in ISE-PIC 133
Role-Based Access Control 133
Cisco ISE-PIC administrators 133
Cisco ISE-PIC administrator groups 134

Privileges of a CLI Administrator Versus a Web-Based Administrator 135
Create a new administrator 135
Administrative access to Cisco ISE-PIC 135
Administrator Access Settings 136
Ports Used by the Administration Portal 139
Configure SMTP Server to Support Notifications 139
Enabling External RESTful Services APIs from the GUI—ERS Settings 140
Configure Security Settings 141

CHAPTER 7 **Monitoring and Troubleshooting Service in ISE-PIC** 143
Live Sessions 143
Available Reports 146
Cisco ISE-PIC Alarms 148
Alarm Settings 156
Add Custom Alarms 157
TCP Dump Utility to Validate Incoming Traffic 158
Use TCP Dump to Monitor Network Traffic 158
Save a TCP Dump File 159
TCP Dump Settings 159
Logging Mechanism 160
Cisco ISE-PIC Logging Mechanism 160
Configure Syslog Purge Settings 160
Active Directory Troubleshooting 161
Prerequisites for Integrating Active Directory and Cisco ISE-PIC 161
Active Directory Account Permissions Required to Perform Various Operations 161
Network Ports that Must Be Open for Communication 162
Active Directory Requirements to Support ISE-PIC 163
Obtaining Additional Troubleshooting Information 173
Cisco ISE-PIC Support Bundle 173
Support Bundle 174
Download Cisco ISE-PIC Log Files 174
Cisco ISE-PIC Debug Logs 175
Obtain Debug Logs 175
Cisco ISE-PIC Components and Corresponding Debug Logs 175

Download Debug Logs 177
Additional References 178
Communications, services, and additional information 178
Cisco Bug Search Tool 178
Documentation feedback 178



CHAPTER 1

# Introduction to ISE-PIC

User identities must be authenticated in order to protect the network from unauthorized threats. To do so, security products are implemented on the networks. Each security product has its own method of retrieving the necessary authentication, often identifying authorized IP addresses, rather than authorized users. As a result, these products refer to different external servers and methods that provide authentications based on user login information, resulting in a de-centralized network. Cisco Identity Services Engine (ISE) Passive Identity Connector (ISE-PIC) offers a centralized installation and implementation enabling you to simply gather passive authentication data from a variety of sources and share those identities with security product subscribers.


- Cisco ISE-PIC Terminology, on page 1
- ISE-PIC Overview, on page 2
- Cisco ISE-PIC Architecture, Deployments, and Nodes, on page 3
- Benefits of ISE-PIC, on page 4
- Comparing ISE-PIC with Cisco ISE and Cisco Context Directory Agent, on page 5


## Cisco ISE-PIC Terminology

This guide uses the following terms when discussing Cisco ISE-PIC:

| Term | Definition |
|---|---|
| GUI | Graphic user interface. GUI refers to any of the screens and tabs in the software installation of ISE-PIC. |
| NIC | Network interface card. |
| Node | An individual physical or virtual Cisco ISE-PIC appliance. |
| PAN | The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN). |

| Term | Definition |
|---|---|
| Parser | The ISE-PIC backend component that receives syslog messages and breaks that input up into parts that can then be managed, mapped and published to ISE-PIC. The parser goes through each line of information of a syslog message as it arrives, looking for key information. For example, if a parser is configured to look for “mac=”, the parser then parses each line while looking for that phrase. The parser is set up to then communicate the defined information to ISE once it has found the key phrase that was configured. |
| Primary node | The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN). |
| Probe | Probes are mechanisms that collect data from a given source. Probe is a generic term that describes any mechanism, but does not specifically describe how the data is collected or what is collected. For example, an Active Directory (AD) probe helps ISE-PIC collect data from AD while a syslog probe collects data from a parser that reads syslog messages. |
| Provider | Clients or sources from which ISE-PIC receives, maps and publishes user identity information. |
| Secondary node | The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN). |
| Subscriber | Systems that subscribe to the ISE-PIC services in order to receive user identity information. |

# ISE-PIC Overview

Passive Identity Connector (ISE-PIC) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to receive and share user identity information with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, ISE-PIC collects user identities from different provider sources, such as Active Directory Domain Controllers (AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.



**Note** For information about the FMC and Stealthwatch releases that are validated with ISE, see *Cisco Identity Services Engine Network Component Compatibility*.

### What is Passive Identity?

Products such as the Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, communicate directly with the user or endpoint, requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

Passive identity services do not authenticate users directly, but rather gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers. ISE-PIC first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

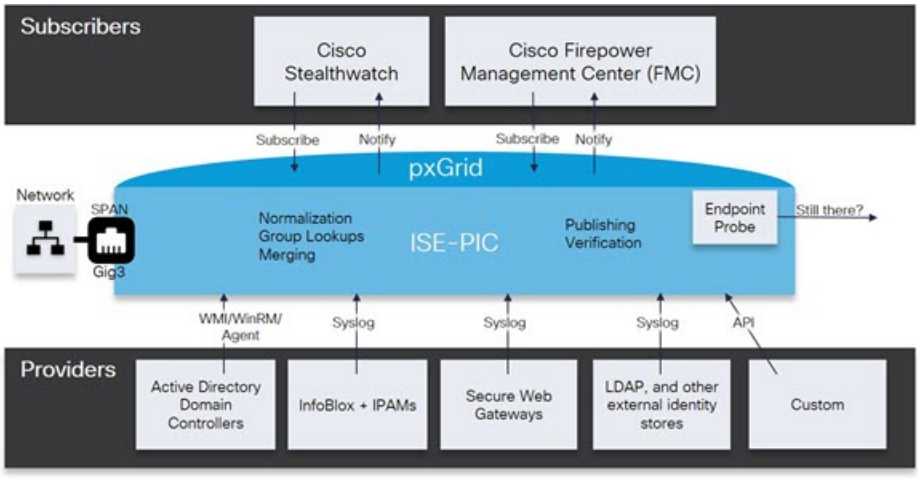
### Passive Identity Connector (ISE-PIC) Flow

The flow for ISE-PIC is as follows:

1. Provider performs the authentication of the user or endpoint.
2. Provider sends authenticated user information to ISE-PIC.
3. ISE-PIC normalizes, performs lookups, merges, parses and maps user information to IP addresses and publishes mapped details to pxGrid.
4. pxGrid subscribers receive the mapped user details.

The following diagram illustrates the high-level flow offered by ISE-PIC.

***Figure 1: High Level Flow***




# Cisco ISE-PIC Architecture, Deployments, and Nodes

Cisco ISE-PIC architecture includes the following components:

- Nodes—in a Cisco ISE-PIC deployment, up to two nodes can be configured as described below
- Network resources
- Endpoints

A deployment that has a single Cisco ISE-PIC node is called a *standalone deployment*.

A deployment that has two Cisco ISE-PIC nodes is called a *high availability deployment*, where one node functions as the primary appliance (the primary administration node, or the PAN). A high availability deployment improves service availability.

The PAN provides all the configuration capabilities that are required for this network model, and the secondary Cisco ISE node (the secondary PAN) functions in a backup role. The secondary node supports the primary node and resumes functionality whenever connectivity is lost with the primary node.

Cisco ISE-PIC synchronizes or replicates all of the content that resides on the primary Cisco ISE-PIC node with the secondary Cisco ISE-PIC node in order to ensure that your secondary node is current with the state of your primary node (and therefore can be used as a backup).

**ISE Community Resource**

For information about deployment and scaling, see ISE Deployment Journey.

**Note** From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

# Benefits of ISE-PIC

ISE-PIC offers you:

- A single identity solution that interacts with a variety of different providers.
- Friendly GUI enabling simple configuration, monitoring and troubleshooting
- Simple installation and configuration
- Easily upgraded to ISE for active authentication. When upgrading from ISE-PIC to a full ISE deployment and using the ISE-PIC node to create a standalone ISE deployment, or when adding this node as your primary node to an existing deployment, ISE will continue to offer all features that were available to you in ISE-PIC prior to upgrade and your existing configuration is preserved.

**Note** In order to upgrade to ISE, download a trial version or, contact your Cisco representative in order to discuss licensing options.

When you add your upgraded ISE-PIC to an existing ISE deployment, but not as the primary node, the previous ISE-PIC configurations will be overwritten.

For a full description of the upgrade flow, see Upgrading ISE-PIC to a Full ISE Installation, on page 132.

# Comparing ISE-PIC with Cisco ISE and Cisco Context Directory Agent

ISE-PIC brings with it many benefits, including the ability to smoothly and easily upgrade to Cisco ISE. In addition to ISE-PIC and Cisco ISE, Cisco also offers Cisco Context Directory Agent (CDA), an additional security mechanism. This section compares the three offers in the following tables:


- A Detailed Comparison of ISE-PIC with Cisco ISE, on page 5
- An Overview Comparison of ISE-PIC with Cisco ISE and CDA, on page 7


## A Detailed Comparison of ISE-PIC with Cisco ISE

ISE-PIC is designed to share passive identities only and provides no authorization or authentication services, both of which are provided by ISE, which offers authentication, authorization and accounting (AAA) servers. The differences between the two products are fully illustrated in the following table.

***Table 1: Comparing ISE-PIC with Cisco ISE***

| Category | Feature | ISE-PIC | Cisco ISE |
|---|---|---|---|
| Smart Licensing | | — | √ |
| Authentication and Authorization types | Authorization policies | — | √ |
| | TrustSec | — | √ |
| | Active Directory passive authentication including WMI | √ | √ |

| Category | Feature | ISE-PIC | Cisco ISE |
|---|---|---|---|
| Passive Identity sources | | √ | √ |
| | Easy Connect | — | √ |
| | SysLog sources | √ | √ |
| | REST API sources | √ | √ |
| | SPAN | √ | √ |
| | Security Group eXchange Protocol (SXP) | — | √ |
| | RADIUS including RADIUS proxy | — | √ |
| | BYOD | — | √ |
| | Guest | — | √ |
| | Posture | — | √ |
| | Device Administration (TACACS+) | — | √ |
| pxGrid | pxGrid controller | √<br>For Cisco subscribers only | √ |
| | pxGrid controller redundancy | √ | √ |
| | Topic extensibility | — | √ |
| Certificate Authority (CA) | pxGrid certificate templates | √ | √ |
| | Endpoint CA | — | √ |
| | Enrollment over secure transport (EST) | — | √ |
| | Other certificate templates | — | √ |
| Visibility and Context | Context Directory | — | √ |
| | Profiling | — | √ |

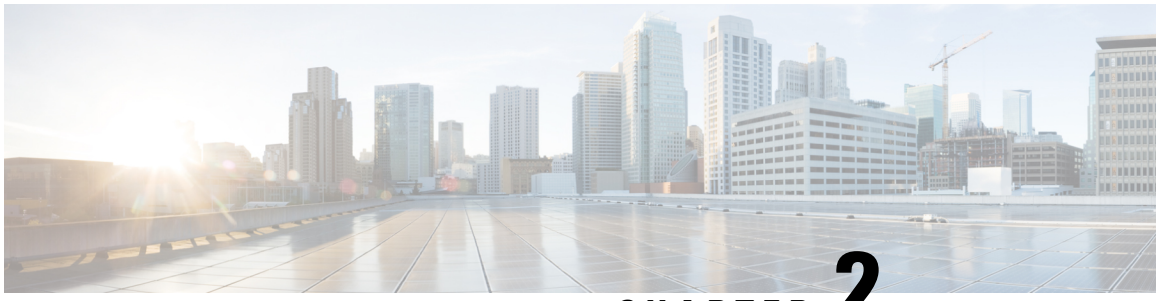
| Category | Feature | ISE-PIC | Cisco ISE |
|---|---|---|---|
| Reports | | !<br>**Note**<br>ISE-PIC offers reports that you can use to monitor the health of the system and troubleshoot issues in the network. However, ISE-PIC offers a subset of functionality in comparison with ISE, and hence some of the ISE reports are not available in ISE-PIC. | √ |

### An Overview Comparison of ISE-PIC with Cisco ISE and CDA

Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). ISE-PIC, however, collects user identities much more precisely by accessing additional data such as user name, MAC addresses and ports. The following table offers a high-level comparison of ISE-PIC, Cisco ISE and CDA.

***Table 2: Comparing ISE-PIC with Cisco ISE and CDA***

| Passive Auth Details | Full ISE | ISE-PIC | CDA |
|---|---|---|---|
| Number of domain controllers | 100 | 100 | 80 |
| Number of subscribers | 20 | 20 | — |
| WMI (Agentless) | Yes | Yes | Yes |
| Windows server agent available | Yes | Yes | — |
| DCOM required | No (SPAN) | No (SPAN) | Yes |
| Easy Connect | Yes | — | — |
| Kerberos sniffing with SPAN | Yes | Yes | — |
| Bindings (IP address, MAC address and user name) | 300,000 | 300,000 | 64,000 |



CHAPTER 2

# Getting Started with ISE-PIC


- Administrator Access Console, on page 9
- Initial Setup and Configuration, on page 10
- ISE-PIC Home Dashboard, on page 15


# Administrator Access Console

The following steps describe how to log in to the administrative portal.

### Before you begin

Ensure that you have correctly installed (or upgraded) and configured Cisco ISE-PIC. For more information and assistance with installation, upgrade and configuration of Cisco ISE-PIC, see *Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Upgrade Guide*.

### Procedure

**Step 1** Enter the Cisco ISE-PIC URL in the address bar of your browser (for example, https://<ise hostname or ip address>/admin/).

**Step 2** Enter the username and case-sensitive password that were specified and configured during the initial Cisco ISE setup.

**Step 3** Click **Login** or press **Enter**.

If your login is unsuccessful, click the **Problem logging in?** link in the log in window and follow the instructions that are displayed.

# Administrator Login Browser Support

The Cisco ISE administration portal supports the following HTTPS-enabled browsers:

- Mozilla Firefox 107 and earlier versions from version 82
- Mozilla Firefox ESR 102.4 and earlier versions
- Google Chrome 107 and earlier versions from version 86
- Microsoft Edge, the latest version and one version earlier than the latest version

**ISE Community Resource**

ISE Pages Fail to Fully Load When Adblock Plus is Used

# Secure SSH Key Exchange Using Diffie-Hellman Algorithm

Configure Cisco ISE-PIC to only allow Diffie-Hellman-Group14-SHA1 Secure Shell (SSH) key exchanges. Enter the following commands from the Cisco ISE-PIC CLI Configuration Mode:

**service sshd key-exchange-algorithm diffie-hellman-group14-sha1**

Here is an example:

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

# Initial Setup and Configuration

To get started using Cisco ISE-PIC quickly, follow this flow:

1. Install and register your licenses. For more information, see ISE-PIC Smart Licensing, on page 10.
2. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE-PIC. For more information, see DNS Server, on page 13.
3. Synchronize clock settings for the NTP servers.
4. Configure an initial provider with the ISE-PIC Setup. For more information, see Getting Started with the PassiveID Setup, on page 18.
5. Configure a single or multiple subscribers.

After setting up an initial provider and subscriber, you can easily create additional providers (see Providers, on page 31) and manage your passive identification from the different providers in ISE-PIC (see Monitoring and Troubleshooting Service in ISE-PIC, on page 143).

# ISE-PIC Smart Licensing

ISE-PIC 3.1 and above licenses are managed entirely through a centralized database that is called the Cisco Smart Software Manager (CSSM). You can register, activate, and manage all your licenses easily and efficiently with single token registration.

ISE-PIC 3.1 and above support only smart licensing and does not support traditional licensing. If you own traditional ISE-PIC licenses, you must convert them to smart licenses to enable license compliance in ISE-PIC 3.1 and above.

The Evaluation license is enabled by default when you first install ISE-PIC. Evaluation licenses are 90-day licenses that give you access to all the ISE-PIC features. During the evaluation period, license compliance status is not reported to the CSSM.

The top-right corner of the ISE-PIC administration portal displays a message with the number of days that are left in the Evaluation mode. You must purchase and activate the required licenses to continue using the ISE-PIC features you need.

When a smart license token is active and registered in the ISE-PIC administration portal, the CSSM monitors the license compliance status of the ISE-PIC node. License compliance status is displayed in the **Licenses** table in ISE-PIC. To view this information, choose **Administration > System > Licensing**.

From the time you register your ISE-PIC with the CSSM, ISE-PIC reports the license compliance status to the CSSM server every six hours. ISE-PIC communicates with the CSSM server by storing a local copy of the CSSM certificate. The CSSM certificate is automatically reauthorized during the daily synchronization, and when you refresh the **Licenses** table. Typically, CSSM certificates are valid for six months.

The registration certificate is automatically refreshed every six months. To manually refresh your Smart Licensing registration certificate, click **Renew Registration** from the top of the **Licensing** window.

If there is a change in the compliance status when ISE-PIC synchronizes with the CSSM server, the **Last Authorization** column of the **Licenses** table is updated accordingly. In addition, when entitlements are no longer compliant, the number of days for which they are out of compliance appears in the **Days Out of Compliance** column.

You should update the General Terms if:

- The evaluation period has ended, and you have not yet registered your license.
- Your license has expired.

An ISE-PIC node can be upgraded to a Cisco ISE node by enabling the Essential license. Before enabling the Essential license, you must purchase and enable both ISE-PIC and ISE-PIC Upgrade licenses on the ISE-PIC node. The Essential license is displayed in the **Licenses** table after you register the license in CSSM. The application services are restarted during the upgrade. For information about Cisco ISE licenses, see the *Cisco Identity Services Engine Administrator Guide*.

ISE-PIC 3.1 and above support the VM Common license. This license replaces the VM Small, VM Medium, and VM Large licenses that were supported in releases earlier than 3.1. This VM License covers the VM nodes in both on-prem and cloud deployments. If you have legacy VM license, you must migrate your VM license to the VM Common license while upgrading to Cisco ISE 3.1 or above. To convert legacy licenses to the new license types, open a case online through the Support Case Manager at http://cs.co/scmswl, or use the contact information that is provided at http://cs.co/TAC-worldwide.

Alarms regarding the licensing status, such as license registration success or failure, license out of compliance, evaluation license expiry, smart licensing communication failure are displayed in the **Alarms** dashlet.

## ISE-PIC Licensing Packages

The following license packages are available for ISE-PIC:

| License Packages | Subscription | Functionality Covered | Notes |
|---|---|---|---|
| ISE-PIC | Perpetual | Passive identity services | One license per node. Each license supports up to 3,000 parallel sessions. |
| ISE-PIC Upgrade | Perpetual | • Enable additional (up to 300,000) parallel sessions<br>• Upgrade to full ISE instance | One license per node. Each license supports up to 300,000 parallel sessions. |

| | | | |
|---|---|---|---|
| Essential | Term-based license | • RADIUS authentication, authorization, and accounting, including 802.1X, MAC authentication bypass, easy connect, and web authentication<br>• MACsec<br>• Authentications that are based on Single Sign-On (SSO), Security Assertion Markup Language (SAML), and Open DataBase Connectivity (ODBC) standards<br>• Guest access and sponsor services<br>• Representational State Transfer (REST) APIs for monitoring purposes, and External RESTful Services APIs for CRUD operations<br>• Passive ID services<br>• Secure wired and wireless access | — |
| Evaluation | Temporary (90 days) | Enables full ISE-PIC functionality for 90 days | — |

## Register and Activate Smart Licenses

### Before you begin

- If you have traditional ISE-PIC licenses, you must convert them to smart licenses.
- Register your new smart license types in CSSM to receive a registration token.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Licensing**.

**Step 2** Click **Registration Details**.

**Step 3** In the **Registration Details** area, enter the registration token that you received from CSSM, in the **Registration Token** field.

**Step 4** Choose a connection method from the **Connection Method** drop-down list:

- **Direct HTTPS**: Choose this option if you have configured a direct connection to the Internet.
- **HTTPS Proxy**: Choose this option if you do not have a direct connection to the Internet and need to use a proxy server. If you change your proxy server configuration after you register the smart licenses, you must update your smart licenses configuration in the **Licensing** window. ISE-PIC establishes a connection with the CSSM using the updated proxy server, avoiding any disruption of ISE-PIC services.
- **Transport Gateway**: This is the recommended option. If you have configured a Transport Gateway, this connection is chosen by default. To choose another connection method, you must remove the Transport Gateway configuration.
- **SSM On-Prem Server**: Choose this option to connect to the configured SSM on-prem server.

**Step 5** In the **Tier** and **Virtual Appliance** areas, check the check boxes for all the licenses you need to enable. The chosen licenses are activated and their compliance is tracked by CSSM.

**Step 6** Click **Register**.

After you register your license token, if your CSSM account does not include certain entitlements and you did not disable them during registration, noncompliant notifications will appear in ISE-PIC. Add those entitlements to your CSSM account, and then click **Refresh** in the **Licenses** table to remove noncompliant notifications.

To remove your ISE-PIC registration from your Smart Account, but continue to use smart licensing till the end of the evaluation period, click **Deregister** from the top of the **Cisco Smart Licensing** area. If you still have time remaining in your evaluation period, ISE-PIC remains in smart licensing. If your evaluation period is about to expire, a notification appears when the browser is refreshed. After you deregister your smart license, you can follow the registration process again in order to register with the same or different UDIs.

## Specific License Reservation

Specific License Reservation is a smart licensing method that helps you manage your smart licensing when your organization's security requirements do not allow a persistent connection between ISE-PIC and CSSM. Specific License Reservation allows you to reserve specific licenses entitlements on an ISE-PIC node.

You create a Specific License Reservation by defining the type and number of licenses you need to reserve, and then activate the reservation on an ISE-PIC node. The ISE-PIC node on which you register and enable the reservation then tracks license usage and enforces license consumption compliance.



**Note** You cannot upgrade an ISE-PIC node to a Cisco ISE node when you are using Specific License Reservation. In order to upgrade, you must first return Specific License Reservation, enable Smart Licensing Registration, and then install ISE-PIC Upgrade and Essential licenses.

# DNS Server

While configuring your DNS server, make sure that you take care of the following:

- The DNS servers that you configure in Cisco ISE must be able to resolve all forward and reverse DNS queries for the domains that you want to use.
- The Authoritative DNS server is recommended to resolve Active Directory records, as DNS recursion can cause delays and have significant negative impact on performance.

- All DNS servers must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.
- Cisco recommends that you add the server IP addresses to SRV responses to improve performance.
- Avoid using DNS servers that query the public Internet. They can leak information about your network when an unknown name has to be resolved.

# Specify System Time and Network Time Protocol Server Settings

Cisco ISE-PIC allows you to configure up to three NTP servers. Use the NTP servers to maintain accurate time and synchronize time across different timezones. You can also specify whether Cisco ISE-PIC must use only authenticated NTP servers and enter one or more authentication keys for that purpose.

We recommend that you set all the Cisco ISE-PIC nodes to the Coordinated Universal Time (UTC) timezone. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized.

Cisco ISE supports public key authentication for NTP servers. NTP Version 4 uses symmetric key cryptography and also provides a new Autokey security model that is based on public key cryptography. Public-key cryptography is considered to be more secure than symmetric key cryptography. This is because the security is based on a private value that is generated by each server and never revealed. With the Autokey security model, all the key distribution and management functions involve only public values, which simplify key distribution and storage considerably.

You can configure the Autokey security model for the NTP server from the Cisco ISE CLI in configuration mode. We recommend that you use the identification friend or foe (IFF) system because this system is most widely used.

### Procedure

**Step 1** In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Settings** > **System Time**.

**Step 2** In the **NTP Server Configuration** area, enter the unique IP addresses (IPv4 or IPv6 or fully qualified domain name [FQDN] value) for your NTP servers.

**Step 3** (Optional) To authenticate the NTP server using private keys, click the **NTP Authentication Keys** tab and specify one or more authentication keys if any of the servers that you specify require authentication through an authentication key. Carry out the following steps:

a) Click **Add**.

b) Enter the necessary values in the **Key ID** and **Key Value** fields. Choose the required Hashed Message Authentication Code (HMAC) value from the **HMAC** drop-down list.The **Key ID** field supports numeric values between 1 to 65535 and the **Key Value** field supports up to 1028 alphanumeric characters.

c) Click **OK**.

d) Return to the **NTP Server Configuration** tab.

**Step 4** (Optional) To authenticate the NTP server using public key authentication, configure the Autokey security model on Cisco ISE from the CLI. See the **ntp server** and **crypto** commands in the Cisco Identity Services Engine CLI Reference Guide for your Cisco ISE release.

**Step 5** Click **Save**.

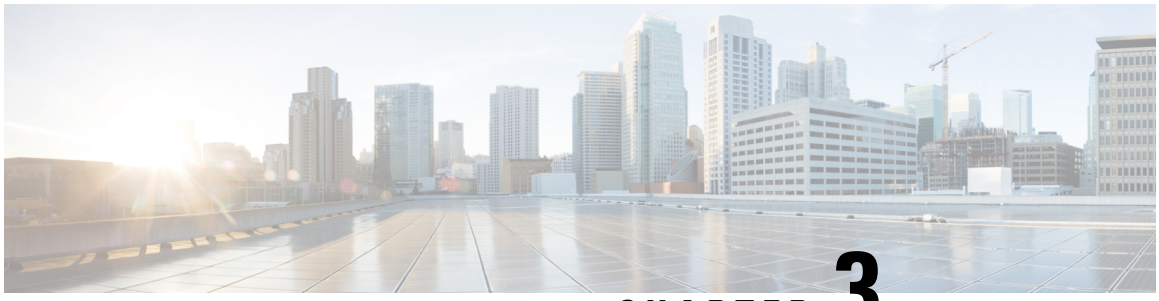


**Note** Use three or more NTP servers to ensure accurate time synchronization across your network, even if one of the servers fails or two of the servers are out of sync. See https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services.

# ISE-PIC Home Dashboard

The Cisco ISE-PIC Home dashboard displays consolidated and correlated summary and statistical data that is essential for effective monitoring and troubleshooting, and is updated in real time. Dashlets show activity over the last 24 hours, unless otherwise noted.

- The **Main** view has a linear Metrics dashboard, chart dashlets, and list dashlets. In ISE-PIC, the dashlets are not configurable. Some dashlets are disabled, and are only available in the full version of ISE. For example, dashlets that display endpoint data. Available dashlets include:
  - **Passive Identity Metrics**: Displays the total number of unique live sessions currently being tracked, the total number of identity providers configured in the system, the total number of agents actively delivering identity data, and the total number of subscribers currently configured.
  - **Providers**: Providers provide user identity information to ISE-PIC. You configure the ISE-PIC probe (mechanisms that collect data from a given source) through which to receive information from the provider sources. For example, an Active Directory (AD) probe and an Agents probe both help ISE-PIC collect data from AD (each with different technology) while a Syslog probe collects data from a parser that reads syslog messages.
  - **Subscribers**: Subscribers connect to ISE-PIC to retrieve user identity information.
  - **OS Types**: The only OS type that can be displayed is Windows. Windows types display by Windows versions. Providers do not report the OS type, but ISE-PIC can query Active Directory to get that information. Up to 1000 entries are displayed in the dashlet. If you have more endpoints than that, or if you wish to display more OS types than Windows, you can upgrade to ISE.
  - **Alarms**: User identity-related alarms.
- The **Additional**view displays Active Sessions on PIC, and a System Summary of the PIC system.



CHAPTER 3

# Active Directory as a Probe and a Provider

Active Directory (AD) is a highly secure and precise source from which to receive user identity information, including user name, IP address, and domain name.

By configuring the Active Directory probe you can also then quickly configure and enable these other probes (which also use Active Directory as their source):

- Active Directory Agents, on page 34

**Note** The Active Directory agents are only supported on Windows Server 2008 and higher.

- SPAN, on page 43
- Endpoint Probe, on page 67

In addition, configure the Active Directory probe in order to use AD user groups when collecting user information. You can use AD user groups for the AD, Agents, SPAN, and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 23.

- Work with Active Directory, on page 17
- Active Directory Settings, on page 27

# Work with Active Directory

Before you configure the Active Directory probe for Passive Identity services, make sure that:

- The Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- The Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE-PIC. For more information, see DNS Server, on page 13.
- Synchronize clock settings for the NTP servers. For more information, see Specify System Time and Network Time Protocol Server Settings, on page 14.

**Note** If you see operational issues when Cisco ISE-PIC is connected to Active Directory, see the AD Connector Operations Report under **Reports**. For more information, see Available Reports, on page 146.

# Getting Started with the PassiveID Setup

ISE-PIC offers a wizard from which you can easily and quickly configure Active Directory as your first user identity provider, in order to receive user identities from Active Directory. By configuring Active Directory for ISE-PIC, you also simplify the process for configuring other provider types later on. Once you have configured Active Directory, you must then configure a Subscriber (such as Cisco Firepower Management Center (FMC) or Stealthwatch), in order to define the client that is to receive the user data.

### Before you begin

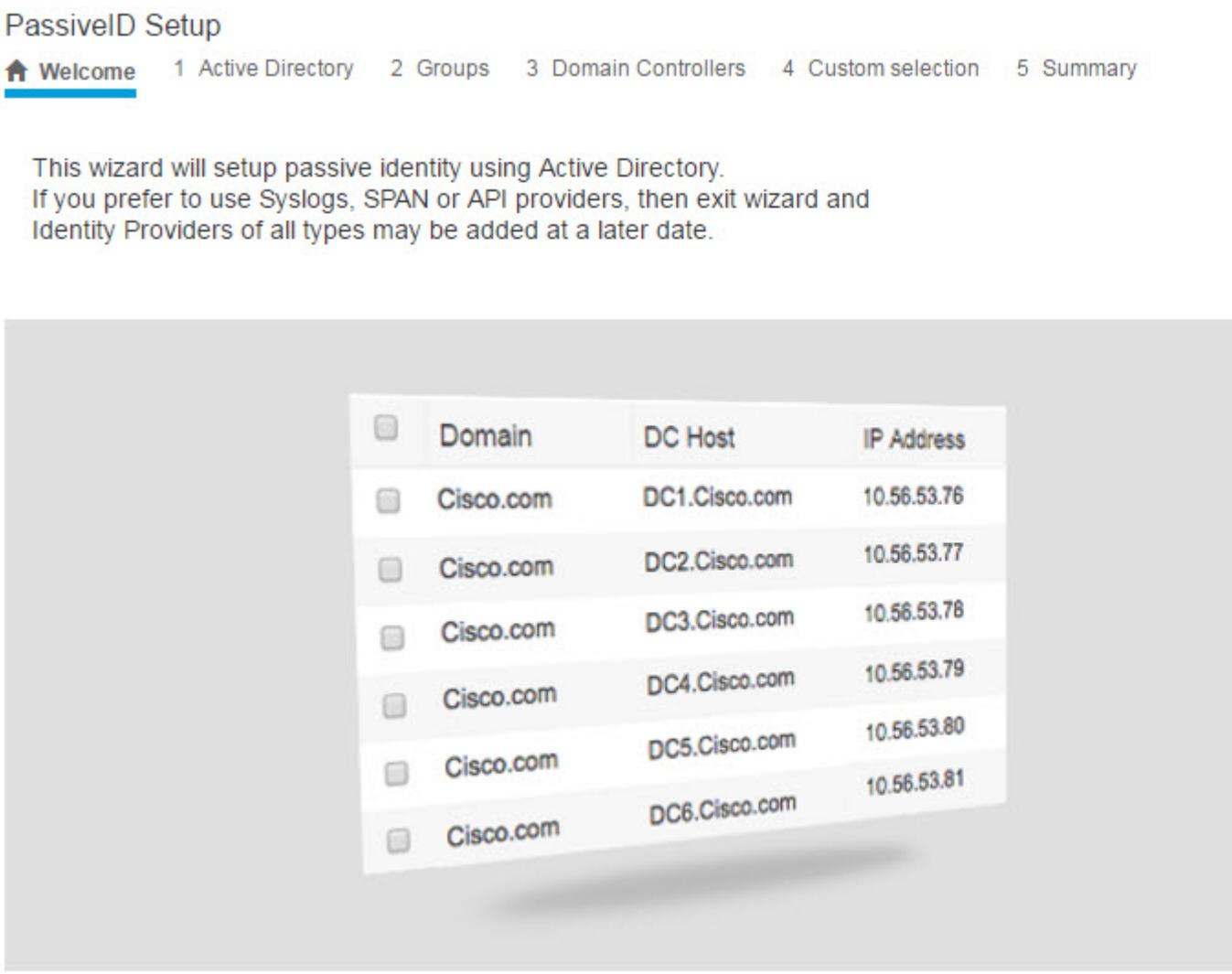
- Ensure the Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure the Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure that ISE-PIC has an entry in the domain name server (DNS). Ensure you have properly configured reverse lookup for the client machine from ISE-PIC. For more information, see DNS Server, on page 13

### Procedure

**Step 1** Choose **Home** > **Introduction**. From the Passive Identity Connector Overview screen, click **Passive Identity Wizard**.

The PassiveID Setup opens:

*Figure 2: The PassiveID Setup*




**Step 2** Click **Next** to begin the wizard.

**Step 3** Enter a unique name for this Active Directory join point. Enter the domain name for the Active Directory Domain to which this node is connected, and enter your Active Directory administrator user name and password.

Your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

**Step 4** Click **Next** to define Active Directory groups and check any user groups to be included and monitored.
The Active Directory user groups automatically appear based on the Active Directory join point you configured in the previous step.

**Step 5** Click **Next**. Select the DCs to be monitored. If you choose Custom, then from the next screen select the specific DCs for monitoring. When finished, click **Next**.

**Step 6** Click **Exit** to complete the wizard.

### What to do next

When you finish configuring Active Directory as your initial provider, you can easily configure additional provider types as well. For more information, see Providers, on page 31. Furthermore, you can now also configure a subscriber, designated to receive the user identity information that is collected by any of the providers you have defined.

# Set Up an Active Directory (WMI) Probe Step-by-Step

To configure Active Directory and WMI for Passive Identity services, use the Getting Started with the PassiveID Setup, on page 18 or follow the steps in this chapter as follows:

1. Configure the Active Directory probe. See Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point, on page 20.
2. Create a list of Active Directory Domain Controllers for the WMI-configured node (or nodes) that receives AD login events.
3. Configure the Active Directory in order for it to integrate with ISE-PIC.
4. (Optional) Manage the Active Directory Provider, on page 23.

## Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point

### Before you begin

Ensure that the Cisco ISE-PIC node can communicate with the networks where the NTP servers, DNS servers, domain controllers, and global catalog servers are located.

Join points must be created in order to work with Active Directory as well as with the Agent, Syslog, SPAN and Endpoint probes .

If you want to use IPv6 when integrating with Active Directory, then you must ensure that you have configured an IPv6 address for the relevant ISE-PIC nodes.

If you use the Google Chrome browser and have ad blocking software enabled, you must disable the ad blocker. This task contains Cisco ISE GUI elements that are affected by ad blockers. Alternatively, you can carry out this task in a Google Chrome Incognito browser.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Click **Add** and enter the domain name and identity store name from the **Active Directory Join Point Name** settings.

**Step 3** Click **Submit**.

A pop-up appears asking if you want to join the newly created join point to the domain. Click **Yes** if you want to join immediately.

If you clicked **No**, then saving the configuration saves the Active Directory domain configuration globally , but none of the Cisco ISE-PIC nodes are joined to the domain yet.

**Step 4** Check the check box next to the new Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE-PIC nodes, the node roles, and their status.

**Step 5** In case the join point was not joined to the domain during Step 3, check the check box next to the relevant Cisco ISE-PIC nodes and click **Join** to join the Cisco ISE-PIC node to the Active Directory domain.

You must do this explicitly even though you saved the configuration. To join multiple Cisco ISE-PIC nodes to a domain in a single operation, the username and password of the account to be used must be the same for all join operations. If different username and passwords are required to join each Cisco ISE-PIC node, the join operation should be performed individually for each Cisco ISE-PIC node.

**Step 6** Enter the Active Directory username and password in the **Join Domain** dialog box.

Your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

The user used for the join operation should exist in the domain itself. If it exists in a different domain or subdomain, the username should be noted in a UPN notation, such as jdoe@acme.com.

**Step 7** (Optional) Check the **Specify Organizational Unit** check box.

You should check this check box in case the Cisco ISE-PIC node machine account is to be located in a specific Organizational Unit other than CN=Computers,DC=someDomain,DC=someTLD. Cisco ISE-PIC creates the machine account under the specified organizational unit or moves it to this location if the machine account already exists. If the organizational unit is not specified, Cisco ISE-PIC uses the default location. The value should be specified in full distinguished name (DN) format. The syntax must conform to the Microsoft guidelines. Special reserved characters, such as /'+,;=<> line feed, space, and carriage return must be escaped by a backslash (\). For example, OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\, and Workstations,DC=someDomain,DC=someTLD. If the machine account is already created, you need not check this check box. You can also change the location of the machine account after you join to the Active Directory domain.

**Step 8** Click **OK**.

You can select more than one node to join to the Active Directory domain.

If the join operation is not successful, a failure message appears. Click the failure message for each node to view detailed logs for that node.

---

Note the following points while configuring the join points:

- When using multiple join points, if alternate UPN suffix is configured only for a single join point or domain, identity lookup is performed only in that join point or domain. Authentication might fail in such cases. As a workaround, you can configure the alternate UPN suffix for all the joint points or domains.
- You can only add up to 200 Domain Controllers on ISE. On exceeding the limit, you will receive the error "Error creating <*DC FQDN*> - Number of DCs Exceeds allowed maximum of 200". For more information on the tested scale limit of domain controllers for deployment, see Performance and Scalability Guide for Cisco Identity Services Engine.

- When the join is complete, Cisco ISE-PIC updates its AD groups and corresponding security identifiers (SIDs). Cisco ISE-PIC automatically starts the SID update process. You must ensure that this process is allowed to complete.
- You might not be able to join Cisco ISE-PIC with an Active Directory domain if the DNS service (SRV) records are missing (the domain controllers do not advertise their SRV records for the domain that you are trying to join to).
- We recommend that you restart the AD connector (under Administration > Identity Management > External Identity Sources > Active Directory > Advanced Tools > Advanced Tuning). This ensures that the AD cache is refreshed with the most recent updates.
- The AD machine account name that is created will not match the Cisco ISE hostname if the hostname contains more than 15 characters. In this case, the machine account name will be created in the following format:

  *first_8_characters_of(hostname) + "-" + 6 random characters + "$"*

  For the machine account name and the hostname to match, the hostname must have 15 characters or less.
- Even if the AD credentials used to join Cisco ISE and AD are no longer valid, the join point between Cisco ISE and AD remains unchanged.

## Add Domain Controllers

**Procedure**

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Check the check box next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE-PIC nodes, the node roles, and their statuses.

**Step 3** **Note**
To add a new Domain Controller (DC) for Passive Identity services, you need the login credentials of that DC.

Go to the PassiveID tab and click **Add DCs**.

**Step 4** Check the check box next to the domain controllers that you would like to add to the join point for monitoring and click **OK**.
The domain controllers appear in the Domain Controllers list of the PassiveID tab.

**Step 5** Configure the domain controller:

a) Checkmark the domain controller and click **Edit**. The **Edit Item** screen appears.
b) Optionally, edit the different domain controller fields.

The DC failover mechanism is managed based on the DC priority list, which determines the order in which the DCs are selected in case of failover. If a DC is offline or not reachable due to some error, its priority is decreased in the priority list. When the DC comes back online, its priority is adjusted accordingly (increased) in the priority list.

From Cisco ISE Release 3.4 onwards, you can choose to override Cisco ISE's internal priority list and determine the order in which the next preferred DCs are selected in case of a failover.

## Configure Active Directory User Groups

Configure Active Directory user groups for them to be available for use when working with different probes that collect user identity information from Active Directory. Internally, Cisco ISE uses security identifiers (SIDs) to help resolve group name ambiguity issues and to enhance group mappings. SID provides accurate group assignment matching.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**. Click the join point for which you would like to add groups.

**Step 2** Click the **Groups** tab.

**Step 3** Do one of the following:

a) Choose **Add** > **Select Groups From Directory** to choose an existing group.

b) Choose **Add** > **Add Group** to manually add a group. You can either provide both group name and SID or provide only the group name and press **Fetch SID**.

Do not use double quotes (”) in the group name for the user interface login.

**Step 4** If you are manually selecting a group, you can search for them using a filter. For example, enter **admin*** as the filter criteria and click **Retrieve Groups** to view user groups that begin with admin. You can also enter the asterisk (*) wildcard character to filter the results. You can retrieve only 500 groups at a time.

**Step 5** Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.

**Step 6** If you choose to manually add a group, enter a name and SID for the new group.

**Step 7** Click **OK**.

**Step 8** Click **Save**.

**Note**
If you delete a group and create a new group with the same name as original, you must click **Update SID Values** to assign new SID to the newly created group. After an upgrade, the SIDs are automatically updated after the first join.

# Manage the Active Directory Provider

Once you have created and configured your Active Directory join points, continue to manage the Active Directory probe with these tasks:


- Test Users for Active Directory Groups, on page 24
- View Active Directory Joins for a Node, on page 24
- Diagnose Active Directory Problems, on page 25
- Leave the Active Directory Domain, on page 25
- Delete Active Directory Configurations, on page 26
- Enable Active Directory Debug Logs, on page 27

## Test Users for Active Directory Groups

The Test User tool can be used to verify user groups from Active Directory. You can run the test for a single join point or for scopes.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Choose one of the following options:

- To run the test on all join points, choose **Advanced Tools** > **Test User for All Join Points**.
- To run the test for a specific join point, select the joint point and click **Edit**. Select the Cisco ISE-PIC node and click **Test User**.

**Step 3** Enter the username and password of the user (or host) in Active Directory.

**Step 4** Choose the authentication type. Password entry in Step 3 is not required if you choose the Lookup option.

**Step 5** Select the Cisco ISE-PIC node on which you want to run this test, if you are running this test for all join points.

**Step 6** Check the Retrieve Groups and Attributes check boxes to retrieve the groups from Active Directory.

**Step 7** Click **Test**.
The result and steps of the test operation are displayed. The steps can help to identify the failure reason and troubleshoot.

You can also view the time taken (in milliseconds) for Active Directory to perform each processing step. Cisco ISE-PIC displays a warning message if the time taken for an operation exceeds the threshold.

## View Active Directory Joins for a Node

You can use the **Node View** button on the **Active Directory** page to view the status of all Active Directory join points for a given Cisco ISE-PIC node or a list of all join points on all Cisco ISE-PIC nodes.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Click **Node View**.

**Step 3** Select a node from the **ISE Node** drop-down list.
The table lists the status of Active Directory by node. If there are multiple join points and multiple Cisco ISE-PIC nodes in a deployment, this table may take several minutes to update.

**Step 4** Click the join point **Name** link to go to that Active Directory join point page and perform other specific actions.

**Step 5** Click the link in the **Diagnostic Summary** column to go to the **Diagnostic Tools** page to troubleshoot specific issues.
The diagnostic tool displays the latest diagnostics results for each join point per node.

## Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every Cisco ISE-PIC node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when Cisco ISE-PIC uses Active Directory.

There are multiple reasons for which Cisco ISE-PIC might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting Cisco ISE-PIC to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Click the **Advanced Tools** drop-down and choose **Diagnostic Tools**.

**Step 3** Select a Cisco ISE-PIC node to run the diagnosis on.

If you do not select a Cisco ISE-PIC node then the test is run on all the nodes.

**Step 4** Select a specific Active Directory join point.

If you do not select an Active Directory join point then the test is run on all the join points.

**Step 5** You can run the diagnostic tests either on demand or on a scheduled basis.

- To run tests immediately, choose **Run Tests Now**.
- To run the tests at an scheduled interval, check the **Run Scheduled Tests** check box and specify the start time and the interval (in hours, days, or weeks) at which the tests must be run. When this option is enabled, all the diagnostic tests are run on all the nodes and instances and the failures are reported in the **Alarms** dashlet in the **Home** dashboard.

**Step 6** Click **View Test Details** to view the details for tests with Warning or Failed status.
This table allows you to rerun specific tests, stop running tests, and view a report of specific tests.

## Leave the Active Directory Domain

If you no longer need to use this Active Directory domain or this join point to collect user identities, you can leave the Active Directory domain.

When you reset the Cisco ISE-PIC application configuration from the command-line interface or restore configuration after a backup or upgrade, it performs a leave operation, disconnecting the Cisco ISE-PIC node from the Active Directory domain, if it is already joined. However, the Cisco ISE-PIC node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Admin portal with the Active Directory credentials because it also removes the node account from the Active Directory domain. This is also recommended when you change the Cisco ISE-PIC hostname.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Check the checkbox next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE-PIC nodes, the node roles, and their statuses.

**Step 3** Check the checkbox next to the Cisco ISE-PIC node and click **Leave**.

**Step 4** Enter the Active Directory username and password, and click **OK** to leave the domain and remove the machine account from the Cisco ISE-PIC database.

If you enter the Active Directory credentials, the Cisco ISE-PIC node leaves the Active Directory domain and deletes the Cisco ISE-PIC machine account from the Active Directory database.

**Note**
To delete the Cisco ISE-PIC machine account from the Active Directory database, the Active Directory credentials that you provide here must have the permission to remove machine account from domain.

**Step 5** If you do not have the Active Directory credentials, check the **No Credentials Available** checkbox, and click **OK**.

If you check the **Leave domain without credentials** checkbox, the primary Cisco ISE-PIC node leaves the Active Directory domain. The Active Directory administrator must manually remove the machine account that was created in Active Directory during the time of the join.

## Delete Active Directory Configurations

You should delete Active Directory configurations if you are not going to use the specific Active Directory configuration as a probe. Do not delete the configuration if you want to join another Active Directory domain. You can leave the domain to which you are currently joined and join a new domain. Do not delete the configuration if it is the only configuration in ISE-PIC

### Before you begin

Ensure that you have left the Active Directory domain.

### Procedure

**Step 1** Choose **Providers** > **Active Directory**.

**Step 2** Check the checkbox next to the configured Active Directory.

**Step 3** Check and ensure that the Local Node status is listed as Not Joined.

**Step 4** Click **Delete**.

You have removed the configuration from the Active Directory database. If you want to use Active Directory at a later point in time, you can resubmit a valid Active Directory configuration.

## Enable Active Directory Debug Logs

Active Directory debug logs are not logged by default. Enabling Active Directory debug logs may affect ISE-PIC performance.

### Procedure

**Step 1** Choose **Administration** > **Logging** > **Debug Log Configuration**.

**Step 2** Click the radio button next to the Cisco ISE-PIC node from which you want to obtain Active Directory debug information, and click **Edit**.

**Step 3** Click the **Active Directory** radio button, and click **Edit**.

**Step 4** Choose **DEBUG** from the drop-down list next to Active Directory. This will include errors, warnings, and verbose logs. To get full logs, choose **TRACE**.

**Step 5** Click **Save**.

# Active Directory Settings

Active Directory (AD) is a highly secure and precise source from which to receive user information, including user name and IP address.

To create and manage Active Directory probes by creating and editing join points, choose **Providers** > **Active Directory**.

For more information, see Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point, on page 20.

Choose **Providers** > **Active Directory** and then check the join point you wish to edit and click **Edit**. For the Join Domain screen, choose **Providers** > **Active Directory**, check the join point you wish to edit and click **Join**.

*Table 3: Active Directory Join Point Name Settings and Join Domain Window*

| Field Name | Description |
|---|---|
| **Join Point Name** | A unique name that distinguishes this configured join point quickly and easily. |
| **Active Directory Domain** | The domain name for the Active Directory Domain to which this node is connected. |
| **Domain Administrator** | This is the user principal name or the user account name for the Active Directory user with administrator priveleges. |
| **Password** | This is the domain administrator's password as configured in Active Directory. |
| **Specifiy Organizational Unit** | Enter the administrator's organizational unit information |

| Field Name | Description |
|---|---|
| **Store Credentials** | Your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.<br>For the Endpoint probe, you must choose **Store credentials**. |

Choose **Providers** > **Active Directory**.

***Table 4: Active Directory Join/Leave Window***

| Field Name | Description |
|---|---|
| **ISE Node** | The URL for the specific node in the installation. |
| **ISE Node Role** | Indicates whether the node is the Primary or Secondary node in the installation. |
| **Status** | Indicates whether the node is actively joined to the Active Directory domain. |
| **Domain Controller** | For nodes that are joined to Active Directory, this column indicates the specific Domain Controller to which the node is connected in the Active Directory Domain. |
| **Site** | Only relevant for a full ISE installation. For more information, see Upgrading ISE-PIC to a Full ISE Installation, on page 132. |

***Table 5: Passive ID Domain Controllers (DC) List***

| Field | Description |
|---|---|
| **Domain** | The fully qualified domain name of the server on which the domain controller is located. |
| **DC Host** | The host on which the domain controller is located. |
| **Site** | Only relevant for a full ISE installation. For more information, see Upgrading ISE-PIC to a Full ISE Installation, on page 132. |
| **IP Address** | The IP address of the domain controller. |
| **Monitor Using** | Monitor Active Directory domain controllers for user identity information by one of these methods:<br>• WMI: Monitor Active Directory directly with the WMI infrastructure.<br>• Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 34. |

***Table 6: Passive ID Domain Controllers (DC) Edit Window***

| Field Name | Description |
|---|---|
| **Host FQDN** | Enter the fully qualified domain name of the server on which the domain controller is located. |

| Field Name | Description |
|---|---|
| **Description** | Enter a unique description for this domain controller in order to easily identiy it. |
| **User Name** | The administrator's user name for accessing Active Directory. |
| **Password** | The administrator's password for accessing Active Directory. |
| **Protocol** | Monitor Active Directory domain controllers for user identity information by one of these methods:<br>• WMI: Monitor Active Directory directly with the WMI infrastructure.<br>• Agent name: If you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 34. |

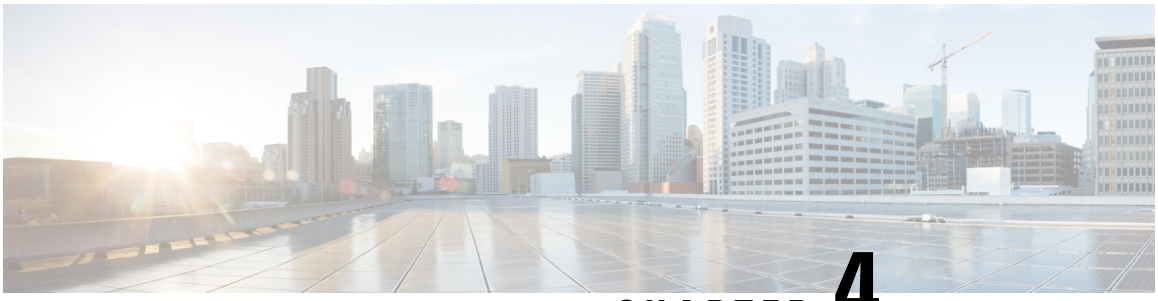
Active Directory groups are defined and managed from Active Directory and the groups for the Active Directory that is joined to this node can be viewed from this tab. For more information about Active Directory, see https://msdn.microsoft.com/en-us/library/bb742437.aspx.

Choose **Providers** > **Active Directory** > **Advanced Settings**.

***Table 7: Active Directory Advanced Settings***

| Field Name | Description |
|---|---|
| **History interval** | The time during which the Passive Identity service reads user login information that already occurred. This is required upon startup or restart of the Passive Identity service to catch up with events generated while it was unavailable. When the Endpoint probe is active, it maintains the frequency of this interval. |
| **User session aging time** | The amount of time the user can be logged in. The Passive Identity service identifies new user login events from the DC, however the DC does not report when the user logs off. The aging time enables ISE-PIC to determine the time interval for which the user is logged in. |
| **NTLM Protocol settings** | You can select either NTLMv1 or NTLMv2 as the communications protocol between ISE-PIC and the DC. NTLMv2 is the recommended default. |

| Field Name | Description |
|---|---|
| **Authorization Flow** | Check this check box to configure authorization policies for PassiveID login users.<br><br>You can configure an authorization policy to assign an SGT to a user based on the Active Directory group membership. This allows you to create TrustSec policy rules even for PassiveID authorization.<br><br>You can use the **PassiveID_Provider**, **PassiveID_Username**, or **PassiveID_Groups** attribute in the **PassiveID** dictionary to create the authorization rules for PassiveID login users. The following values can be set for the **PassiveID_Provider** attribute:<br><br>• **API**<br>• **Agent**<br>• **SPAN**<br>• **Syslog**<br>• **WMI**<br>• **Other**<br><br>The IP-SGT mapping and Active Directory group details of PassiveID login users are included in the session topic. These details can be published through pxGrid, pxGrid Cloud, or SXP.<br><br>You can view the authorization policy status and the SGT details in the **RADIUS Live Logs** window (**Operations > RADIUS > Live Logs**) and the **RADIUS Live Sessions** window (**Operations > RADIUS > Live Sessions**).<br><br>**Note**<br>• Ensure that the PassiveID, pxGrid, pxGrid Cloud, and SXP services are enabled on the node. To enable these services, choose **Administration > System > Deployment**.<br>• You must enable the **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** option in the **SXP Settings** window (**Work Centers > TrustSec > Settings > SXP Settings**) to include PassiveID mappings in the SXP mappings.<br>• SGT details of the PassiveID login users that are authenticated using API provider cannot be published using SXP. However, the SGT details of these users can be published through pxGrid and pxGrid Cloud. |



CHAPTER 4

# Providers

In order to enable ISE-PIC to provide identity information to consumers that subscribe to the service (subscribers), you must first configure an ISE-PIC probe, which connects to the identity provider.

The table below provides details about all of the provider and probe types available from ISE-PIC. For more information about Active Directory, see Active Directory as a Probe and a Provider, on page 17.

You can define these provider types:

*Table 8: Provider Types*

| Provider Type (Probe) | Description | Source System (Provider) | Technology | User Identity Information Collected | Document Link |
|---|---|---|---|---|---|
| Active Directory (AD) | A highly secure and precise source, as well as the most common, from which to receive user information.<br>As a probe, AD works with WMI technology to deliver authenticated user identities.<br>In addition, AD itself, rather than the probe, functions as a source system (a provider) from which other probes retrieve user data as well. | Active Directory Domain Controller | WMI | • User name<br>• IP address<br>• Domain | Active Directory as a Probe and a Provider, on page 17 |
| Agents | A native 32-bit application installed on Active Directory domain controllers or on member servers. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. | | Agents installed on the domain controller or on a member server. | • User name<br>• IP address<br>• Domain | Active Directory Agents, on page 34 |
| Endpoint | | | WMI | Whether the user is still connected | Endpoint Probe, on page 67 |

| Provider Type (Probe) | Description | Source System (Provider) | Technology | User Identity Information Collected | Document Link |
|---|---|---|---|---|---|
| | Always runs in the background in addition to other configured probes, in order to verify whether the user is still connected. | | | | |
| SPAN | Sits on the network switch in order to listen to network traffic, and extract user identity information based on Active Directory data. | | SPAN, installed on the switch, and Kerberos messages | • User name<br>• IP address<br>• Domain | SPAN, on page 43 |
| API providers | Gather user identity information from any system programmed to communicate with a RESTful API client, using the RESTful API service offered by ISE-PIC. | Any system programmed to communicate with a REST API client. | RESTful APIs. User identity sent to subscribers in JSON format. | • User name<br>• IP address<br>• Port range<br>• Domain | API Providers, on page 38 |
| Syslog | Parse syslog messages and retrieve user identities, including MAC addresses. | • Regular syslog message providers<br>• DHCP servers | Syslog messages | • User name<br>• IP address<br>• MAC address<br>• Domain | Syslog Providers, on page 44 |

**Note** pxGrid sends 200 events per second for session topics to avoid overloading the clients. If the publisher sends more than 200 events, the additional events are queued and sent in next batch.

If pxGrid consistently receives more than 200 events per second for a prolonged period of time, it might consume more memory than usual for storing the backlog events. This might affect the performance of pxGrid.

- Active Directory Agents, on page 34
- API Providers, on page 38
- SPAN, on page 43
- Syslog Providers, on page 44
- Filter Passive Identity Services, on page 66
- Endpoint Probe, on page 67
- Generate pxGrid Certificates for Subscribers, on page 68
- Enable Subscribers, on page 70
- View Subscriber Events from Live Logs, on page 70
- Configure Subscriber Settings, on page 70


# Active Directory Agents

From ISE-PIC install the native 32-bit application, Domain Controller (DC) agents, anywhere on the Active Directory (AD) domain controller (DC) or on a member server (based on your configurations) to retrieve user identity information from AD and then send those identities to the subscribers you have configured. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. Agents can be installed on a separate domain, or on the AD domain, and once installed, they provide status updates to ISE-PIC once every minute.

The agents can be either automatically installed and configured by ISE-PIC , or you can manually install them. Upon installation, the following occurs:

- The agent and its associated files are installed at the following path: **`Program Files/Cisco/Cisco ISE PassiveID Agent`**
- A config file called **`PICAgent.exe.config`** is installed indicating the logging level for the agent. You can manually change the logging level from within the config file.
- The CiscoISEPICAgent.log file is stored with all logging messages.
- The nodes.txt file contains the list of all nodes in the deployment with which the agent can communicate. The agent contacts the first node in the list. If that node cannot be contacted, the agent continues to attempt communication according to the order of the nodes in the list. For manual installations, you must open the file and enter the node IP addresses. Once installed (manually or automatically), you can only change this file by manually updating it. Open the file and add, change or delete node IP addresses as necessary.
- The Cisco ISE PassiveID Agent service runs on the machine, which you can manage from the Windows Services dialog box.
- The Active Directory agents are only supported on Windows Server 2008 and higher. If you cannot install agents, then use the Active Directory probe for passive identity services. For more information, see Active Directory as a Probe and a Provider, on page 17.

**Note**

- Even if you are running the AD agent on a member server, it still queries the Active Directory for the login requests.
- Usernames ending with special characters, specifically the dollar sign ($), are classified as machine login requests and these sessions are not forwarded to the session directory. All other sessions, regardless of the location of special characters in the usernames, are forwarded to the session directory and included in the **Live Sessions** page.

# Automatically Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE-PIC , or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to enable automatic installation and configure the agent to monitor a domain controller.

### Before you begin

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE-PIC, see DNS Server, on page 13
- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 17.

  Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 23.

### Procedure

**Step 1** Choose **Providers** > **Agents**.

**Step 2** To add a new agent, click **Add** from the top of the table.

**Step 3** To create the new agent and automatically install it on the host that you indicate in this configuration, select **Deploy New Agent**.

**Step 4** Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 37.

**Step 5** Click **Deploy**.
The agent is automatically installed on the host according to the domain that you indicated in the configuration, and the settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

**Step 6** Choose **Providers** > **Active Directory** to view all currently configured join points.

**Step 7** Click the link for the join point from which you would like to enable the agent you created.

**Step 8** Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

**Step 9** Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

**Step 10** From the **Protocol** drop-down list, select **Agent**

**Step 11** Select the agent you created from the **Agent** drop-down list. Enter the user name and password credentials of the agent that you created, and click **Save**.

The user name and password credentials are used to install the agent on the domain controller. Finally, when you click on **Deploy**, the *picagent.exe* is copied from */opt/pbis/bin* to the specified Windows machine.

# Manually Install and Deploy Active Directory Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE-PIC , or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to manually install and configure the agent to monitor a domain controller.

### Before you begin

- Configure reverse lookup for the relevant DNS servers from the server side. For more information about the DNS server configuration requirements for ISE-PIC, see DNS Server, on page 13
- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 17.

  Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 23.

### Procedure

**Step 1** Choose **Providers** > **Agents**.

**Step 2** Click **Download Agent** to download the `picagent-installer.zip` file for manual installation.
The file is downloaded to your standard Windows Download folder.

**Step 3** Place the zip file on the designated host machine and run the installation.

**Step 4** From the ISE-PIC GUI, again choose **Providers** > **Agents**.

**Step 5** To configure a new agent, click **Add** from the top of the table.

**Step 6** To configure the agent that you have already installed on the host machine, select **Register Existing Agent**.

**Step 7** Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory Agent Settings, on page 37.

**Step 8** Click **Save**.
The agent settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

**Step 9** Choose **Providers** > **Active Directory** to view all currently configured join points.

**Step 10** Click the link for the join point from which you would like to enable the agent you created.

**Step 11** Choose the **Passive ID** tab to configure the domain controllers that you added as part of the prerequisites.

**Step 12** Select the domain controller that you would like to monitor with the agent you created and click **Edit**.

**Step 13** From the **Protocol** drop-down list, select **Agent**.

**Step 14** Select the agent you created from the **Agent** drop-down list. Enter the user name and password to connect to the agent, and click **Save**

The user account must have the necessary permissions to read security events. A user account for a WMI-based agent must have WMI/DCOM permissions.

# Uninstall the Agent

Agents, installed automatically or manually, can be easily (manually) uninstalled directly from Windows.

**Procedure**

**Step 1** From the Windows dialog, go to **Programs and Features**.

**Step 2** Find and select the Cisco ISE PassiveID Agent in the list of installed programs.

**Step 3** Click **Uninstall**.

# Active Directory Agent Settings

Allow ISE-PIC to automatically install agents on a specified host in the network in order to retrieve user identity information from different Domain Controllers (DC) and deliver that information to ISE-PIC subscribers.

To create and manage agents, choose **Providers** > **Agents**. See Automatically Install and Deploy Active Directory Agents, on page 35.

***Table 9: Agents Window***

| Field Name | Description |
|---|---|
| **Name** | The agent name as you configured it. |
| **Host** | The fully qualified domain name of the host on which the agent is installed. |
| **Monitoring** | This is a comma separated list of domain controllers that the specified agent is monitoring. |

*Table 10: Agents New*

| Field | Description |
|---|---|
| **Deploy New Agent or Register Existing Agent** | • Deploy New Agent: Install a new agent on the specified host.<br>**Note**<br>The user must have Domain User and Domain Admin privileges to deploy an agent on the specified host.<br>• Register Existing Agent: Manually install the agent on the host and then configure that agent from this screen for ISE-PIC to enable the service. |
| **Name** | Enter a name by which you can easily recognize the agent. |
| **Description** | Enter a description by which you can easily recognize the agent. |
| **Host FQDN** | This is the fully qualified domain name for the host on which the agent is installed (register existing agent), or is to be installed (automatic deployment). |
| **User Name** | Enter your user name in order to access the host on which to install the agent. ISE-PIC uses these credentials in order to install the agent for you.<br>The user account must have permissions to connect remotely and install the PIC agent. |
| **Password** | Enter your user password in order to access the host on which to install the agent. ISE-PIC uses these credentials in order to install the agent for you. |

# API Providers

The API Providers feature in Cisco ISE-PIC enables you to push user identity information from your customized program or from the terminal server (TS)-Agent to the built-in ISE-PIC REST API service. In this way, you can customize a programmable client from your network to send user identities that were collected from any network access control (NAC) system to the service. Furthermore, the Cisco ISE-PIC API provider enables you to interface with network applications such as the TS-Agent on a Citrix server, where all users have the same IP address but are assigned unique ports.

For example, an agent running on a Citrix server that provides identity mappings for users authenticated against an Active Directory (AD) server can send REST requests to ISE-PIC to add or delete a user session whenever a new user logs in or off. ISE-PIC then takes the user identity information, including the IP address and assigned ports, delivered from the client and sends it to pre-configured subscribers, such as the Cisco Firepower Management Center (FMC).

The ISE-PIC REST API framework implements the REST service over the HTTPS protocol (no client certificate validation necessary) and the user identity information is delivered in JSON (JavaScript Object Notation) format. For more information about JSON, see http://www.json.org/.

The ISE-PIC REST API service parses user identities and in addition, maps that information to port ranges, in order to distinguish between the different users logged in simultaneously to one system. Everytime a port is allocated to a user, the API sends a message to ISE-PIC.

### The REST API Provider Flow

After you have configured a bridge to your customized client from ISE-PIC by declaring that client as a Provider for ISE-PIC and enabling that specific customized program (the client) to send RESTful requests, the ISE-PIC REST service works in the following way:

1. For client authentication, Cisco ISE-PIC requires an authentication token. A customized program on the client machine sends a request for an authentication token when initiating contact and then every time ISE-PIC notifies that the previous token has expired. The token is returned in response to the request, enabling ongoing communication between the client, and the ISE-PIC service.
2. After a user has logged into the network, the client retrieves user identity information and posts that information to the ISE-PIC REST service using the API Add command.
3. Cisco ISE-PIC receives and maps the user identity information.
4. Cisco ISE-PIC sends the mapped user identity information to the subscriber.
5. Whenever necessary, the customized machine can send a request to remove user information by sending a Remove API call and including the user ID received as the response when the Add call was sent.

### Work with REST API Providers in ISE-PIC

Follow these steps to activate the REST service in ISE-PIC:

1. Configure the client side. For more information, see the client user documentation.
2. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE-PIC. For more information about the DNS server configuration requirementsISE-PIC, see DNS Server, on page 13
3. See Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services, on page 39.



**Note** To configure the API Provider to work with a TS-Agent add the TS-Agent information when creating a bridge from ISE-PIC to that agent, and then consult with the TS-Agent documentation for information about sending API calls.

4. Generate an authentication token and send add and remove requests to the API service.

# Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services

In order to enable the ISE-PIC REST API service to receive information from a specific client, you must first define the specific client from Cisco ISE-PIC. You can define multiple REST API clients with different IP addresses.

### Before you begin

- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from Cisco ISE-PIC. For more information about the DNS server configuration requirements for Cisco ISE-PIC, see DNS Server, on page 13

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Providers** > **API Providers** to view all currently configured clients, to edit and delete existing clients, and to configure new clients..
The API Providers table is displayed, including status information for each existing client.

**Step 2** To add a new client, click **Add** from the top of the table.

**Step 3** Complete all mandatory fields in order to configure the client correctly. For more information, see API Provider Settings, on page 40.

**Step 4** Click **Submit**.
The client configuration is saved and the screen displays the updated API Providers table. The client can now send posts to the ISE-PIC REST service.

### What to do next

Set up your customized client to post authentication tokens and user identities to the ISE-PIC REST service. See Send API Calls to the ISE-PIC REST Service, on page 40.

# Send API Calls to the ISE-PIC REST Service

### Before you begin

Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services, on page 39

### Procedure

**Step 1** Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*)

**Step 2** Enter the username and password that you specified and configured from the **API Providers** window. For more information, see Configure a Bridge to the ISE-PIC REST Service for Passive Identity Services, on page 39.

**Step 3** Press **Enter**.

**Step 4** Enter the API call in the URL Address field of the target node.

**Step 5** Click **Send** to issue the API call.

### What to do next

See API Calls, on page 41 for more information and details about the different API calls, their schemas and their results.

# API Provider Settings

In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Providers** > **API Providers** to configure a new REST API client for Passive Identity services.

**Note** The full API definition and object schemas can be retrieved with a request call as follows:

- For the full API specifications (wadl)—https://YOUR_ISE:9094/application.wadl
- For the API model and object schemas—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

*Table 11: API Providers Settings*

| Field | Description |
|---|---|
| Name | Enter a unique name for this client that distinguishes it quickly and easily from other clients. |
| Description | Enter a clear description of this client. |
| Status | Select **Enabled** to enable the client to interact with the REST services immediately upon completing configuration. |
| Host/ IP | Enter the IP address for the client host machine. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE-PIC. |
| User name | Create a unique user name to be used when posting to the REST service. |
| Password | Create a unique password to be used when posting to the REST service. |

# API Calls

Use these API calls to manage user identity events for Passive Identity services with Cisco ISE-PIC.

### Purpose: Generate Authentication Token

- **Request**

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  The request should contain the BasicAuth authorization header. Provide the API provider's credentials as previously created from the ISE-PIC GUI. For more information see API Provider Settings, on page 40.

- **Response Header**

  The header includes the X-auth-access-token. This is the token to be used when posting additional REST requests.

- **Response Body**

  HTTP 204 No Content

### Purpose: Add User

- **Request**

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

  Add X-auth-access-token in the header of the POST request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

  201 Created

- **Response Body**

  {

  "user": "<username>",

  "srcPatRange": {

  "userPatStart": <user PAT start value>,

  "userPatEnd": <user PAT end value>,

  "patRangeStart": <PAT range start value>

  },

  "srcIpAddress": "<src IP address>",

  "agentInfo": "<Agent name>",

  "timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<domain>"

  }

- **Notes**

  - srcPatRange can be removed in above json to create a single IP user binding.
  - Response body contains the "ID" which is the unique identifier for the user session binding created. Use this ID when sending a DELETE request to indicate which user should be removed.
  - This reponse also contains the self link which is the URL for this newly created user session binding.

### Purpose: Remove User

- **Request**

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  In <id> enter the ID as was received from the Add response.

  Add the X-auth-access-token in the header of the DELETE request, for example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- **Response Header**

200 OK

- **Response Body**

  Response body contains the details about the user session binding which got deleted.

# SPAN

SPAN allows you to quickly and easily enable Cisco ISE-PIC to listen to the network and retrieve user information without having to configure Active Directory to work directly with Cisco ISE-PIC. SPAN sniffs network traffic, specifically examining Kerberos messages, extracts user identity information also stored by Active Directory and sends that information to ISE-PIC. ISE-PIC then parses the information, ultimately delivering user name, IP address and domain name to the subscribers that you have also already configured from ISE-PIC.

In order for SPAN to listen to the network and extract Active Directory user information, ISE-PIC and Active Directory must both be connected to the same switch on the network. In this way, SPAN can copy and mirror all user identity data from Active Directory.

With SPAN, user information is retrieved in the following way:

1. The user endpoint logs in to the network.
2. Log in and user data are stored in Kerberos messages.
3. When the user logs in and the user data passes through the switch, SPAN mirrors the network data.
4. Cisco ISE-PIC listens to the network for user information and retrieves the mirrored data from the switch.
5. Cisco ISE-PIC parses the user information and updates passive ID mappings.
6. Cisco ISE-PIC delivers the parsed user information to the subscribers.

## Working with SPAN

### Before you begin

In order to enable ISE-PIC to receive SPAN traffic from a network switch, you must first define which nodes and node interfaces are to listen to the switch. You can configure SPAN in order to listen to the different installed ISE-PIC nodes. For each node, only one interface can be configured to listen to the network and the interface used to listen must be dedicated to SPAN only.

In addition, you must:

- Ensure Active Directory is configured on your network.
- Run a CLI on the switch in the network that is also connected to Active Directory in order to ensure the switch can communicate with ISE-PIC.
- Configure the switch to mirror the network from AD.
- Configure a dedicated ISE-PIC network interface card (NIC) for SPAN. This NIC is used only for SPAN traffic.
- Ensure the NIC that you have dedicated to SPAN is activated via the command line interface.

- Create a VACL that sends only Kerberos traffic into the SPAN port.

### Procedure

**Step 1** Choose **Providers** > **SPAN** to configure SPAN.

**Step 2** **Note**
We recommend that the GigabitEthernet0 network interface card (NIC) remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Enter a meaningful description (optional), select status **Enabled**, and choose the nodes and the relevant NICs that will be used to listen to the network switch. For more information, see SPAN Settings, on page 44.

**Step 3** Click **Save**.
The SPAN configuration is saved and ISE-PIC is now actively listening to network traffic.

# SPAN Settings

From each node that you have deployed, quickly and easily configure ISE-PIC to receive user identities by installing SPAN on a client network.

***Table 12: SPAN Settings***

| Field | Description |
|---|---|
| **Description** | Enter a unique description to remind you of which nodes and interfaces are currently enabled. |
| **Status** | Select **Enabled** to enable the client immediately upon completing configuration. |
| **Interface NIC** | Select one or both of the nodes installed for ISE-PIC, and then for each selected node, choose the node interface that is to listen to the network for information.<br>**Note**<br>We recommend that the GigabitEthernet0 NIC remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes. |

# Syslog Providers

ISE-PIC parses syslog messages from any client (identity data provider) that delivers syslog messages, including regular syslog messages (from providers such as InfoBlox, Blue Coat, BlueCat, and Lucent) as well as DHCP syslog messages, and sends back user identity information, including MAC addresses. This mapped user identity data is then delivered to subscribers.

You can specify the syslog clients from which to receive the user identity data (see Configure Syslog Clients, on page 45). While configuring the provider, you must specify the connection method (TCP or UDP) and the syslog template to be used for parsing.

**Note** When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, ISE-PIC attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in ISE-PIC. To view this list, choose **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to guarantee parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 50.

The syslog probe sends syslog messages that are received to the ISE-PIC parser, which maps the user identity information, and publishes that information to ISE-PIC. ISE-PIC then delivers the parsed and mapped user identity information to ISE-PIC subscribers.

**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE-PIC can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, the message is not parsed and user identity is not delivered.

To parse syslog messages for user identity from ISE-PIC :

- Configure syslog clients from which to receive user identity data. See Configure Syslog Clients, on page 45.
- Customize a single message header. See Customize Syslog Headers, on page 50.
- Customize message bodies by creating templates. See Customize the Syslog Message Body, on page 50.
- Use the message templates pre-defined in ISE-PIC when configuring your syslog client as the message template used for parsing, or base your customized header or body templates on these pre-defined templates. See Work with Syslog Predefined Message Templates, on page 54.

# Configure Syslog Clients

In order to enable Cisco ISE-PIC to listen to syslog messages from a specific client, you must first define the specific client from Cisco ISE-PIC. You can define multiple providers with different IP addresses.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Providers** > **Syslog Providers** to view all currently configured clients, to edit and delete existing clients, and to configure new clients.
The Syslog Providers table is displayed, including status information for each existing client.

**Step 2** To configure a new syslog client, click **Add** from the top of the table.

**Step 3** Complete all mandatory fields (see Syslog Settings, on page 46 for more details) and create a message template if necessary (see Customize the Syslog Message Body, on page 50 for more details) to configure the client correctly.

**Step 4** Click **Submit**.

## Syslog Settings

Configure Cisco ISE-PIC to receive user identities, including MAC addresses, by way of syslog messages from a specific client. You can define multiple providers with different IP addresses.

***Table 13: Syslog Providers***

| Field Name | Description |
|---|---|
| **Name** | Enter a unique name that distinguishes this configured client quickly and easily. |
| **Description** | A meaningful description of this Syslog provider. |
| **Status** | Select **Enabled** to enable the client immediately upon completing configuration. |
| **Host** | Enter the FQDN of the host machine. |
| **Connection Type** | Enter UDP or TCP to indicate the channel by which ISE-PIC listens for syslog messages.<br>**Note**<br>When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, then Cisco ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in Cisco ISE.<br>To view this list, choose **Providers** > **Syslog Providers**. We recommend that you check the message headers and customize if necessary to ensure that parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 50. |

| Field Name | Description |
| --- | --- |
| Template | |

| Field Name | Description |
|---|---|
| | A template indicates precise body message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered.<br><br>For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received.<br><br>From this field, indicate the template (for the body of the syslog message) to be used in order to recognize and correctly parse the syslog message.<br><br>Choose either from the pre-defined dropdown list, or click **New** to create your own customized template. For more information about creating new templates, see Customize the Syslog Message Body, on page 50. Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions.<br><br>**Note**<br>Only customized templates can be edited or removed, while pre-defined system templates in the dropdown cannot be altered.<br><br>ISE-PIC currently offers these pre-defined DHCP provider templates:<br>• InfoBlox<br>• BlueCat<br>• Lucent_QIP<br>• DHCPD<br>• MSAD DHCP<br><br>**Note**<br>DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information.<br><br>If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.<br><br>Cisco ISE offers these pre-defined regular syslog provider templates:<br>• ISE<br>• ACS<br>• F5_VPN<br>• ASA_VPN<br>• Blue Coat<br>• Aerohive<br>• Safe connect_NAC |

| Field Name | Description |
|---|---|
| | • Nortel_VPN<br><br>For information about templates, see Work with Syslog Predefined Message Templates, on page 54. |
| **Default Domain** | If the domain is not identified in the syslog message for the specific user, this default domain is automatically assigned to the user in order to ensure that all users are assigned a domain.<br><br>With the default domain or with the domain that was parsed from the message, the user name is appended to username@domain, thereby including that domain, in order to get more information about the user and user groups. |

# Customize Syslog Message Structures (Templates)

A template indicates precise message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. Templates determine the supported structures for both new and remove mapping messages.

Cisco ISE-PIC enables you to customize a single message header and multiple body structures, to be used by the ISE-PIC parser.

The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the ISE-PIC parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

When customizing your message templates, you can choose to base your customization on the message templates pre-defined in ISE-PIC by consulting with the regular expressions and message structures used within those pre-defined options. For more information about the pre-defined template regular expressions, message structures, examples and more, see Work with Syslog Predefined Message Templates, on page 54.

You can customize:

- A single message header—Customize Syslog Headers, on page 50
- Multiple message bodies—Customize the Syslog Message Body, on page 50.



**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

# Customize the Syslog Message Body

Cisco ISE-PIC enables you to customize your own syslog message templates (by customizing the message body) to be parsed by the ISE-PIC parser. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain.

**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that Cisco ISE can first check users registered in the local session directory (displayed from Live Sessionss) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Create and edit syslog message body templates from within the syslog client configuration screen.

**Note** You can only edit your own customized templates. Pre-defined templates offered by the system cannot be changed.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Providers** > **Syslog Providers** to view all currently configured clients, to edit and delete existing clients, and to configure new clients.
The Syslog Providers table is displayed, including status information for each existing client.

**Step 2** Click **Add** to add a new syslog client or **Edit** to update an already configured client. For more information about configuring and updating syslog clients, see Configure Syslog Clients, on page 45.

**Step 3** In the **Syslog Providers** window, click **New** to create a new message template. To edit an existing template, select the template from the dropdown list and click **Edit**.

**Step 4** Complete all mandatory fields.

For information about how to enter the values correctly, see Syslog Customized Template Settings and Examples, on page 52.

**Step 5** Click **Test** to ensure the message is correctly parsed based on the strings you have entered.

**Step 6** Click **Save**.

# Customize Syslog Headers

Syslog headers also contain the host name from which the message originated. If your syslog messages are not recognized by the Cisco ISE-PIC message parser, you may need to customize the message header by configuring the delimiter that proceeds the host name, thereby enabling Cisco ISE-PIC to recognize the host

name and parse the message correctly. For more details about the fields in this screen, see Syslog Customized Template Settings and Examples, on page 52. The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

**Note** You can only customize a single header. After you customize a header, when you click **Custom Header** and create a template, only the newest configuration is saved.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Providers** > **Syslog Providers** to view all currently configured clients, to edit and delete existing clients, and to configure new clients.
The Syslog Providers table is displayed, including status information for each existing client.

**Step 2** Click **Custom Header** to open the Syslog Custom Header screen.

**Step 3** In the **Paste sample syslog** field, enter an example of the header format in your syslog messages. For example, copy and paste this header from one of your messages: `<181>Oct 10 15:14:08 Cisco.com`.

**Step 4** In the **Separator** field, indicate whether words are separated by spaces or tabs.

**Step 5** In the **Position of hostname in header** field, indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.

The **Hostname** field displays the host name based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows:

<181>Oct 10 15:14:08 Cisco.com

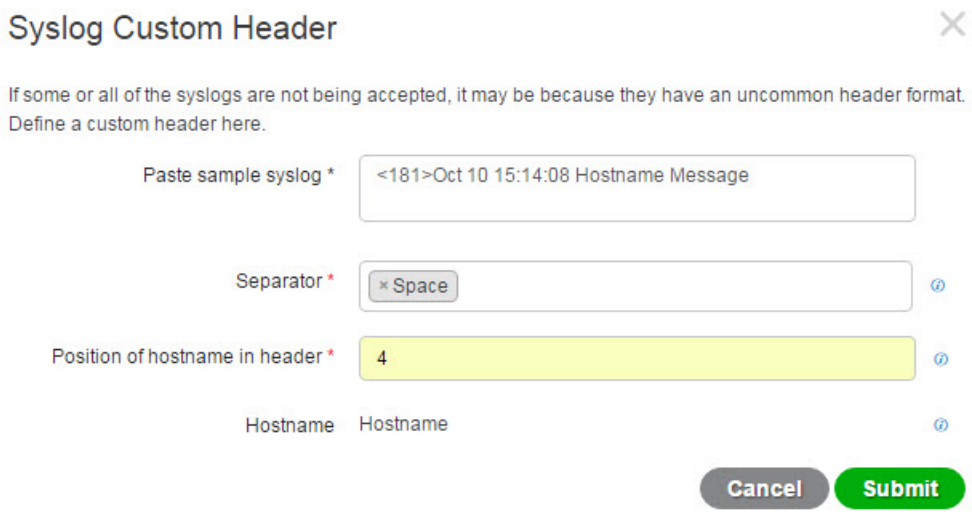
The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4.

The **Hostname** will automatically appear as Cisco.com, which is the fourth word in the header phrase pasted in the **Paste sample syslog** field.

If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields.

This example is as in the following screen capture:

*Figure 3: Customize Syslog Headers*




**Step 6** Click **Submit**.
The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

## Syslog Customized Template Settings and Examples

Cisco ISE-PIC enables you to customize your own syslog message templates to be parsed by the ISE-PIC parser. Customized templates determine the supported structures for both new and remove mapping messages. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the ISE-PIC parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

**Note** Most of the pre-defined templates use regular expressions. Customized templates should also use regular expressions.

### Syslog Header Parts

You can customize a single header that is recognized by the Syslog probe by configuring the delimiter that proceeds the host name.

The following table describes the different parts and fields that can be included in your customized syslog header. For more information about regular expressions, see Table 16: Regular Expressions for Customized Templates, on page 54.

***Table 14: Syslog Custom Header***

| Field | Description |
|---|---|
| Paste sample syslog | Enter an example of the header format in your syslog messages. For example, copy and paste this header:<br>`<181>Oct 10 15:14:08 Hostname Message` |
| Separator | Indicate whether words are separated by spaces or tabs. |
| Position of hostname in header | Indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this. |
| Hostname | Displays the hostname based on the details indicated in the first three fields. For example, if the header example in **Paste sample syslog** is as follows:<br><181>Oct 10 15:14:08 Hostname Message<br>The separator is indicated as **Space** and the **Position of hostname in header** is entered as 4.<br>The **Hostname** will automatically appear as Hostname.<br>If the host name is incorrectly displayed, check the data you have entered in the **Separator** and **Position of hostname in header** fields. |

### Syslog Template Parts and Descriptions for the Message Body

The following table describes the different parts and fields that can be included in your customized syslog message templates. For more information about regular expressions, see Table 16: Regular Expressions for Customized Templates, on page 54.

***Table 15: Syslog Template***

| Part | Field | Description |
|---|---|---|
| | Name | A unique name by which to recognize the purpose of this template. |
| Mapping Operations | New Mapping | A regular expression that describes the kind of mapping used with this template to add a new user. For example, enter "logged on from" in this field to indicate a new user that has logged on to the F5 VPN. |
| | Removed Mapping | A regular expression that describes the kind of mapping used with this template to remove a user. For example, enter "session disconnect" in this field to indicate a user that should be removed for ASA VPN. |

| Part | Field | Description |
|---|---|---|
| User Data | IP Address | A regular expression that indicates the IP addresses to be captured.<br>For example, for Bluecat messages, to capture identities for users within this IP address range, enter:<br>(.\|\s)((?:25[0-5]\|2[0-4][0-9]\|[01]?[0-9][0-9]?).){3}(?:25[0-5]\|2[0-4][0-9]\|[01]?[0-9][0-9]?) |
| | User Name | A regular expression that indicates the user name format to be captured. |
| | Domain | A regular expression that indicates the domain to be captured. |
| | Mac Address | A regular expression that indicates the MAC address format to be captured. |

### Regular Expression Examples

In order to parse messages use regular expressions. This sections offers regular expression examples in order to parse IP address, user name and add mapping messages.

For example, use regular expressions to parse the following messages:

<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session

<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

The regular expressions are as defined in the following table.

***Table 16: Regular Expressions for Customized Templates***

| Part | Regular Expression |
|---|---|
| IP address | Address <([^\s]+)>\|address ([^\s]+) |
| User name | User <([^\s]+)>\| Username = ([^\s]+) |
| Add mapping message | (%ASA-4-722051\|%ASA-6-713228) |

# Work with Syslog Predefined Message Templates

Syslog messages have a standard structure which include a header and the message body.

The predefined templates offered by Cisco ISE-PIC are described in this section, including content details for the headers that are supported, as well as the supported body structure, based on the origin of the messages.

In addition, you can create your own templates with customized body content for sources that are not predefined in the system. The supported structure for customized templates is also described in this section. You can configure a single customized header to be used in addition to the headers predefined in the system, when parsing messages, and you can configure multiple customized templates for the message body. For more information about customizing the header, see Customize Syslog Headers, on page 50. For more information about customizing the body, see Customize the Syslog Message Body, on page 50.



**Note** Most of the predefined templates use regular expressions, and customized templates should also use regular expressions.

### Message Headers

There are two header types recognized by the parser, for all message types (new and remove), for all client machines. These headers are as follows:

- <171>Host message
- <171>Oct 10 15:14:08 Host message

Once received, the header is parsed for host name, which can be IP address, hostname, or full FQDN.

Headers can also be customized. To customize your headers, see Customize Syslog Headers, on page 50.

## Syslog ASA VPN Pre-Defined Template

The supported syslog message format and types for ASA VPN are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

| Body Message | Parsing Example |
|---|---|
| %ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1 | [UserA,10.0.0.11] |
| %ASA-6-602303 IPsec: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created. | |
| %ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created. | |
| %ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string | |
| %ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user | |

| Body Message | Parsing Example |
|---|---|
| %ASA-6-113039 Group group User UserA IP 10.0.0.11 agent parent session started. | |
| %ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started. | |
| %ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user | [UserA,172.16.0.11]<br>**Note**<br>The parsed IP address from this message type is the private IP address, as indicated in the message. |
| %ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session | [UserA,172.16.0.12]<br>**Note**<br>The parsed IP address from this message type is the IPv4 address. |

### Remove Mapping Body Messages

The Remove Mapping messages supported for ASA VPN by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

**[UserA,10.1.1.1]**

| Body Message |
|---|
| %ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason |
| %ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number |
| %ASA-6-602304 IPsec: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted. |

| Body Message |
| --- |
| %ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted. |
| %ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA |
| %ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user. |
| %ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated. |
| %ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available. |
| %ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel. |
| %ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: Agent not enabled or invalid agent image on the ASA. |
| %ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated. |
| %ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted. |

## Syslog Bluecat Pre-Defined Template

The supported syslog message format and types for Bluecat are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

The messages supported for New Mapping for Bluecat syslog are as described in this section.

Once received, the body is parsed for user details as follows:

**[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]**

| Body |
| --- |
| Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17 |

### Remove Mapping Messages

There are no remove mapping messages known for Bluecat.

## Syslog F5 VPN Pre-Defined Template

The supported syslog message format and types for F5 VPN are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different F5 VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[user=UserA,ip=172.16.0.12]**

| Body |
| --- |
| Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\ |

### Remove Mapping Messages

Currently there are no remove messages for F5 VPN that are supported.

## Syslog Infoblox Pre-Defined Template

The supported syslog message format and types for Infoblox are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]**

| Body Message |
| --- |
| Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600 |
| Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW) |
| Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1 |

### Remove Mapping Messages

Once received, the body is parsed for user details as follows:

- If MAC address is included:

  **[00:0c:29:a2:18:34,10.0.10.100]**

- If MAC address is not included:

  **[10.0.10.100]**

| Body Message |
| --- |
| 07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired |
| 07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34 |
| 07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd |

## Syslog Linux DHCPd3 Pre-Defined Template

The supported syslog message format and types for Linux DHCPd3 are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Messages

There are different Linux DHCPd3 body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]**

| Body Message |
| --- |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1 |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1 |

### Remove Mapping Body Messages

The Remove Mapping messages supported for Linux DHCPd3 by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

**[00:0c:29:a2:18:34 ,10.0.10.100]**

| Body Message |
| --- |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired |
| Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1 |

## Syslog MS DHCP Pre-Defined Template

The supported syslog message format and types for MS DHCP are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different MS DHCP body messages that are recognized by the parser as described in the following table.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

**[macAddress=000C29912E5D, ip=10.0.10.123]**

| Body Message |
| --- |
| Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,,0x4D53465420352E30,MSFT,5.0 |

### Remove Mapping Body Messages

The Remove Mapping messages supported for MS DHCP by the parser are as described in this section.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

**[macAddress=000C29912E5D, ip=10.0.10.123]**

| Body Message |
| --- |
| Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0 |

## Syslog SafeConnect NAC Pre-Defined Template

The supported syslog message format and types for SafeConnect NAC are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different SafeConnect NAC body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]**

| Body Message |
| --- |
| Apr 10 09:33:58 nac Safe*Connect: authenticationResult\|xxx.xx.xxx.xxx\|xxx.xx.xxx.xxx\|UserA\|true\|Resnet-Macs\|TCNJ-Chain\|001b63b79018\|MAC |

### Remove Mapping Messages

Currently there are no remove messages for Safe Connect that are supported.

## Syslog Aerohive Pre-Defined Templates

The supported syslog message format and types for Aerohive are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different Aerohive body messages that are recognized by the parser as described in the following table.

Details parsed from the body include user name and IP address. The regular expression used for parsing is as in the following examples:

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

Once received, the body is parsed for user details as follows:

**[UserA,10.5.50.52]**

| Body Message |
| --- |
| 2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA |

### Remove Mapping Messages

Currently the system does not support remove mapping messages from Aerohive.

## Syslog Blue Coat Pre-Defined Templates—Main Proxy, Proxy SG, Squid Web Proxy

The system supports the following message types for Blue Coat:

- BlueCoat Main Proxy
- BlueCoat Proxy SG
- BlueCoat Squid Web Proxy

The supported syslog message format and types for Bluecoat messages are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different Blue Coat body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

**[UserA,192.168.10.24]**

| Body Message (this example is taken from a BlueCoat Proxy SG message) |
|---|
| 2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable |

The following table describes the different regular expression structures used per client for new mapping messages.

| Client | Regular expressions |
|---|---|
| BlueCoat Main Proxy | New mapping<br>**(TCP_HIT\|TCP_MEM){1}**<br>IP<br>**\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})\|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\s**<br>User name<br>**\s\-\s([a-zA-Z0-9_]+)\s\-\s** |
| BlueCoat Proxy SG | New mapping<br>**(\-\sPROXIED){1}**<br>IP<br>**\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})\|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\s[a-zA-Z0-9_]+\s\-**<br>User name<br>**\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-** |
| BlueCoat Squid Web Proxy | New mapping<br>**(TCP_HIT\|TCP_MEM){1}**<br>IP<br>**\s((?:(?:[0-9]{1,3}\.){3}[0-9]{1,3})\|(?:(?:[a-zA-Z0-9]{1,4}\:{1,2}){1,7}[a-zA-Z0-9]{1,4}))\sTCP**<br>User name<br>**\s([a-zA-Z0-9\._]+)\s\-\/** |

### Remove Mapping Messages

Remove mapping messages are supported for Blue Coat clients, though no examples are currently available.

The following table describes the different known regular expression structure examples used per client for remove mapping messages.

| Client | Regular expressions |
|---|---|
| BlueCoat Main Proxy | **(TCP_MISS\|TCP_NC_MISS){1}** |
| BlueCoat Proxy SG | No example currently available. |
| BlueCoat Squid Web Proxy | **(TCP_MISS\|TCP_NC_MISS){1}** |

## Syslog ISE and ACS Pre-Defined Templates

When listening to ISE or ACS clients, the parser receives the following message types:

- Pass authentication: When the user is authenticated by ISE or ACS, the pass authentication message is issued notifying that authentication succeeded, and including user details. The message is parsed and the user details and session ID are saved from this message.
- Accounting start and accounting update messages (new mapping): The accounting start or accounting update message is parsed with the user details and session ID that were saved from the Pass Authentication message and then the user is mapped.
- Accounting stop (remove mapping): The user mapping is deleted from the system.

The supported syslog message format and types for ISE and ACS are as described below.

### Pass Authentication Messages

The following messages are supported for Pass Authentication.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  User name and session ID only are parsed.

  **[UserA,5]**

### Accounting Start/Update (New Mapping) Messages

The following messages are supported for New Mapping.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  [UserA,10.0.0.16]

### Remove Mapping Messages

The following messages are supported for Remove Mapping.

- **Header**

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- **Body**

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- **Parsing Example**

  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in the message.

  **[UserA,10.0.0.16]**

## Syslog Lucent QIP Pre-Defined Template

The supported syslog message format and types for Lucent QIP are as described below.

### Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Predefined Message Templates, on page 54.

### New Mapping Body Messages

There are different Lucent QIP body messages that are recognized by the parser as described in the following table.

The regular expression structure for these messages is as follows:

**DHCP_GrantLease|:DHCP_RenewLease**

Once received, the body is parsed for user details as follows:

**[00:0C:29:91:2E:5D,10.0.0.11]**

| Body Message |
| --- |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC= 00:0C:29:91:2E:5D |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC= 00:0C:29:91:2E:5D |

#### Remove Mapping Body Messages

The regular expression structure for these messages is as follows:

**Delete Lease:|DHCP Auto Release:**

Once received, the body is parsed for user details as follows:

**[10.0.0.11]**

| Body Message |
| --- |
| DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$ |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$ |

# Filter Passive Identity Services

You can filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. The Live Session shows Passive Identity service components that are not filtered out by the Mapping Filters. You can add as many filters as needed. The “OR” logic operator applies between filters. If both the fields are specified in a single filter, the “AND” logic operator applies between these fields.

### Procedure

**Step 1** Choose **Providers** > **Mapping Filters**.

**Step 2** Click **Add**, enter the Username and or IP address of the user you want to filter and click **Submit**.

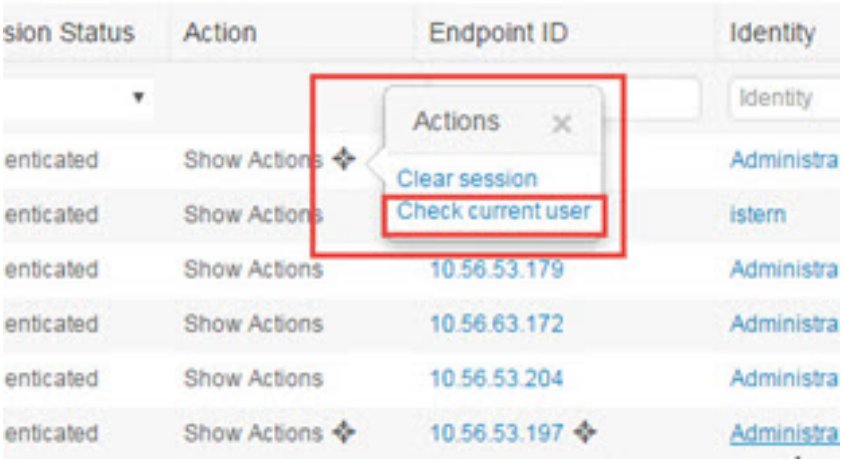
# Endpoint Probe

In addition to the customized providers that you can configure the Endpoint probe is enabled in ISE-PIC by default upon installation and always runs in the background. The Endpoint probe periodically checks whether each specific user is still logged in to the system.

**Note** In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point and ensure you choose to **Store Credentials**. For more information about configuring the Endpoint probe, see Work with the Endpoint Probe, on page 68.

To manually check for endpoint status go to **Live Sessions**, from the **Actions** column, click **Show Actions** and choose **Check current user**, as in the following figure.

***Figure 4: Check Current User***




For more information about endpoint user status, and manually running the check, see Live Sessions, on page 143.

When the Endpoint probe recognizes that a user has connected, if 4 hours have passed since the last time the session was updated for the specific endpoint, it checks whether that user is still logged in and collects the following data:

- MAC address
- Operating system version

Based on the this check, the probe does the following:

- When the user is still logged in, the probe updates Cisco ISE-PIC with the status Active User.
- When the user has logged out, the session state is updated as Terminated and fifteen minutes later, the user is removed from the Session Directory.

- When the user cannot be contacted, for example, when a firewall prevents contact or the endpoint has shut down, the status is updated as Unreachable and the Subscriber policy will determine how to handle the user session. The endpoint will remain in the Session Directory.

# Work with the Endpoint Probe

### Before you begin

The Endpoint Probe is enabled by default when ISE-PIC is installed. To enable and disable the probe, first ensure you have configured the following:

- Endpoints must have network connectivity to port 445.
- From ISE-PIC, configure an initial Active Directory join point. For more information about join points, see Active Directory as a Probe and a Provider, on page 17.



**Note** In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point, which enables the Endpoint probe to run even when the Active Directory probe is not fully configured.

### Procedure

**Step 1** Choose **Providers** > **Endpoint Probes**.

**Step 2** Choose **Enabled** or **Disabled**.
The screen does not change. However, the probe is enabled or disabled based on your selection, and if enabled, is now running in the background and collecting data.

# Generate pxGrid Certificates for Subscribers

### Before you begin



**Note** From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

At installation, ISE-PIC automatically generates self-signed certificates for the pxGrid services that are digitally signed by the primary ISE-PIC node. Thereafter, you can generate certificates for pxGrid subscribers in order

to guarantee mutual trust between pxGrid and the subscribers, thereby ultimately enabling user identities to be passed from ISE-PIC to the subscribers.

### Procedure

**Step 1** Choose **Subscribers** and go to the **Certificates** tab.

**Step 2** Select one of the following options from the **I want to** drop-down list:

- **Generate a single certificate without a certificate signing request**: You must enter the Common Name (CN) if you select this option. In the Common Name field, enter the pxGrid FQDN which includes pxGrid as the prefix. For example, www.pxgrid-ise.ise.net. Or, alternatively, use wildcards. For example, *.ise.net
- **Generate a single certificate with a certificate signing request**: You must enter the Certificate Signing Request details if you select this option.
- **Generate bulk certificates**: You can upload a CSV file that contains the required details.
- **Download Root Certificate Chain**: Download the ISE public root certificates in order to add them to the pxGrid client's trusted certificate store. The ISE pxGrid node only trusts the newly signed pxGrid client certificate and vice-versa, eliminating the need for outside certificate authorities.

**Step 3** (optional) You can enter a description for this certificate.

**Step 4** View or edit the pxGrid Certificate template on which this certificate is based. Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template. For pxGrid, only the pxGrid certificate template can be used when working with Passive Identity services and only the Subject information can be edited for this template. To edit this template, choose **Certificates** > **Certificate TemplatesAdministration** > **Certificates** > **Certificate Authority** > **Certificate Templates**.

**Step 5** Specify the Subject Alternative Name (SAN). You can add multiple SANs. The following options are available:

- **FQDN**: Enter the fully qualified domain name of the ISE node. For example www.isepic.ise.net. Or, alternatively, use wildcards for the FQDN. For example, *.ise.net

  An additional line can be added for FQDN in which the pxGrid FQDN can also be entered. This should be identical to the FQDN you used in the Common Name field.

- **IP address**: Enter the IP address of the ISE node to be associated with the certificate. This information must be entered if the subscriber uses IP addresses instead of an FQDN.

**Note**
This field is not displayed if you have selected the Generate Bulk Certificate option.

**Step 6** Select one of the following options from the **Certificate Download Format** drop-down list:

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**: The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM formatted certificate are BASE64-encoded ASCII files. Each certificate starts with the "--------BEGIN CERTIFICATE-----" tag and ends with the "-------END CERTIFICATE----" tag. The end entity's private key is stored using PKCS* PEM. It starts with the "-----BEGIN ENCRYPTED PRIVATE KEY----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY----" tag.

- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)**: A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity 's certificate and private key in one encrypted file.

**Step 7** Enter a certificate password.

**Step 8** Click **Create**.

# Enable Subscribers

You must perform this task, or alternatively automatically enable approvals, in order to allow subscribers to receive user identities from Cisco ISEISE-PIC. See Configure Subscriber Settings, on page 70.

**Procedure**

**Step 1** Choose **Subscribers** and ensure you are viewing the **Clients** tab.

**Step 2** Check the checkbox next to the subscriber and click **Approve**.

**Step 3** Click **Refresh** to view the latest status.

# View Subscriber Events from Live Logs

The Live Logs page displays all the Subscriber events. Event information includes the subscriber and capability names along with the event type and timestamp.

Navigate to **Subscribers** and select the **Live Log** tab to view the list of events. You can also clear the logs and resynchronize or refresh the list.

# Configure Subscriber Settings

**Procedure**

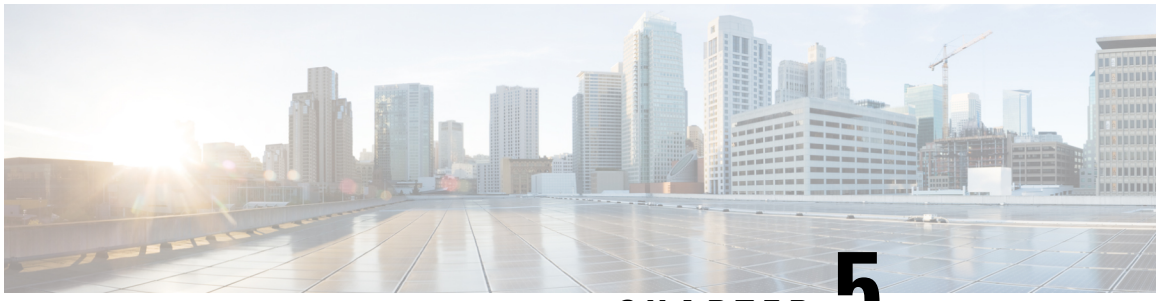
**Step 1** Choose **Subscribers** and go to the **Settings** tab.

**Step 2** Select the following options based on your requirements:

- **Automatically Approve New Accounts**: Check this checkbox to automatically approve the connection requests from new pxGrid clients.
- **Allow Password Based Account Creation**: Check this checkbox to enable username/password based authentication for pxGrid clients. If this option is enabled, the pxGrid clients cannot be automatically approved.

A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

**Step 3** Click **Save**.



CHAPTER 5

# Certificate Management in Cisco ISE-PIC

A certificate is an electronic document that identifies an individual, a server, a company, or other entity and associates that entity with a public key. Public Key Infrastructure (PKI) is a cryptographic technique that enables secure communication and verifies the identity of a user using digital signatures. Certificates are used in a network to provide secure access. Certificates can be self-signed or they can be digitally signed by an external Certificate Authority (CA). A self-signed certificate is signed by its own creator. A CA-signed digital certificate is considered industry standard and more secure. ISE-PIC can act as an external CA for pxGrid, digitally signing pxGrid certificates for the pxGrid subscribers.

Cisco ISE-PIC uses certificates for internode communication (each node presents its certificate to the other node in order to communicate with each other), and for communicating with pxGrid (ISE-PIC and pxGrid present certificates to each other). One certificate can be generated per node for each of these two purposes. Certificates identify a Cisco ISE node to pxGrid and secure the communication between pxGrid and the Cisco ISE node.

At installation, ISE-PIC automatically generates self-signed certificates for each ISE-PIC node (during installation, the administrator is prompted to accept the certificate that has been created for the secondary node automatically from the primary node) and certificates for the pxGrid services that are digitally signed by the primary ISE-PIC node. Thereafter, you can generate certificates for pxGrid subscribers in order to guarantee mutual trust between pxGrid and the subscribers, thereby ultimately enabling user identities to be passed from ISE-PIC to the subscribers. The **Certificate** menus in ISE-PIC are available in order to enable you to view the certificates, to generate additional ISE-PIC certificates and to perform some advanced tasks.

**Note** While an administrator has the ability to use an enterprise certificate, ISE-PIC has been designed by default to use the internal authority for issuance of pxGrid certificates for subscribers.


- Certificate Matching in Cisco ISE-PIC, on page 74
- Wildcard Certificates, on page 74
- Certificate Hierarchy in ISE-PIC, on page 77
- System Certificates, on page 77
- Trusted Certificates Store, on page 81
- Certificate-Signing Requests, on page 88
- Cisco ISE CA Service, on page 94
- OCSP Services, on page 102

# Certificate Matching in Cisco ISE-PIC

When you set up Cisco ISE-PIC nodes in a deployment, the nodes communicate with each other. The system checks the FQDN of each Cisco ISE-PIC node to ensure that they match (for example ise1.cisco.com and ise2.cisco.com or if you use wildcard certificates then *.cisco.com). In addition, when an external machine presents a certificate to a Cisco ISE-PIC server, the external certificate that is presented for authentication is checked (or matched) against the certificate in the Cisco ISE-PIC server. If the two certificates match, the authentication succeeds.

For CiscoISE-PIC, matching is performed between the ISE-PIC nodes (if there are two), and between Cisco ISE-PIC and pxGrid.

Cisco ISE-PIC checks for a matching subject name as follows:

1. Cisco ISE-PIC looks at the subject alternative name extension of the certificate. If the subject alternative name contains one or more DNS names, then one of the DNS names must match the FQDN of the Cisco ISE node. If a wildcard certificate is used, then the wildcard domain name must match the domain in the Cisco ISE node's FQDN.
2. If there are no DNS names in the subject alternative name, or if the subject alternative name is missing entirely, then the common name in the **Subject** field of the certificate or the wildcard domain in the **Subject** field of the certificate must match the FQDN of the node.
3. If no match is found, the certificate is rejected.

# Wildcard Certificates

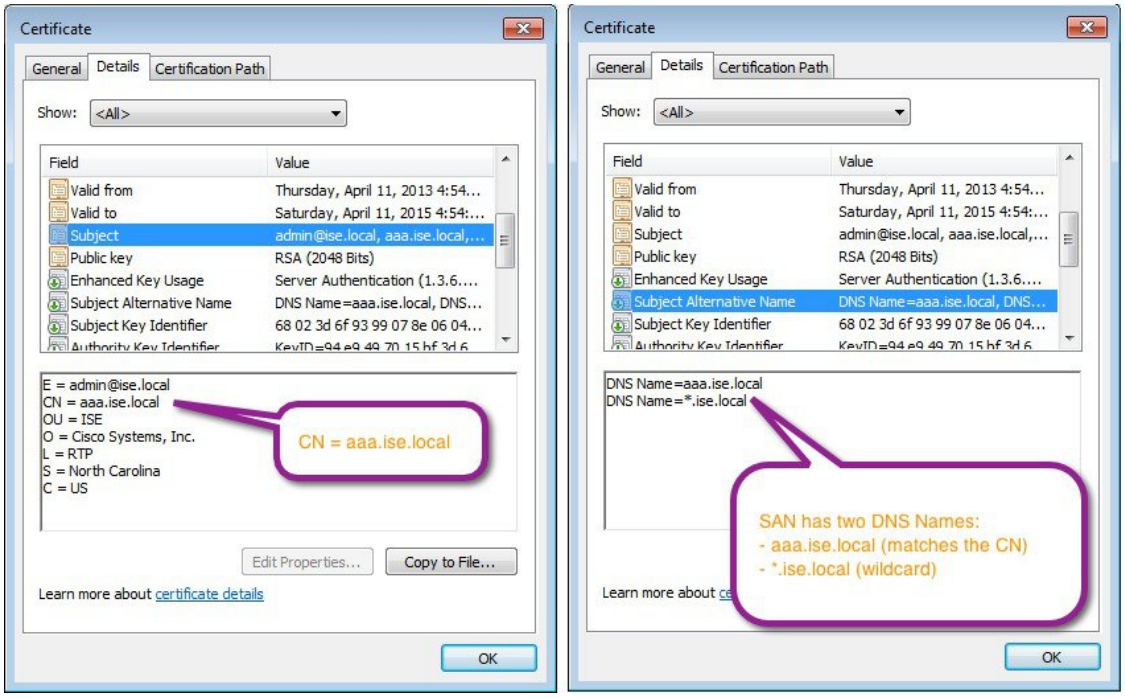
A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and the certificate can be shared across multiple hosts in an organization. For example, the **CN** value for the certificate subject would be a generic hostname such as aaa.ise.local and the SAN field would include the same generic hostname and a wildcard notation such as DNS.1=aaa.ise.local and DNS.2=*.ise.local.

If you configure a wildcard certificate to use *.ise.local, you can use the same certificate to secure any other host whose DNS name ends with ".ise.local," such aspsn.ise.local.

Wildcard certificates secure communication in the same way as a regular certificate, and requests are processed using the same validation methods.

The following figure is an example of a wildcard certificate that is used to secure a website.

*Figure 5: Example of Wildcard Certificate*




Using an asterisk (*) in the SAN field allows you to share a single certificate with all of your nodes (if you have installed more than one node) and helps prevent certificate name mismatch warnings. However, the use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node separately.

**Note** Some of the examples for FQDN are taken from a full Cisco ISE installation and therefore may be different than addresses relevant to the ISE-PIC installation.

# Advantages of Using Wildcard Certificates

- Cost savings: Certificates that are signed by third-party CAs are expensive, especially as the number of servers increases. Wildcard certificates can be used on multiple nodes in the Cisco ISE deployment.
- Operational efficiency: Wildcard certificates allow all PSNs to share the same certificate for EAP and web services. In addition to significant cost savings, certificate administration is also simplified by creating the certificate once and applying it on all the PSNs.
- Reduced authentication errors: Wildcard certificates address issues seen with Apple iOS devices when the client stores trusted certificates within the profile and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a PSN, it does not explicitly trust the PSN certificate, although a trusted CA has signed the certificate. Using a wildcard certificate, the certificate is the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without errors or prompts.

- Simplified supplicant configuration: For example, a Microsoft Windows supplicant with PEAP-MSCHAPv2 and a trusted server certificate requires that you specify each of the server certificate to trust, or the user may be prompted to trust each PSN certificate when the client connects using a different PSN. With wildcard certificates, a single server certificate can be trusted rather than individual certificates from each PSN.
- Wildcard certificates result in an improved user experience with less prompting and more seamless connectivity.

# Disadvantages of Using Wildcard Certificates

The following are some of the security considerations that are related to the use of wildcard certificates:

- Loss of auditability and nonrepudiation.
- Increased exposure of the private key.
- Not common or understood by administrators.

Wildcard certificates are considered less secure than using a unique server certificate in each Cisco ISE node. But cost and other operational factors outweigh the security risk.

Security devices such as Cisco Adaptive Security Appliance also support wildcard certificates.

You must be careful when deploying wildcard certificates. For example, if you create a certificate with *.company.local and an attacker is able to recover the private key, that attacker can spoof any server in the company.local domain. Therefore, it is considered a best practice to partition the domain space to avoid this type of compromise.

To address this possible issue and to limit the scope of use, wildcard certificates may also be used to secure a specific subdomain of your organization. Add an asterisk (*) in the subdomain area of the common name where you want to specify the wildcard.

For example, if you configure a wildcard certificate for *.ise.company.local, that certificate may be used to secure any host whose DNS name ends in ".ise.company.local", such as:

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

# Wildcard Certificate Compatibility

Wildcard certificates are usually created with the wildcard listed as the common name of the certificate subject. Cisco ISE supports this type of construction. However, not all endpoint supplicants support the wildcard character in the certificate subject.

All the Microsoft native supplicants that were tested (including Windows Mobile which is now discontinued) do not support wildcard character in the certificate subject.

You can use another supplicant, such as Network Access Manager that might allow the use of wildcard characters in the Subject field.

You can also use special wildcard certificates such as DigiCert's Wildcard Plus that is designed to work with incompatible devices by including specific subdomains in the Subject Alternative Name of the certificate.

Although the Microsoft supplicant limitation appears to be a deterrent to using wildcard certificates, there are alternative ways to create the wildcard certificate that allow it to work with all the devices tested for secure access, including the Microsoft native supplicants.

To do this, instead of using the wildcard character in the Subject, you must use the wildcard character in the Subject Alternative Name field instead. The Subject Alternative Name field maintains an extension that is designed for checking the domain name (DNS name). See RFC 6125 and RFC 2128 for more information.

# Certificate Hierarchy in ISE-PIC

In ISE-PIC, view the certificate hierarchy or the certificate trust chain of all certificates. The certificate hierarchy includes the certificate, all the intermediate CA certificates, and the root certificate. For example, when you choose to view a system certificate from the ISE-PIC, the details of the corresponding system certificate are displayed. The certificate hierarchy is displayed at the top of the certificate. Click a certificate in the hierarchy to view its details. The self-signed certificate does not have any hierarchy or trust chain.

In the certificate listing windows, you will see one of the following icons in the **Status** column:

- Green icon: Indicates a valid certificate (valid trust chain).
- Red icon: Indicates an error (for example, trust certificate missing or expired).
- Yellow icon: Warns that a certificate is about to expire and prompts renewal.

# System Certificates

Cisco ISE-PIC system certificates are server certificates that identify a Cisco ISE-PIC node to other nodes in the deployment and to client applications. To access system certificates, choose **Administration** > **System** > **Certificates** > **System Certificates**. System certificates are:

- Used for inter-node communication in a Cisco ISE-PIC deployment. Check the **Admin** check box in the **Usage** area of these certificates.
- Used to communicate with the pxGrid controller. Check the **pxGrid** check box in the **Usage** area of these certificates.

Install valid system certificates on each node in your Cisco ISE-PIC deployment. By default, two self-signed certificates and one signed by the internal Cisco ISE CA are created on a Cisco ISE-PIC node during installation time:

- A self-signed server certificate designated for Admin and pxGrid use (it has a key size of 2048 and is valid for one year).
- A self-signed SAML server certificate that can be used to secure communication with a SAML identity provider (it has a key size of 2048 and is valid for one year).
- An internal Cisco ISE CA-signed server certificate that can be used to secure communication with pxGrid clients (it has a key size of 4096 and is valid for one year).

When you set up a deployment and register a secondary node, the certificate that is designated for pxGrid controller is automatically replaced with a certificate that is signed by the primary node's CA. Thus, all pxGrid certificates become part of the same PKI trust hierarchy.

For supported key and cipher information for your release, see the appropriate version of the Cisco Identity Services Engine Network Component Compatibility guide.

We recommend that you replace the self-signed certificate with a CA-signed certificate for greater security. To obtain a CA-signed certificate, you must:

1. Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 88
2. Import a Root Certificate into the Trusted Certificate Store, on page 86
3. Bind a CA-Signed Certificate to a Certificate Signing Request, on page 89

# View System Certificates

The **System Certificate** window lists all the system certificates added to Cisco ISE-PIC.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **System Certificates**.

**Step 2** The following columns are displayed in the **System Certificates** window:

- **Friendly Name**: Name of the certificate.
- **Usage**: The services for which this certificate is used.
- **Portal group tag**: Applicable only for certificates that are designated for portal use. This field specifies which certificate has to be used for portals.
- **Issued To**: Common Name of the certificate subject.
- **Issued By**: Common Name of the certificate issuer
- **Valid From**: Date on which the certificate was created, also known as the "Not Before" certificate attribute.
- **Valid To (Expiration)**: Expiration date of the certificate, also known as the "Not After" certificate attribute. The following icons are displayed next to the expiration date:
  - Green icon: Expiring in more than 90 days.
  - Blue icon: Expiring in 90 days or less.
  - Yellow icon: Expiring in 60 days or less.
  - Orange icon: Expiring in 30 days or less.
  - Red icon: Expired.

# Import a System Certificate

You can import a system certificate for any Cisco ISE-PIC node from the administration portal.

**Note** Changing the certificate of the admin role certificate on a primary PAN node restarts services on all other nodes. The system restarts one node at a time, after the primary PAN restart is complete.

### Before you begin

- Ensure that you have the system certificate and the private key file on the system that is running on the client browser.
- If the system certificate that you import is signed by an external CA, import the relevant root CA and intermediate CA certificates into the Trusted Certificates store (**Certificates > Trusted Certificates**).
- If the system certificate that you import contains basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.

### Procedure

**Step 1** Choose **Certificates** > **System Certificates**.

**Step 2** Click **Import**.
The **Import Server Certificate** window is displayed.

**Step 3** Enter the values for the certificate that you are going to import.

**Step 4** Click **Submit**.

# Generate a Self-Signed Certificate

Add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you plan to deploy Cisco ISE-PIC in a production environment, use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

**Note** If you use a self-signed certificate and you want to change the hostname of your Cisco ISE-PIC node, log in to the Cisco ISE-PIC node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE-PIC continues to use the self-signed certificate with the old hostname.

**Procedure**

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **System Certificates**.

**Step 2** Click **Generate Self Signed Certificate** and enter the details in the window displayed.

**Step 3** Check the **Allow Wildcard Certificates** check box to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject or the DNS name in the Subject Alternative Name. For example, the DNS name that is assigned to the SAN can be *.amer.cisco.com.

**Step 4** Check the check boxes in the **Usage** area based on the service for which you want to use this certificate.

**Step 5** Click **Submit** to generate the certificate.

To restart the secondary nodes, from the CLI, enter the following commands in the following order:

a) **application stop ise**
b) **application start ise**

# Edit a System Certificate

Use this window to edit a system certificate and to renew a self-signed certificate. When you edit a wildcard certificate, the changes are replicated to all the nodes in the deployment. If you delete a wildcard certificate, that wildcard certificate is removed from all the nodes in the deployment.

**Procedure**

**Step 1** Choose **Certificates** > **System Certificates**.

**Step 2** Check the check box next to the certificate that you want to edit, and click **Edit**.

**Step 3** To renew a self-signed certificate, check the **Renewal Period** check box and enter the expiration Time to Live (TTL) in days, weeks, months, or years. Choose the required value from the drop-down lists.

**Step 4** Click **Save**.

If the **Admin** check box is checked, then the application server on the Cisco ISE-PIC node restarts.

# Delete a System Certificate

Although you can delete multiple certificates from the System Certificates store at a time, you must have at least one certificate to use for Admin authentication. Also, you cannot delete any certificate that is in use for Admin or pxGrid controller. However, you can delete the pxGrid certificate when the service is disabled.

If you choose to delete a wildcard certificate, the certificate is removed from all the Cisco ISE nodes in the deployment.

**Procedure**

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **System Certificates**.

**Step 2** Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message is displayed.

**Step 3** Click **Yes** to delete the certificate.

# Export a System Certificate

You can export a system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

**Procedure**

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **System Certificates**. .

**Step 2** Check the check box next to the certificate that you want to export and click **Export**.

**Step 3** Choose whether to export only the certificate, or the certificate and its associated private key.

**Tip**
We do not recommend exporting the private key that is associated with a certificate because its value may be exposed. If you must export a private key (for example, when you export a wildcard system certificate to be imported into the other Cisco ISE nodes for inter-node communication), specify an encryption password for the private key. You must specify this password while importing this certificate into another Cisco ISE-PIC node to decrypt the private key.

**Step 4** Enter the password if you have chosen to export the private key. The password should be at least eight characters long.

**Step 5** Click **Export** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the PEM format. If you export both the certificate and private key, the certificate is exported as a .zip file that contains the certificate in the PEM format and the encrypted private key file.

# Trusted Certificates Store

The Trusted Certificates store contains X.509 certificates that are used for trust and for Simple Certificate Enrollment Protocol (SCEP).

X.509 certificates imported to Cisco ISE must be in PEM or Distinguished Encoding Rule format. Files containing a certificate chain, a system certificate along with the sequence of trust certificates that sign it, are imported, subject to certain restrictions.

When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until the Cisco ISE services restart.

X.509 certificates are only valid until a specific date. When a trusted certificate expires, the Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE notifies you about the pending expiration of a system certificate when the expiration date is within 90 days. This notification appears in several ways:

- Colored expiration status icons are displayed in the **System Certificates** window.
- Expiration messages appear in the Cisco ISE System Diagnostic report (**Operations** > **Reports** > **Reports** > **Diagnostics** > **System Diagnostic**.
- Expiration alarms are generated 90 days, 60 days, and 30 days before expiration, and every day in the final 30 days before expiration.

If the expiring certificate is a self-signed certificate, you can extend its expiration date by editing the certificate. For a CA-signed certificate, allow sufficient time to acquire the replacement certificate from your CA.

Cisco ISE uses the trusted certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing ISE-PICusing certificate-based administrator authentication.
- To enable secure communication between Cisco ISE-PIC nodes in a deployment. The Trusted Certificates store must contain the chain of CA certificates needed to establish trust with the system certificate on each node in a deployment.
    - If a self-signed certificate is used for the system certificate, the self-signed certificate from each node must be placed in the Trusted Certificates store of the PAN.
    - If a CA-signed certificate is used for the system certificate, the CA root certificate, and any intermediate certificates in the trust chain, must be placed in the Trusted Certificates store of the PAN.

At installation, the Trusted Certificate store is populated with automatically generated trusted certificates. The Root certificate (Cisco Root CA) signs the Manufacturing (Cisco CA Manufacturing) certificate.

# Trusted Certificate Naming Constraints

A trusted certificate in CTL may contain a name constraint extension. This extension defines a namespace for values of all subject name and subject alternative name fields of subsequent certificates in a certificate chain. Cisco ISE does not check constraints that are specified in a root certificate.

Cisco ISE supports the following name constraints:

- Directory name

  The directory name constraint should be a prefix of the directory name in the subject or subject alternative name field. For example:

    - Correct subject prefix:

      CA certificate name constraint: Permitted: O=Cisco

      Client certificate subject: O=Cisco,CN=Salomon

    - Incorrect subject prefix:

CA certificate name constraint: Permitted: O=Cisco

Client certificate subject: CN=Salomon,O=Cisco

- DNS
- Email
- URI (The URI constraint must start with a URI prefix such as http://, https://, ftp://, or ldap://).

Cisco ISE does not support the following name constraints:

- IP Address
- OtherName

When a trusted certificate contains a constraint that is not supported and the certificate that is being verified does not contain the appropriate field, Cisco ISE rejects the certificate because it cannot verify unsupported constraints.

The following is an example of the name constraints definition within the trusted certificate:

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                  DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

An acceptable client certificate subject that matches the above definition is as follows:

```
           Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

# View Trusted Certificates

The **Trusted Certificates** window lists all the trusted certificates that are available in Cisco ISE-PIC.

### Procedure

**Step 1** To view all the certificates, choose Choose **Certificates** > **Trusted Certificates**. The Trusted Certificates window displayed, listing all the trusted certificates.

**Step 2** Check the check box of the trusted certificate and click **Edit**, **View**, **Export**, or **Delete** to perform the required task.

# Change the Status of a Certificate in Trusted Certificates Store

The status of a certificate must be enabled so that Cisco ISE-PIC can use the certificate for establishing trust. When a certificate is imported into the Trusted Certificates store, it is automatically enabled.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Trusted Certificates**.

**Step 2** Check the check box next to the certificate you want to enable or disable, and click **Edit**.

**Step 3** Choose the status from the **Status** drop-down list.

**Step 4** Click **Save**.

# Add a Certificate to Trusted Certificates Store

The **Trusted Certificate** store window allows you to add CA certificates to Cisco ISE-PIC.

### Before you begin

- The certificate that you want to add must be in the file system of the computer where your browser is running. The certificate must be in PEM or DER format.
- To use the certificate for Admin or EAP authentication, define the basic constraints in the certificate and set the CA flag to true.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Trusted Certificates**.

**Step 2** Click **Import**.

**Step 3** Configure the field values as necessary.

To use any sub-CA certificate in the certificate chain for EAP authentication or certificate-based administrator authentication, check the **Trust for client authentication and Syslog** check box while importing all the certificates in the certificate chain up until the root CA. You can import more than one CA certificate with the same subject name. For certificate-based administrator authentication, check the **Trust for certificate based admin authentication** check box when adding a trusted certificate. You cannot check the **Trust for certificate based admin authentication** check box for a certificate in the trusted certificate store if there is another certificate in the store with the same subject, and has the **Trust for certificate based admin authentication** check box enabled.

When you change the authentication type from password-based authentication to certificate-based authentication, Cisco ISE-PIC restarts the application server on each node in your deployment, starting with the application server on the PAN.

# Edit a Trusted Certificate

After you add a certificate to the Trusted Certificates store, you can further edit it by using the **Edit** options.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Trusted Certificates**.

**Step 2** Check the check box next to the certificate that you want to edit, and click **Edit**.

**Step 3** (Optional) Enter a name for the certificate in the **Friendly Name** field. If you do not specify a friendly name, a default name is generated in the following format:

*common-name#issuer#nnnnn*

**Step 4** Define the usage of the certificate by checking the necessary check boxes in the **Trusted For** area.

**Step 5** (Optional) Enter a description for the certificate in the **Description** field.

**Step 6** Click **Save**.

# Delete a Trusted Certificate

You can delete trusted certificates that you no longer need. However, you must not delete Cisco ISE-PIC internal CA certificates. Cisco ISE-PIC internal CA certificates can be deleted only when you replace the Cisco ISE-PIC root certificate chain for the entire deployment.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Trusted Certificates**.

**Step 2** Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message is displayed. To delete the Cisco ISE-PIC Internal CA certificates, click one of the following options:

- **Delete**: To delete the Cisco ISE-PIC internal CA certificates. All endpoint certificates that are signed by the Cisco ISE-PIC internal CA become invalid and the endpoints cannot join the network. To allow the endpoints on the network again, import the same Cisco ISE-PIC internal CA certificates into the Trusted Certificates store.
- **Delete & Revoke**: Deletes and revokes the Cisco ISE-PIC internal CA certificates. All endpoint certificates that are signed by the Cisco ISE-PIC internal CA become invalid and the endpoints cannot get on to the network. This operation cannot be undone. You must replace the Cisco ISE-PIC root certificate chain for the entire deployment.

**Step 3** Click **Yes** to delete the certificate.

# Export a Certificate from Trusted Certificates Store

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

**Note** If you export certificates from the internal CA and plan to use the exported certificates to restore from backup, use the CLI command **application configure ise**. See Export Cisco ISE CA Certificates and Keys, on page 100.

### Procedure

**Step 1** Check the check box next to the certificate that you want to export, and click **Export**. You can export only one certificate at a time.

**Step 2** The chosen certificate downloads in the PEM format into the file system that is running your client browser.

# Import a Root Certificate into the Trusted Certificate Store

When you import the root CA and intermediate CA certificates, specify the services for which the trusted CA certificates are to be used.

When you import an external root CA certificate, enable the **Trust for certificate based admin authentication** usage option in Step 5 of the following task.

### Before you begin

You must have the root certificate and other intermediate certificates from the CA that signed your certificate signing requests and returned the digitally signed CA certificates.

### Procedure

**Step 1** Click **Import**.

**Step 2** In the **Import a new Certificate into the Certificate Store** window, click **Choose File** to select the root CA certificate that is signed and returned by your CA.

**Step 3** Enter a **Friendly Name**.

If you do not enter a **Friendly Name**, Cisco ISE-PIC autopopulates this field with a name of the format *common-name#issuer#nnnnn*, where *nnnnn* is a unique number. You can also edit the certificate later to change the **Friendly Name**.

**Step 4** Check the check boxes next to the services for which you want to use this trusted certificate.

**Step 5** (Optional) In the **Description** field, enter a description for your certificate.

**Step 6** Click **Submit**.

### What to do next

Import the intermediate CA certificates into the Trusted Certificates store (if applicable).

# Certificate Chain Import

You can import multiple certificates from a single file that contains a certificate chain received from a Certificate store. All certificates in the file must be in the PEM format, and the certificates must be arranged in the following order:

- The last certificate in the file must be the client or server certificate issued by the CA.
- All preceding certificates must be the root CA certificate plus any intermediate CA certificates in the signing chain for the issued certificate.

Importing a certificate chain is a two-step process:

1. Import the certificate chain file into the Trusted Certificate store in the Cisco ISE administration portal. This operation imports all certificates from the file except the last one into the Trusted Certificates store.
2. Import the certificate chain file using the Bind a CA-Signed Certificate operation. This operation imports the last certificate from the file as a local certificate.

# Trusted Certificate Import Settings

The following table describes the fields in the Trusted Certificate Import window, which you can use to add CA certificates to Cisco ISE-PIC. To view this window, click the **Menu** icon (☰) and choose **Certificates** > **Trusted Certificates** > **Import**.

*Table 17: Trusted Certificate Import Settings*

| Field Name | Description |
|---|---|
| **Certificate File** | Click **Browse** to choose the certificate file from the computer that is running the browser. |
| **Friendly Name** | Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE-PIC automatically creates a name in the format <common name>#<issuer>#<nnnnn>, where <nnnnn> is a unique five-digit number. |
| **Trust for authentication within ISE** | Check the check box if you want this certificate to be used to verify server certificates (from other ISE-PIC nodes or LDAP servers). |
| **Trust for client authentication and Syslog** | (Applicable only if you check the Trust for authentication within ISE-PIC check box) Check the check box if you want this certificate to be used to:<br>• Authenticate endpoints that connect to ISE-PIC using the EAP protocol<br>• Trust a Syslog server |

| Field Name | Description |
|---|---|
| **Trust for authentication of Cisco Services** | Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service. |
| **Validate Certificate Extensions** | (Only if you check both the Trust for client authentication and Enable Validation of Certificate Extensions options) Ensure that the "keyUsage" extension is present and the "keyCertSign" bit is set, and that the basic constraints extension is present with the CA flag set to true. |
| **Description** | Enter an optional description. |

**Related Topics**

Trusted Certificates Store, on page 81
Certificate Chain Import, on page 87
Import a Root Certificate into the Trusted Certificate Store, on page 86

# Certificate-Signing Requests

For a CA to issue a signed certificate, you must create a certificate signing request and submit it to the CA.

The list of certificate-signing requests that you have created is available in the **Certificate-Signing Requests** window. To view this window, click the **Menu** icon (☰) and choose**Administration** > **System** > **Certificates** > **Certificate-Signing Requests**. To obtain signatures from a CA, you must export the certificate-signing request and then send the certificates to the CA. The CA signs and returns your certificates.

You can manage the certificates centrally from the Cisco ISE administration portal. You can create certificate-signing requests for all the nodes in your deployment and export them. Then, you should submit the certificate-signing requests to a CA, obtain the signed certificates from the CA, import the root and intermediary CA certificates given by the CA into the Trusted Certificates store, and bind the CA-signed certificates to the certificate-signing requests.

## Create a Certificate-Signing Request and Submit it to a Certificate Authority

You can generate a certificate-signing request to obtain a CA-signed certificate for the nodes in your deployment. You can generate the certificate-signing request for a specific node in the deployment or for all the nodes in your deployment.

**Procedure**

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Certificate-Signing Requests**.

**Step 2** Click **Generate Certificate-Signing Requests (CSR)** to generate the certificate-signing request.

**Step 3** Enter the values for generating a certificate-signing request. See Trusted Certificate Settings, on page 97 for information on each of the fields in the window displayed.

**Step 4** (Optional) Check the check box of the signing request that you want to download and and click **Export** to download the request.

**Step 5** Copy all the text from "**-----BEGIN CERTIFICATE REQUEST-----**" through "**-----END CERTIFICATE REQUEST-----.**" and paste the contents of the request in the certificate request of the chosen CA.

**Step 6** Download the signed certificate.

Some CAs might email the signed certificate to you. The signed certificate is in the form of a .zip file that contains the newly issued certificate and the public signing certificates of the CA that you must add to the Cisco ISE-PIC trusted certificates store. The digitally-signed CA certificate, root CA certificate, and other intermediate CA certificate (if applicable) can be downloaded to the local system running your client browser.

# Bind a CA-Signed Certificate to a Certificate Signing Request

After the CA returns the digitally signed certificate, you must bind it to the certificate-signing request. You can perform the bind operation for all the nodes in your deployment, from the Cisco ISE administration portal.

### Before you begin

- You must have the digitally signed certificate, and the relevant root intermediate CA certificates sent by the CA.
- Import the relevant root and intermediate CA certificates to the Trusted Certificates store (**Certificates** > **Trusted Certificates**. ).

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Certificate-Signing Requests**.

**Step 2** Check the check box next to the certificate signing request you must bind with the CA-signed certificate.

**Step 3** Click **Bind Certificate**.

**Step 4** In the **Bind CA Signed Certificate** window displayed, click **Choose File** to choose the CA-signed certificate.

**Step 5** Enter a value in the **Friendly Name** field.

**Step 6** Check the **Validate Certificate Extensions** check box if you want Cisco ISE-PIC to validate certificate extensions.

If you enable the **Validate Certificate Extensions** option, and the certificate that you import contains a basic constraints extension with the CA flag set to True, ensure that the key usage extension is present, and that the keyEncipherment bit or the keyAgreement bit, or both, are also set.

**Note**
Cisco ISE requires EAP-TLS client certificates to have digital signature key usage extension.

**Step 7** (Optional) Check the services for which this certificate will be used in the **Usage** area.

This information is autopopulated if you have enabled the **Usage** option while generating the certificate signing request. You can also choose to edit the certificate at a later time to specify the usage.

Changing the **Admin** usage certificate on a primary PAN restarts the services on all the other nodes. The system restarts one node at a time, after the primary PAN restarts.

**Step 8** Click **Submit** to bind the certificate-signing request with the CA-signed certificate.

If this certificate is marked for Cisco ISE-PIC internode communication usage, the application server on the Cisco ISE-PIC node restarts.

Repeat this process to bind the certificate-signing request with the CA-signed certificate on the other nodes in the deployment.

### What to do next

Import a Root Certificate into the Trusted Certificate Store, on page 86

# Export a Certificate-Signing Request

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Certificate-Signing Requests**.

**Step 2** Check the check box next to the certificates that you want to export, and click **Export**.

**Step 3** The certificate-signing request is downloaded to your local file system.

# Certificate-Signing Request Settings

Cisco ISE-PIC allows you to generate certificate-signing requests for the nodes in your deployment from the administration portal in a single request. Also, you can choose to generate the certificate signing request for a single node or nodes in the deployment. If you choose to generate a certificate signing request for a single node, ISE automatically substitutes the Fully Qualified Domain Name (FQDN) of that particular node in the CN field of the certificate subject. If you enter a domain name other than the FQDN of that node in the CN field, Cisco ISE rejects authentication with that certificate. If you choose to include an entry in the Subject Alternative Name (SAN) field of the certificate, you must enter the FQDN of the ISE-PIC node in addition to other SAN attributes. If necessary, you can also add additional FQDNs in the SAN field. If you choose to generate certificate signing requests for both nodes in your deployment, check the Allow Wildcard Certificates check box and enter the wildcard FQDN notation in the SAN field (DNS name), for example, *.amer.example.com. If you plan to use the certificate for EAP Authentication, do not enter the wildcard value in the CN= field.

With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE-PIC node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE-PIC node.

The following table describes the fields in the certificate-signing request window, which you can use to generate a certificate-signing request that can be signed by a Certificate Authority (CA). To view this window, click the **Menu** icon (☰) and choose **Certificates** > **Certificate Management** > **Certificate-Signing Request**.

*Table 18: Certificate-Signing Request Settings*

| Field | Usage Guidelines |
|---|---|
| Certificate(s) will be used for | |

| Field | Usage Guidelines |
|---|---|
| | Choose the service for which you are going to use the certificate:<br>**Cisco ISE Identity Certificates**<br>• **Multi-Use**: Used for multiple services (Admin, EAP-TLS Authentication, pxGrid). Multi-use certificates use both client and server key usages. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:<br>  • **Key Usage**: Digital Signature (Signing)<br>  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)<br>• **Admin**: Used for server authentication (to secure communication with the Admin portal and between ISE-PIC nodes in a deployment). The certificate template on the signing CA is often called a Web Server certificate template. This template has the following properties:<br>  • **Key Usage**: Digital Signature (Signing)<br>  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)<br>• **ISE Messaging Service**: Used by the feature Syslog Over Cisco ISE Messaging, which enables MnT WAN survivability for built-in UDP syslog collection targets (LogCollector and LogCollector2).<br>  • **Key Usage**: Digital Signature (Signing)<br>  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)<br>• **pxGrid**: Used for both client and server authentication (to secure communication between the pxGrid client and server). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:<br>  • **Key Usage**: Digital Signature (Signing)<br>  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)<br>• **SAML**: Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on.<br>  • **Key Usage**: Digital Signature (Signing)<br>  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)<br>**Note**<br>We recommend that you do not use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute. If you use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute, the certificate is considered invalid and the following error message is displayed:<br>`source=local ; type=fatal ; message="unsupported certificate"`<br>**Cisco ISE Certificate Authority Certificates** |

| Field | Usage Guidelines |
|---|---|
| | • **ISE Root CA**: (Applicable only for the internal CA service ) Used for regenerating the entire internal CA certificate chain including the root CA on the Primary PAN and subordinate CAs on the PSNs.<br>• **ISE Intermediate CA**: (Applicable only for the internal CA service when ISE-PIC acts as an intermediate CA of an external PKI) Used to generate an intermediate CA certificate on the Primary PAN and subordinate CA certificates on the PSNs. The certificate template on the signing CA is often called a Subordinate Certificate Authority. This template has the following properties:<br>  • **Basic Constraints**: Critical, Is a Certificate Authority<br>  • **Key Usage**: Certificate Signing, Digital Signature<br>  • **Extended Key Usage**: OCSP Signing (1.3.6.1.5.5.7.3.9)<br>• **Renew ISE OCSP Responder Certificates**: (Applicable only for the internal CA service) Used to renew the ISE-PIC OCSP responder certificate for the entire deployment (and is not a certificate signing request). For security reasons, we recommend that you renew the ISE-PIC OCSP responder certificates every six months. |
| **Allow Wildcard Certificates** | Check this check box to use a wildcard character (*) in the CN and/or the DNS name in the SAN field of the certificate. If you check this check box, all the nodes in the deployment are selected automatically. You must use the asterisk (*) wildcard character in the left-most label position. If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it might lead to security issues. |
| **Generate CSRs for these Nodes** | Check the check boxes next to the nodes for which you want to generate the certificate. To generate a CSR for select nodes in the deployment, you must uncheck the Allow Wildcard Certificates option. |
| **Common Name (CN)** | By default, the common name is the FQDN of the ISE-PIC node for which you are generating the certificate signing request. $FQDN$ denotes the FQDN of the ISE-PIC node. When you generate certificate signing requests for multiple nodes in the deployment, the Common Name field in the certificate signing requests is replaced with the FQDN of the respective ISE nodes. |
| **Organizational Unit (OU)** | Organizational Unit name. For example, Engineering. |
| **Organization (O)** | Organization name. For example, Cisco. |
| **City (L)** | (Do not abbreviate) City name. For example, San Jose. |
| **State (ST)** | (Do not abbreviate) State name. For example, California. |
| **Country (C)** | Country name. You must enter the two-letter ISO country code. For example, US. |

| Field | Usage Guidelines |
|---|---|
| **Subject Alternative Name (SAN)** | An IP address, DNS name, Uniform Resource Identifier (URI), or Directory Name that is associated with the certificate.<br>• **DNS Name**: If you choose the DNS name, enter the fully qualified domain name of the ISE-PIC node. If you have enabled the Allow Wildcard Certificates option, specify the wildcard notation (an asterisk and a period before the domain name). For example, *.amer.example.com.<br>• **IP Address**: IP address of the ISE-PIC node to be associated with the certificate.<br>• **Uniform Resource Identifier**: A URI that you want to associate with the certificate.<br>• **Directory Name**: A string representation of distinguished name(s) (DNs) defined per RFC 2253. Use a comma (,) to separate the DNs. For "dnQualifier" RDN, escape the comma and use backslash-comma "\," as separator. For example, CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL |
| **Key Type** | Specify the algorithm to be used for creating the public key: RSA or ECDSA. |
| **Key Length** | Specify the bit size for the public key.<br>The following options are available for RSA:<br>• 512<br>• 1024<br>• 2048<br>• 4096<br>The following options are available for ECDSA:<br>• 256<br>• 384<br>**Note**<br>RSA and ECDSA public keys might have different key length for the same security level.<br>Choose 2048 or greater if you plan to get a public CA-signed certificate or deploy Cisco ISE-PIC as a FIPS-compliant policy management system. |
| **Digest to Sign With** | Choose one of the following hashing algorithm: SHA-1 or SHA-256. |
| **Certificate Policies** | Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs. |

# Cisco ISE CA Service

Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). ISE-PIC can act as an external Certificate Authority (CA) for pxGrid, digitally signing the pxGrid certificate. A CA-signed digital certificate is considered industry standard and more secure. The ISE-PIC CA offers the following functionalities:

- Certificate Issuance: Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to your network.
- Key Management: Generates and securely stores keys and certificates.
- Certificate Storage: Stores certificates issued to users and devices.
- Online Certificate Status Protocol (OCSP) Support: Provides an OCSP responder to check for the validity of certificates.

When a CA Service is disabled on the primary administrative node, the CA service is still seen as running on the secondary administration node's CLI. Ideally, the CA service should be seen as disabled. This is a known Cisco ISE issue.



**Note** When Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are used as the admin certificates for ISE nodes, the ISE CA cannot issue new client certificates.

# Elliptical Curve Cryptography Certificates Support

Cisco ISE-PIC CA service supports certificates that are based on Elliptical Curve Cryptography (ECC) algorithms. ECC offers more security and better performance than other cryptographic algorithms even when using a much smaller key size.

The following table compares the key sizes of ECC and RSA and security strength.

| ECC Key Size (in bits) | RSA Key Size (in bits) |
|---|---|
| 160 | 1024 |
| 224 | 2048 |
| 256 | 3072 |
| 384 | 7680 |
| 521 | 15360 |

Because of the smaller key size, encryption is quicker.

Cisco ISE-PIC supports the following ECC curve types. The higher the curve type or key size, the greater is the security.

- P-192
- P-256
- P-384
- P-521

ISE-PIC does not support explicit parameters in the EC part of a certificate. If you try to import a certificate with explicit parameters, you get the error: Validation of certificate failed: Only named ECParameters supported.

You can generate ECC certificates from the Certificate Provisioning Portal.

# Cisco ISE-PIC Certificate Authority Certificates

The Certificate Authority (CA) Certificates page lists all the certificates related to the internal Cisco ISE-PIC CA. These certificates are listed node wise in this page. You can expand a node to view all the ISE-PIC CA certificates of that particular node. The Primary and Secondary Administration nodes have the root CA, node CA, subordinate CA, and OCSP responder certificates. The other nodes in the deployment have the endpoint subordinate CA and OCSP certificates.

When you enable the Cisco ISE-PIC CA service, these certificates are generated and installed on all the nodes automatically. Also, when you replace the entire ISE-PIC Root CA Chain, these certificates are regenerated and installed on all the nodes automatically. There is no manual intervention required.

The Cisco ISE-PIC CA certificates follow the following naming convention: **Certificate Services** <***Endpoint Sub CA/Node CA/Root CA/OCSP Responder***>-<*node_hostname*>#*certificate_number*.

From the CA Certificates page, you can edit, import, export, delete, and view the Cisco ISE-PIC CA certificates.

## Edit a Cisco ISE-PIC CA Certificate

After you add a certificate to the Cisco ISE-PIC CA Certificates Store, you can further edit it by using the edit settings.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**.

**Step 2** Check the check box next to the certificate that you want to edit, and click **Edit**.

**Step 3** Modify the editable fields as required. See Trusted Certificate Settings, on page 97 for a description of the fields.

**Step 4** Click **Save** to save the changes you have made to the certificate store.

## Export a Cisco ISE CA Certificate

To export the Cisco ISE root CA and node CA certificates:

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**.

**Step 2** Check the check box next to the certificate that you want to export, and click **Export**. You can export only one certificate at a time.

**Step 3** Save the privacy-enhanced mail file to the file system that is running your client browser.

# Import a Cisco ISE-PIC CA Certificate

If a client tries to authenticate to your network using a certificate issued by Cisco ISE-PIC CA from another deployment, you must import the Cisco ISE-PIC root CA, node CA, and endpoint sub CA certificates from that deployment in to the Cisco ISE-PIC Trusted Certificates store.

### Before you begin

- Export the ISE-PIC root CA, node CA, and endpoint sub CA certificates from the deployment where the endpoint certificate is signed and store it on the file system of the computer where your browser is running.

### Procedure

**Step 1** Choose **Certificates** > **Trusted Certificates**.

**Step 2** Click **Import**.

**Step 3** Configure the field values as necessary. See Trusted Certificate Import Settings, on page 87 for more information.

If client certificate-based authentication is enabled, then Cisco ISE-PIC will restart the application server on each node in your deployment, starting with the application server on the PAN.

# Trusted Certificate Settings

The following table describes the fields in the **Edit** window of a Trusted Certificate. Edit the CA certificate attributes in this window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**. Check the check box for the Trusted Certificate you want to edit, and click **Edit**.

***Table 19: Trusted Certificate Edit Settings***

| Field Name | Usage Guidelines |
|---|---|
| Certificate Issuer | |
| **Friendly Name** | Enter a friendly name for the certificate. This is an optional field. If you do not enter a friendly name, a default name is generated in the following format:<br>*common-name#issuer#nnnnn* |
| **Status** | Choose **Enabled** or **Disabled** from the drop-down list. If the certificate is disabled, Cisco ISE will not use the certificate for establishing trust. |
| **Description** | (Optional) Enter a description. |
| Usage | |
| **Trust for authentication within ISE** | Check this check box if you want this certificate to verify server certificates (from other Cisco ISE nodes or LDAP servers). |

| Field Name | Usage Guidelines |
|---|---|
| **Trust for client authentication and Syslog** | (Applicable only if you check the **Trust for authentication within ISE** check box) Check the check box if you want this certificate to be used to:<br>• Authenticate endpoints that connect to Cisco ISE using the EAP protocol.<br>• Trust a Syslog server. |
| **Trust for certificate based admin authentication** | You can check this check box only when **Trust for client authentication and Syslog** is selected.<br>Check this check box to enable usage for certificate-based authentications for admin access. Import the required certificate chains into the Trusted Certificate store. |
| **Trust for authentication of Cisco Services** | Check this check box if you want this certificate to be used to trust external Cisco services such as the Feed Service. |
| **Certificate Status Validation** | Cisco ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first way is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second way is to validate the certificate against a CRL which is downloaded from the CA into Cisco ISE. Both of these methods can be enabled, in which case OCSP is used first and only if a status determination cannot be made then the CRL is used. |
| **Validate Against OCSP Service** | Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box. |
| **Reject the request if OCSP returns UNKNOWN status** | Check the check box to reject the request if certificate status is not determined by the OCSP service. If you check this check box, an unknown status value that is returned by the OCSP service causes Cisco ISE to reject the client or server certificate currently being evaluated. |
| **Reject the request if OCSP Responder is unreachable** | Check the check box for Cisco ISE to reject the request if the OCSP Responder is not reachable. |
| **Download CRL** | Check the check box for the Cisco ISE to download a CRL. |
| **CRL Distribution URL** | Enter the URL to download the CRL from a CA. This field is automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.” |
| **Retrieve CRL** | The CRL can be downloaded automatically or periodically. Configure the time interval between downloads. |
| **If download failed, wait** | Configure the time interval that Cisco ISE must wait. Cisco ISE tries to download the CRL again. |
| **Bypass CRL Verification if CRL is not Received** | Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file. |

| Field Name | Usage Guidelines |
|---|---|
| **Ignore that CRL is not yet valid or expired** | Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL.<br><br>Uncheck this check box if you want Cisco ISE to check the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected. |

**Related Topics**

Trusted Certificates Store, on page 81
Edit a Trusted Certificate, on page 85

# Backup and Restoration of Cisco ISE-PIC CA Certificates and Keys

You must back up the Cisco ISE-PIC CA certificates and keys securely to be able to restore them back on a Secondary Administration Node in case of a PAN failure and you want to promote the Secondary Administration Node to function as the root CA or intermediate CA of an external PKI. The Cisco ISE-PIC configuration backup does not include the CA certificates and keys. Instead, you should use the Command Line Interface (CLI) to export the CA certificates and keys to a repository and to import them. The **application configure ise** command now includes export and import options to backup and restore CA certificates and keys.

The following certificates from the Trusted Certificates Store are restored on the Secondary Administration Node:

- Cisco ISE Root CA certificate
- Cisco ISE Sub CA certificate
- Cisco ISE Endpoint RA certificate
- Cisco ISE OCSP Responder certificate

You must back up and restore Cisco ISE CA certificates and keys when you:

- Have a Secondary Administration Node in the deployment
- Replace the entire Cisco ISE-PIC CA root chain
- Configure Cisco ISE-PIC root CA to act as a subordinate CA of an external PKI
- Restore data from a configuration backup. In this case, you must first regenerate the Cisco ISE-PIC CA root chain and then back up and restore the ISE CA certificates and keys.

**Note** Whenever the Cisco ISE internal CA is replaced in a deployment, then the ISE messaging service must also be refreshed that time to retrieve the complete certificate chain.

# Export Cisco ISE CA Certificates and Keys

You must export the CA certificates and keys from the PAN to import them on the Secondary Administration Node. This option enables the Secondary Administration Node to issue and manage certificates for endpoints when the PAN is down and you promote the Secondary Administration Node to be the PAN.

### Before you begin

Ensure that you have created a repository to store the CA certificates and keys.

### Procedure

**Step 1** Enter **application configure ise** command from the Cisco ISE CLI.

**Step 2** Enter 7 to export the certificates and keys.

**Step 3** Enter the repository name.

**Step 4** Enter an encryption key.

A success message appears with the list of certificates that were exported, along with the subject, issuer, and serial number.

**Example:**

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

# Import Cisco ISE-PIC CA Certificates and Keys

After you register the Secondary Administration Node, you must export the CA certificates and keys from the PAN and import them in to the Secondary Administration Node.

### Procedure

**Step 1** Enter **application configure ise** command from the Cisco ISE-PIC CLI.

**Step 2** Enter 8 to import the CA certificates and keys.

**Step 3** Enter the repository name.

**Step 4** Enter the name of the file that you want to import. The file name should be in the format **ise_ca_key_pairs_of_<vm hostname>**.

**Step 5** Enter the encryption key to decrypt the file.

A success message appears.

**Example:**

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

# Generate Root CA and Subordinate CAs

When you set up the deployment, Cisco ISE-PIC generates a root CA on the node. However, when you change the domain name or the hostname of the node, you must regenerate root CA on the primary PAN and sub CAs on the PSNs respectively.

**Note** PXgrid and IMS certificates will not be replaced by Internal CA while regenerating root CA if the respective certificate is externally signed.

If you want to change the signing by Internal CA for PXgrid certificate, generate a self-signed Pxgrid certificate and regenerate the root CA.

If you want to change the signing by Internal CA for Cisco ISE Messaging Services certificate, regenerate the Cisco ISE Messaging Services certificate from the CSR page.

**Procedure**

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **Certificate Signing Requests**.

**Step 2** Click **Generate Certificate Signing Requests (CSR)**.

**Step 3** Choose ISE Root CA from the **Certificate(s) will be used for** drop-down list.

**Step 4** Click **Replace ISE Root CA Certificate chain**.

The root CA and subordinate CA certificates get generated for all the nodes in your deployment.

## Configure Cisco ISE-PIC Root CA as Subordinate CA of an External PKI

If you want the root CA on the primary PAN to act as a subordinate CA of an external PKI, generate an ISE-PIC intermediate CA certificate signing request, send it to the external CA, obtain the root and CA-signed certificates, import the root CA certificate in to the Trusted Certificates Store, and bind the CA-signed certificate to the CSR. In this case, the external CA is the root CA, the node is a subordinate CA of the external CA, and the PSNs are subordinate CAs of the node.

### Procedure

**Step 1** Choose **Certificates** > **Certificate Signing Requests**.

**Step 2** Click **Generate Certificate Signing Requests (CSR)**.

**Step 3** Choose ISE Intermediate CA from the **Certificate(s) will be used for** drop-down list.

**Step 4** Click **Generate**.

**Step 5** Export the CSR, send it to the external CA, and obtain the CA-signed certificate.

**Step 6** Import the root CA certificate from the external CA in to the Trusted Certificates store.

**Step 7** Bind the CA-signed certificate with the CSR.

# OCSP Services

The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the Certificate Revocation List (CRL) and addresses issues that result in handling CRLs.

Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications. The OCSP configuration is configured in a reusable configuration object that can be referenced from any certificate authority (CA) certificate that is configured in Cisco ISE.

You can configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP. If a communication problem is detected with both the primary and secondary OCSP servers, or if an unknown status is returned for a given certificate, Cisco ISE switches to checking the CRL.

## Cisco ISE CA Service Online Certificate Status Protocol Responder

The Cisco ISE CA OCSP responder is a server that communicates with OCSP clients. The OCSP clients for the Cisco ISE CA include the internal Cisco ISE OCSP client and OCSP clients on the Adaptive Security Appliance (ASA). The OCSP clients should communicate with the OCSP responder using the OCSP request/response structure defined in RFC 2560, 5019.

The Cisco ISE CA issues a certificate to the OCSP responder. The OCSP responder listens on port 2560 for any incoming requests. This port is configured to allow only OCSP traffic.

The OCSP responder accepts a request that follows the structure defined in RFC 2560, 5019. Nonce extension is supported in the OCSP request. The OCSP responder obtains the status of the certificate and creates an OCSP response and signs it. The OCSP response is not cached on the OCSP responder, although you can cache the OCSP response on the client for a maximum period of 24 hours. The OCSP client should validate the signature in the OCSP response.

The self-signed CA certificate (or the intermediate CA certificate if ISE acts as an intermediate CA of an external CA) on the PAN issues the OCSP responder certificate. This CA certificate on the PAN issues the OCSP certificates on the PAN and PSNs. This self-signed CA certificate is also the root certificate for the entire deployment. All the OCSP certificates across the deployment are placed in the Trusted Certificates Store for ISE to validate any response signed using these certificates.



**Note** Cisco ISE receives from OCSP responder servers a thisUpdate value, which indicates the time since the last certificate revocation. If the thisUpdate value is greater than 7 days, the OCSP certificate verification fails in Cisco ISE.

# OCSP Certificate Status Values

OCSP services return the following values for a given certificate request:

- Good—Indicates a positive response to the status inquiry. It means that the certificate is not revoked, and the state is good only until the next time interval (time to live) value.
- Revoked—The certificate was revoked.
- Unknown—The certificate status is unknown. OCSP service returns this value if the certificate was not issued by the CA of this OCSP responder.
- Error—No response was received for the OCSP request.

# OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, and they are called primary and secondary OCSP servers. Each OCSP server configuration contains the following parameters:

- URL—The OCSP server URL.
- Nonce—A random number that is sent in the request. This option ensures that old communications cannot be reused in replay attacks.
- Validate response—Cisco ISE validates the response signature that is received from the OCSP server.

In case of timeout (which is 5 seconds), when Cisco ISE communicates with the primary OCSP server, it switches to the secondary OCSP server.

Cisco ISE uses the secondary OCSP server for a configurable amount of time before attempting to use the primary server again.

# OCSP Failures

The three general OCSP failure scenarios are as follows:

- Failed OCSP cache or OCSP client side (Cisco ISE) failures.
- Failed OCSP responder scenarios, for example:

  The first primary OCSP responder not responding, and the secondary OCSP responder responding to the Cisco ISE OCSP request.

  Errors or responses not received from Cisco ISE OCSP requests.

  An OCSP responder may not provide a response to the Cisco ISE OCSP request or it may return an OCSP Response Status as not successful. OCSP Response Status values can be as follows:

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

    There are many date-time checks, signature validity checks and so on, in the OCSP request. For more details, refer to *RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* which describes all the possible states, including the error states.

- Failed OCSP reports

# Add OCSP Client Profiles

You can use the OCSP Client Profile page to add new OCSP client profiles to Cisco ISE.

### Before you begin

If the Certificate Authority (CA) is running the OCSP service on a nonstandard port (other than 80 or 443), you must configure ACLs on the switch to allow for communication between Cisco ISE and the CA on that port. For example:

**permit tcp** <*source ip*> <*destination ip*> **eq** <*OCSP port number*>

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Certificates** > **OCSP Client Profile**.

**Step 2** Enter the values to add an OCSP Client Profile.

**Step 3** Click **Submit**.

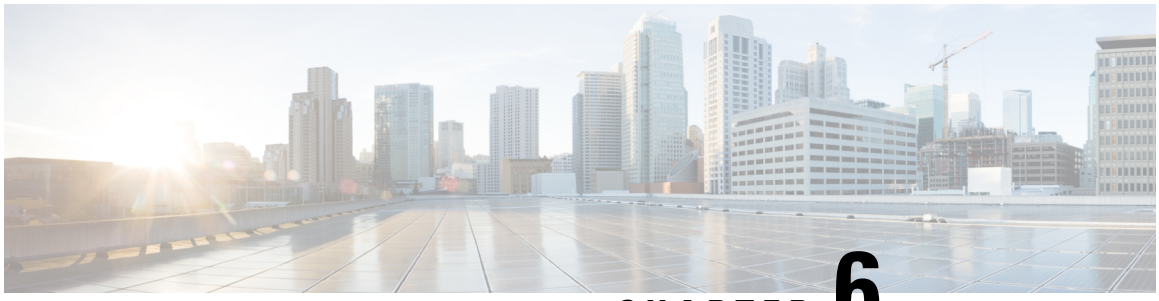
# OCSP Statistics Counters

Cisco ISE uses OCSP counters to log and monitor the data and health of the OCSP servers. Logging occurs every five minutes. Cisco ISE sends a syslog message to the Monitoring node and it is preserved in the local store. The local store contains data from the previous five minutes. After Cisco ISE sends the syslog message, the counters are recalculated for the next interval. This means, after five minutes, a new five-minute window interval starts again.

The following table lists the OCSP syslog messages and their descriptions.

***Table 20: OCSP Syslog Messages***

| Message | Description |
|---|---|
| OCSPPrimaryNotResponsiveCount | The number of nonresponsive primary requests |
| OCSPSecondaryNotResponsiveCount | The number of nonresponsive secondary requests |
| OCSPPrimaryCertsGoodCount | The number of ‘good’ certificates that are returned for a given CA using the primary OCSP server |
| OCSPSecondaryCertsGoodCount | The number of ‘good’ statuses that are returned for a given CA using the primary OCSP server |
| OCSPPrimaryCertsRevokedCount | The number of ‘revoked’ statuses that are returned for a given CA using the primary OCSP server |
| OCSPSecondaryCertsRevokedCount | The number of ‘revoked’ statuses that are returned for a given CA using the secondary OCSP server |
| OCSPPrimaryCertsUnknownCount | The number of ‘Unknown’ statuses that are returned for a given CA using the primary OCSP server |
| OCSPSecondaryCertsUnknownCount | The number of ‘Unknown’ statuses that are returned for a given CA using the secondary OCSP server |
| OCSPPrimaryCertsFoundCount | The number of certificates that were found in cache from a primary origin |
| OCSPSecondaryCertsFoundCount | The number of certificates that were found in cache from a secondary origin |
| ClearCacheInvokedCount | How many times clear cache was triggered since the interval |
| OCSPCertsCleanedUpCount | How many cached entries were cleaned since the t interval |
| NumOfCertsFoundInCache | Number of the fulfilled requests from the cache |
| OCSPCacheCertsCount | Number of certificates that were found in the OCSP cache |



CHAPTER 6

# Administer ISE-PIC


- Manage ISE-PIC Nodes, on page 107
- Manage the ISE-PIC Installation, on page 112
- Manage Settings in ISE-PIC, on page 133


# Manage ISE-PIC Nodes

Add or remove the secondary node, synchronize data between nodes, promote the secondary node to be the primary node, and more.

## Cisco ISE-PIC Deployment Setup

After you install Cisco ISE-PIC on all your nodes, as described in the *Cisco Identity Services Engine Hardware Installation Guide*, the nodes come up in a standalone state. You must then define one node as your Primary Administration Node (PAN) and register the secondary node to the PAN.

All Cisco ISE-PIC system and functionality-related configurations should be done only on the PAN. The configuration changes that you perform on the PAN are replicated to the secondary node in your deployment. From the secondary node, the only action you can perform is to promote that secondary node to become the PAN.

After you have registered the secondary node to the PAN, while logging in to the Admin portal of that secondary node, you must use the login credentials of the PAN.

## Data Replication from Primary to Secondary ISE-PIC Nodes

When you register an Cisco ISE node as a secondary node, Cisco ISE-PIC immediately creates a data replication channel from the primary to the secondary node and begins the process of replication. Replication is the process of sharing Cisco ISE-PIC configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data present in the two Cisco ISE-PIC nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE-PIC node as a secondary node. Incremental replication occurs after a full replication and ensures that any new changes such as additions, modifications, or deletions to the configuration data in the PAN are reflected in the secondary nodes. The process of replication ensures that the Cisco ISE-PIC nodes in a deployment are in sync. You can view the status of replication in the Node Status column from the deployment pages of the Cisco ISE-PIC admin portal. When you register a

Cisco ISE-PIC node as a secondary node or perform a manual synchronization with the PAN, the node status shows an orange icon indicating that the requested action is in progress. Once it is complete, the node status turns green indicating that the secondary node is synchronized with the PAN.

# Effects of modifying nodes in Cisco ISE-PIC

When you make any of the following changes to a node in a Cisco ISE-PIC, that node restarts, which causes a delay:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Change a primary node to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Promote an node (Secondary to Primary)
- Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes



**Note** When you promote the secondary Administration node to the primary PAN position, the primary node will assume a secondary role. This causes both the primary and secondary nodes to restart, causing a delay.

# Guidelines for Setting Up Two Nodes in a Deployment

Read the following statements carefully before you set up Cisco ISE-PIC with two nodes.

- Choose the same Network Time Protocol (NTP) server for both the nodes. To avoid timezone issues among the nodes, you must provide the same NTP server name during the setup of each node. This setting ensures that the reports and logs from the various nodes in your deployment are always synchronized with timestamps.
- Configure the Cisco ISE-PIC Admin password when you install Cisco ISE-PIC. The previous Cisco ISE-PIC Admin default login credentials (admin/cisco) are no longer valid. Use the username and password that was created during the initial setup or the current password if it was changed later.
- Configure the Domain Name System (DNS) server. Enter the IP addresses and fully qualified domain names (FQDNs) of both the Cisco ISE-PIC nodes that are part of your deployment in the DNS server. Otherwise, node registration will fail.
- Configure the forward and reverse DNS lookup for both Cisco ISE-PIC nodes in your high-availability deployment from the DNS server. Otherwise, you may run into deployment related issues when registering and restarting Cisco ISE-PIC nodes. Performance might be degraded if reverse DNS lookup is not configured for both of the nodes.
- (Optional) Deregister a secondary Cisco ISE-PIC node from the PAN to uninstall Cisco ISE-PIC from it.
- Ensure that the PAN and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE-PIC.

# View Nodes in a Deployment

In the **Deployment Nodes** window, you can view the ISE-PIC nodes, primary and secondary, that are a part of your deployment.

### Procedure

**Step 1** Log in to the primary Cisco ISE-PIC Admin portal.

**Step 2** Choose **Administration** > **Deployment**.

All the Cisco ISE nodes that are part of your deployment are listed.

# Register a Secondary Cisco ISE-PIC Node

After you register the secondary node, the configuration of the secondary node is added to the database of the primary node and the application server on the secondary node is restarted. After the restart is complete, you can view all the configuration changes that you make from the Deployment page of the PAN. However, expect a delay of 5 minutes for your changes to take effect and appear on the Deployment page.

### Procedure

**Step 1** Log in to the PAN.

**Step 2** Choose **Administration** > **Deployment**.
If no secondary node is registered in the deployment then the **Add Secondary Node** section appears at the bottom of the page.

**Step 3** From the **Add Secondary Node** section, enter the DNS-resolvable hostname of the secondary Cisco ISE node.

If you are using the hostname while registering the Cisco ISE-PIC node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com,* must be DNS-resolvable from the PAN. Otherwise, node registration fails. You must have previously defined the IP address and the FQDN of the secondary node in the DNS server.

**Step 4** Enter a UI-based administrator credential for the standalone node in the Username and Password fields.

**Step 5** Click **Save**.

Cisco ISE-PIC contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it.

When the secondary node is registered to the deployment, the node is restarted, which may take up to 5 minutes before the secondary node information is displayed from the Deployment page.

Once the secondary node is registered successfully, the Deployment page displays the details for that node in the **Secondary Node** section.

After a secondary node is registered successfully, you will receive an alarm on your PAN that confirms a successful node registration. If the secondary node fails to register with the PAN, the alarm is not generated. When a node is registered, the application server on that node is restarted. After successful registration and database synchronization, enter the credentials of the primary administrative node to log in to the user interface of the secondary node.



**Note** In addition to the existing Primary node in the deployment, when you successfully register a new node, no alarm corresponding to the newly registered node is displayed. The Configuration Changed alarms reflect information corresponding to the newly registered nodes. You can use this information to ascertain the successful registration of the new node.

# Synchronize Primary and Secondary Cisco ISE-PIC Nodes

You can make configuration changes to Cisco ISE-PIC only through the primary PAN. The configuration changes get replicated to all the secondary nodes. If, for some reason, this replication does not occur properly, you can manually synchronize the secondary PAN with the primary PAN.

### Procedure

**Step 1** Log in to the primary PAN.

**Step 2** Choose **Administration** > **Deployment**.

**Step 3** Check the check box next to the node that you want to synchronize with the primary PAN, and click **Syncup** to force a full database replication.

# Manually Promote Secondary PAN to Primary

If the Primary PAN fails you must manually promote the Secondary PAN to become the new Primary PAN.

### Before you begin

Ensure that you have a second Cisco ISE-PIC node configured to promote as your Primary PAN.

### Procedure

**Step 1** Log in to the Secondary PAN GUI.

**Step 2** Choose **Administration** > **Deployment**.

**Step 3** lick **Promote to Primary**.

If the node that was originally the Primary PAN, comes back up, it will be demoted automatically and become the Secondary PAN. You must perform a manual synchronization on this node (that was originally the Primary PAN) to bring it back into the deployment.

**Step 4** Click **Save**.

# Remove a Node from Deployment

To remove a node from a deployment, you must deregister it. The deregistered node becomes a standalone Cisco ISE-PIC node.

When a node is deregistered, the endpoint data is lost. If you want the node to retain the endpoint data after it becomes a standalone node, you can obtain a backup from the primary PAN and restore this data backup on it.

You can view these changes in the **Deployment** window of the primary PAN. However, expect a delay of five minutes for the changes to take effect and appear in the **Deployment** window.

### Before you begin

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the PAN, the status of the deregistered node changes to standalone and the connection between the primary and the secondary node will be lost. Replication updates are no longer sent to the deregistered standalone node.

Before you remove a secondary node from a deployment, perform a backup of Cisco ISE-PIC configuration, which you can then restore later, if needed.

### Procedure

**Step 1** Choose **Administration** > **Deployment**.

**Step 2** Click **Deregister**, located next to the secondary node details.

**Step 3** Click **OK**.

**Step 4** Verify the receipt of an alarm on your primary PAN to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the primary PAN, it means the alarm is not generated.

# Change the Hostname or IP Address of a Cisco ISE-PIC Node

You can change the hostname, IP address, or domain name of standalone Cisco ISE-PIC nodes. However, you cannot use **localhost** as the hostname for a node.

### Before you begin

If a Cisco ISE-PIC node is a part of a two-node deployment, you must first remove it from the deployment and ensure that it is a standalone node.

**Procedure**

**Step 1** Change the hostname or IP address of the Cisco ISE-PIC node using the **hostname**, **ip address,** or **ip domain-name** command from the Cisco ISE CLI.

**Step 2** Reset the Cisco ISE-PIC application configuration using the **application stop ise** command from the Cisco ISE CLI to restart all the services.

**Step 3** Register the Cisco ISE-PIC node to the primary PAN if it is a part of a two-node deployment.

**Note**
If you are using the hostname while registering the Cisco ISE-PIC node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com*, must be DNS-resolvable from the primary PAN. Otherwise, node registration fails. You must enter the IP addresses and FQDNs of the Cisco ISE-PIC nodes that are a part of your deployment in the DNS server.

After you register the Cisco ISE-PIC node as a secondary node, the primary PAN replicates the change in the IP address, hostname, or domain name to the other Cisco ISE-PIC nodes in your deployment.

# Replace the Cisco ISE-PIC Appliance Hardware

You should replace the Cisco ISE-PIC appliance hardware only if there is an issue with the hardware. For any software issues, you can reimage the appliance and reinstall the Cisco ISE-PIC software.

**Procedure**

**Step 1** Re-image or re-install the Cisco ISE-PIC software on the new nodes.

**Step 2** Obtain a license with the UDI for the Primary and Secondary PANs and install it on the Primary PAN.

**Step 3** Restore the backup on the replaced Primary PAN.

The restore script will try to sync the data on the Secondary PAN, but the Secondary PAN is now a standalone node and the sync will fail. Data is set to the time the backup was taken on the Primary PAN.

**Step 4** Register the new node as a secondary server with the Primary PAN.

# Manage the ISE-PIC Installation

Install patches, run backups or implement a system restoration.

# Install a software patch

**Procedure**

**Step 1** Choose **Administration** > **Maintenance** > **Patch Management** and click **Install.**

**Step 2** Click **Browse** and choose the patch that you downloaded from Cisco.com.

**Step 3** Click **Install** to install the patch.

After the patch is installed on the PAN, Cisco ISE-PIC logs you out and you have to wait for a few minutes before you can log in again.

**Note**
When patch installation is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

**Step 4** Choose **Administration** > **Maintenance** > **Patch Management** to return to the Patch Installation page.

**Step 5** Click the radio button next to the patch that you have installed and click **Show Node Status** to verify whether installation is complete.

## Cisco ISE-PIC software patches

Cisco ISE-PIC software patches are always cumulative. Cisco ISE-PIC allows you to perform patch installation and rollback from CLI or GUI.

You can install patches on Cisco ISE-PIC servers in your deployment from the Primary PAN. To install a patch from the Primary PAN, you must download the patch from Cisco.com to the system that runs your client browser.

If you install the patch using the GUI, the system installs the patch on the Primary PAN first. The system installs the patch on the remaining nodes in the deployment according to the order shown in the GUI. You cannot change the update order. You can also manually install patches, roll back patches, and view patch versions. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administrator > System > Maintenance > Patch management**.

When you install the patch from the CLI, you can control the update order for the nodes. However, we recommend installing the patch on the Primary PAN first. The installation order for the other nodes does not matter. You can install the patch on multiple nodes at the same time to speed up the process.

To validate the patch on specific nodes before upgrading the entire deployment, use the CLI to install the patch on those nodes.

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

For more information, see the "Install Patch" section in the "Cisco ISE CLI Commands in EXEC Mode" chapter in Cisco Identity Services Engine CLI Reference Guide.

You can install the required patch version directly. For example, if you are using Cisco ISE release 2.x and want to install patch 5, you can install patch 5 without installing patches 1 through 4.

To view the current patch version in the CLI, use this command:

```
show version
```

## Software patch installation guidelines

When you install a patch on a Cisco ISE node, the node is rebooted after the installation is complete. You might have to wait for a few minutes before you can log in again. You can schedule patch installations during a maintenance window to avoid temporary outage.

Ensure that you install patches that are applicable for the Cisco ISE-PIC version that is deployed in your network. Cisco ISE-PIC reports any mismatch in versions as well as any errors in the patch file.



**Note** Cisco ISE patches can be installed on ISE-PIC as well.

You cannot install a patch with a version that is lower than the patch that is currently installed on Cisco ISE-PIC. Similarly, you cannot roll back changes of a lower-version patch if a higher version is currently installed on Cisco ISE-PIC. For example, if patch 3 is installed on your Cisco ISE-PIC servers, you cannot install or roll back patch 1 or 2.

When you install a patch from the Primary PAN that is part of a two-node deployment, Cisco ISE-PIC installs the patch on the primary node and then on the secondary node. If the patch installation is successful on the Primary PAN, Cisco ISE-PIC then continues patch installation on the secondary node. If it fails on the Primary PAN, the installation does not proceed to the secondary node.

# Roll back software patches

When you roll back a patch from the PAN in a deployment with multiple nodes, Cisco ISE-PIC rolls back the patch on the primary node and then on the secondary node in the deployment.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Administration** > **Maintenance** > **Patch Management**.

**Step 2** Select the patch version that you want to roll back, then click **Rollback**.

**Note**
When a patch rollback is in progress, only the **Show Node Status** function is accessible on the Patch Management page.

After Cisco ISE rolls back the patch from the PAN, you are logged out. Wait a few minutes before you log in again

**Step 3** After you log in, click the **Alarms** link at the bottom of the page to view the status of the rollback operation.

**Step 4** To view the progress of the patch rollback, choose the patch in the Patch Management page and click **Show Node Status**.

**Step 5** Select the patch and click **Show Node Status** on a secondary node to ensure the patch is rolled back from all nodes in your deployment.

If the patch is not rolled back from any secondary node, ensure the node is operational. Repeat this process to roll back changes from any remaining nodes. Cisco ISE-PIC rolls back the patch only from nodes that still have this version of the patch installed.

## Software patch rollback guidelines

To roll back a patch from Cisco ISE-PIC nodes in a deployment, you must first roll back the change from the PAN. If this is successful, the patch is then rolled back from the secondary node. If the rollback process fails on the PAN, the patches are not rolled back from the secondary node.

While Cisco ISE-PIC rolls back the patch from the secondary node, you can continue to perform other tasks from the PAN GUI. The secondary node will be restarted after the rollback.

# Backup and Restore Data



**Note** Cisco ISE-PIC functions in many cases identically to the Cisco ISE backup and restore procedures, and therefore, the term Cisco ISE may occassionally be used interchangeably to indicate operations and features relevant for Cisco ISE-PIC.

Cisco ISE-PIC allows you to back up data from the primary or standalone node. Backup can be done from the CLI or user interface.

Cisco ISE-PIC allows you to back up the following type of data:

- Configuration data—Contains both application-specific and Cisco ADE operating system configuration data.
- Operational Data—Contains monitoring and troubleshooting data.

## Backup and Restore Repositories

Cisco ISE-PIC allows you to create and delete repositories. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

You can create the repository type as CD-ROM for the virtual CD-ROM created using the KVM.



**Note** Repositories are local to each device.



**Note** We recommend that you have a repository size of 10 GB for small deployments (100 endpoints or less), 100 GB for medium deployments, and 200 GB for large deployments.

# Create Repositories

You can use the CLI and GUI to create repositories. We recommend that you use the GUI due to the following reasons:

- Repositories that are created through the CLI are saved locally and do not get replicated to the other deployment nodes. These repositories do not get listed in the GUI's repository page.
- Repositories that are created on the primary PAN get replicated to the other deployment nodes.

The keys are generated only at the primary PAN on GUI, and so during upgrade you need to generate the keys again at GUI of new primary admin and export it to the SFTP server. If you remove the nodes from your deployment, you need to generate the keys on GUI of non-admin nodes and export it to the SFTP server.

You can configure an SFTP repository in Cisco ISE-PIC with RSA public key authentication. Instead of using an administrator-created password to encrypt the database and logs, you can choose the RSA public key authentication that uses secure keys. In case of SFTP repository created with RSA public key, the repositories created through the GUI do not get replicated in the CLI and the repositories created through the CLI do not get replicated in the GUI. To configure same repository on the CLI and GUI, generate RSA public keys on both CLI and GUI and export both the keys to the SFTP server.



**Note** Cisco ISE initiates outbound SSH or SFTP connections in FIPS mode even if FIPS mode is not enabled on ISE. Ensure that the remote SSH or SFTP servers that communicate with ISE allow FIPS 140 approved cryptographic algorithms.

Cisco ISE uses embedded FIPS 140 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.

### Before you begin

- If you want to create an SFTP repository with RSA public key authentication, perform the following steps:
  - Enable RSA public key authentication in the SFTP repository.
  - You must log in as the Admin CLI user. Enter the host key of the SFTP server from the Cisco ISE CLI using the **crypto host_key add** command. The host key string should match the hostname that you enter in the **Path** field of the repository configuration page.
  - Generate the key pairs and export the public key to your local system from the GUI. From the Cisco ISE CLI, generate the key pairs using the **crypto key generate rsa passphrase** *test123* command, where, passphrase must be greater than 13 letters, and export the keys to any repository (local disk or any other configured repository).
  - Copy the exported RSA public key to the PKI-enabled SFTP server and add it to the "authorized_keys" file.

**Note** When primary PAN and primary MnT are separate nodes, you can use the **Generate Key Pairs** option in the **Repository List** window to generate RSA keys for both primary PAN and primary MnT nodes. You can use the **Export Public Key** option in the **Repository List** window to export the generated RSA keys from both primary PAN and primary MnT nodes.

### Procedure

**Step 1** Choose **Administration** > **Maintenance** > **Repository**.

**Step 2** Click **Add** to add a new repository.

**Step 3** Enter the values as required to set up new repository. See Repository Settings, on page 117 for a description of the fields.

**Step 4** Click **Submit** to create the repository.

**Step 5** Verify that the repository is created successfully by clicking **Repository** from the **Operations** navigation pane on the left or click the **Repository List** link at the top of **Repository** window to go to the repository listing page.

### What to do next

- Ensure that the repository that you have created is valid. You can do so from the **Repository Listing** window. Select the corresponding repository and click **Validate**. Alternatively, you can execute the following command from the Cisco ISE command-line interface:

  **show repository** *repository_name*

  where *repository_name* is the name of the repository that you have created.

**Note** If the path that you provided while creating the repository does not exist, then you will get the following error:

```
%Invalid Directory
```

- Run an on-demand backup or schedule a backup.

## Repository Settings

The following table describes the fields on the **Repository List** window, which you can use to create repositories to store your backup files. To view this window, click the **Menu** icon (☰) and choose **Administration** > **Maintenance** > **Repository**.

**Note** You may encounter a cURL timeout error when performing an AWS ISE backup using FTP/SFTP with a bandwidth range of 7 to 13 Mbps.

*Table 21: Repository Settings*

| Fields | Usage Guidelines |
|---|---|
| Repository | Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters. |
| Protocol | Choose one of the available protocols that you want to use. |
| Host | (Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IP address (IPv4 or IPv6) of the server where you want to create the repository.<br>**Note**<br>Ensure that the ISE eth0 interface of is configured with an IPv6 address if you are adding a repository with an IPv6 address. |
| Path | Enter the path to your repository. The path must be valid and must exist at the time you create the repository.<br>Note that some of the special characters like !, ?, ~ (that are not included in the list above) are allowed for the FTP and SFTP password configuration via GUI. However, these special characters are not allowed for configuration via CLI or Open API. |

**Related Topics**

Backup and Restore Repositories

Create Repositories, on page 116

## Enable RSA Public Key Authentication in SFTP Repository

In the SFTP server, each node must have two RSA public keys, one each for CLI and for GUI. To enable RSA public key authentication in SFTP repository, perform the following steps:

**Note** After you enable RSA public key authentication in SFTP repository, you will not be able to log in using SFTP credentials. You can either use PKI-based authentication or credential-based authentication. If you want to use credential-based authentication again, you must remove the public key pair from the SFTP server.

### Procedure

**Step 1** Log in to SFTP server with an account that has permission to edit the */etc/ssh/sshd_config.file*.

**Note**
The location of the *sshd_config* file might vary based on the operating system installation.

**Step 2** Enter the **vi /etc/ssh/sshd_config** command.

The contents of the sshd_config file is listed.

**Step 3** Remove the "#" symbol from the following lines to enable RSA public key authentication:

- RSAAuthentication yes

- PubkeyAuthentication yes

**Note**
If Public Auth Key is no, change it to yes.

- AuthorizedKeysFile ~/.ssh/authorized_keys

## On-Demand and Scheduled Backups

You can configure on-demand backups of the primary PAN. Perform an on-demand backup when you want to back up data immediately.

You can schedule system-level backups to run once, daily, weekly, or monthly. Because backup operations can be lengthy, you can schedule them so they are not a disruption. You can schedule a backup from the Admin portal.



**Note** If you are using the internal CA, you should use the CLI to export certificates and keys. Backup using in the administration portal does not back up the CA chain.

For more information, see the "Export Cisco ISE CA Certificates and Keys" section in the "Basic Setup" chapter *Cisco Identity Services Engine Administrator Guide*.

Configurational and operational backups on Cisco ISE can overload your system for a short time. This expected behavior of temporary system overload will depend on the configuration and monitoring database size of your system.

### Perform an On-Demand Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE-PIC to the configuration state that existed at the time of obtaining the backup.

**Important** When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you have to choose from one of these options to avoid errors:

- **Option 1:**

  Export the CA certificates from the source ISE-PIC node through the CLI and import them in to the target system through the CLI

  **Pros:** Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys

  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA

  **Pros:** This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system continues to be trusted

  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued

### Before you begin

- Before you perform an on-demand backup, you should have a basic understanding of the backup data types in Cisco ISE-PIC.
- Ensure that you have created repositories for storing the backup files.
- Do not back up using a local repository.

### Procedure

**Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Administration** > **Maintenance** > **Backup and Restore**

**Step 2** Choose the type of backup: Configuration or Operational

**Step 3** Click **Backup Now**

**Step 4** Enter the values as required to perform a backup

**Step 5** Click **Backup**

**Step 6** Verify that the backup completed successfully

Cisco ISE-PIC appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE-PIC adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository

Do not promote a node when the backup is running. This will shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node changes

**Note**
High CPU usage might be observed and High Load Average alarm might be seen when the backup is running. CPU usage will be back to normal when the backup is complete.

## Schedule a Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE-PIC to the configuration state that existed at the time of obtaining the backup.



**Important** When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**

  Export the CA certificates from the source ISE-PIC node through the CLI and import them in to the target system through the CLI.

  **Pros:** Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA.

  **Pros:** This option is the recommended and clean method, where the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.

  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

### Before you begin

- Before you schedule a backup, you should have a basic understanding of the backup data types in Cisco ISE-PIC.
- Ensure that you have configured repositories.
- Do not back up using a local repository.



**Note** For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

### Backup Using the CLI

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI. However, you can perform operational backup on the secondary monitoring node only from the CLI.

### Backup History

Backup history provides basic information about scheduled and on-demand backups. It lists the name of the backup, backup file size, repository where the backup is stored, and time stamp that indicates when the backup was obtained. This information is available in the Operations Audit report and on the Backup and Restore page in the History table.

For failed backups, Cisco ISE-PIC triggers an alarm. The backup history page provides the failure reason. The failure reason is also cited in the Operations Audit report. If the failure reason is missing or is not clear, you can run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

While the backup operation is in progress, you can use the **show backup status** CLI command to check the progress of the backup operation.

Backup history is stored along with the Cisco ADE operating system configuration data. It remains there even after an application upgrade and are only removed when you reimage the PAN.

### Backup Failures

If backup fails, check the following:

- Check if there is any NTP sync or service failure issue. When the NTP service on Cisco ISE is not working, Cisco ISE raises the NTP Service Failure alarm. When Cisco ISE cannot sync with all the configured NTP servers, Cisco ISE raises the NTP Sync Failure alarm. Cisco ISE backup might fail if the NTP services are down or if there is any sync issue. Check the Alarms dashlet and fix the NTP sync or service issue before you retry the backup operation.
- Make sure that no other backup is running at the same time.
- Check the available disk space for the configured repository.
    - Monitoring (operational) backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your node is allocated 600 GB, and the monitoring data takes up more than 450 GB of storage, then monitoring backup fails.
    - If the database disk usage is greater than 90%, a purge occurs to bring the database size to less than or equal to 75% of its allocated size.
- Verify if a purge is in progress. Backup and restore operations will not work while a purge is in progress.
- Verify if the repository is configured correctly.

# Cisco ISE Restore Operation

You can restore configuration data on a primary or standalone node. After you restore data on the Primary PAN, you must manually synchronize the secondary nodes with the Primary PAN.



**Note** The new backup/restore user interface in Cisco ISE-PIC makes use of meta-data in the backup filename. Therefore, after a backup completes, you should not modify the backup filename manually. If you manually modify the backup filename, the Cisco ISE-PIC backup/restore user interface will not be able to recognize the backup file. If you have to modify the backup filename, you should use the Cisco ISE CLI to restore the backup.

## Guidelines for Data Restoration



**Note**

- From Cisco ISE Release 3.2 and above, Root CA regeneration happens automatically in the restore flow. Thus, Root CA regeneration post config-backup is not required.

Following are guidelines to follow when you restore Cisco ISE-PIC backup data.

- Cisco ISE allows you to obtain a backup from an ISE node (A) and restore it on another ISE node (B), both having the same host names (but different IP addresses). However, after you restore the backup on node B, do not change the hostname of node B because it might cause issues with certificates and portal group tags.
- We recommend that you do not create DNS records for new Cisco ISE nodes if old Cisco ISE deployment nodes are still operational to mitigate DNS resolution conflicts.
- If you obtain a backup from the Primary PAN in one timezone and try to restore it on another Cisco ISE-PIC node in another timezone, the restore process might fail. This failure happens if the timestamp in the backup file is later than the system time on the Cisco ISE-PIC node on which the backup is restored. If you restore the same backup a day after it was obtained, then the timestamp in the backup file is in the past and the restore process succeeds.
- When you restore a backup on the Primary PAN with a different hostname than the one from which the backup was obtained, the Primary PAN becomes a standalone node. The deployment is broken and the secondary nodes become nonfunctional. You must make the standalone node the primary node, reset the configuration on the secondary nodes, and reregister them with the primary node. To reset the configuration on Cisco ISE-PIC nodes, enter the following command from the Cisco ISE CLI:
  - **application reset-config ise**
- We recommend that you do not change the system timezone after the initial Cisco ISE-PIC installation and setup.
- If you changed the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data from the standalone Cisco ISE-PIC node or Primary PAN. Otherwise, if you try to restore data using an older backup, the communication between the nodes might fail.
- After you restore the configuration backup on the Primary PAN, you can import the Cisco ISE CA certificates and keys that you exported earlier.

**Note** If you did not export the Cisco ISE CA certificates and keys, then after you restore the configuration backup on the Primary PAN, generate the root CA and subordinate CAs on the Primary PAN.

- If you are trying to restore a platinum database without using the correct FQDN (FQDN of a platinum database), you need to regenerate the CA certificates. (To view this window, click the **Menu** icon (☰) and choose **Administration** > **Certificates** > **Certificate Signing Requests** > **Replace ISE Root CA certificate chain**).However, If you restore the platinum database with the correct FQDN, note that the CA certificates regenerated automatically.
- You need a data repository, which is the location where Cisco ISE-PIC saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.
- If you have a standalone node that fails, you must run the configuration backup to restore it. If the Primary PAN fails, you can promote your Secondary Administration Node to become the primary. You can then restore data on the Primary PAN after it comes up.

**Note** Cisco ISE-PIC also provides the **backup-logs** CLI command that you can use to collect log and configuration files for troubleshooting purposes.

## Restoration of Configuration or Monitoring (Operational) Backup from the CLI

To restore configuration data through the Cisco ISE CLI, use the **restore** command in the EXEC mode. Use the following command to restore data from a configuration or operational backup:

**restore** *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

Syntax Description

| | |
|---|---|
| **restore** | Type this command to restore data from a configuration or operational backup. |
| *filename* | Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters.<br>**Note**<br>You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg). |
| **repository** | Specifies the repository that contains the backup. |
| *repository-name* | Name of the repository you want to restore the backup from. |
| **encryption-key** | (Optional) Specifies user-defined encryption key to restore backup. |
| **hash** | Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters. |
| **plain** | Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters. |
| *encryption-key name* | Enter the encryption key. |

| | |
|---|---|
| **include-adeos** | (Optional, applicable only for configuration backup) Enter this command operator parameter if you want to restore ADE-OS configuration from a configuration backup. When you restore a configuration backup, if you do not include this parameter, Cisco ISE restores only the Cisco ISE application configuration data. |

### Defaults

No default behavior or values.

### Command Modes

EXEC

### Usage Guidelines

When you use restore commands in Cisco ISE-PIC, the Cisco ISE-PIC server restarts automatically.

The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the **restore** command without the encryption key.

### Examples

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
 Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

### Related Commands

| | Description |
|---|---|
| **backup** | Performs a backup (Cisco ISE-PIC and Cisco ADE OS) and places the backup in a repository. |
| **backup-logs** | Backs up system logs. |
| **repository** | Enters the repository submode for configuration of backups. |
| **show repository** | Displays the available backup files located on a specific repository. |

| | Description |
|---|---|
| **show backup history** | Displays the backup history of the system. |
| **show backup status** | Displays the status of the backup operation. |
| **show restore status** | Displays the status of the restore operation. |

If the sync status and replication status after application restore for any secondary node is *Out of Sync*, you have to reimport the certificate of that secondary node to the Primary PAN and perform a manual synchronization.

## Restore Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal.

### Procedure

**Step 1** Choose **Administration** > **Maintenance** > **Backup and Restore**.

**Step 2** Select the name of the backup from the list of Configurational backup and click **Restore**.

**Step 3** Enter the Encryption Key used during the backup.

**Step 4** Click **Restore**.

**Note**
After performing the restore operation, you must toggle off and toggle on the **Monitoring** button in **Operations > System 360 > Settings** to restart the system monitoring service.

### What to do next

If you are using the Cisco ISE CA service, you must:

1. Regenerate the entire Cisco ISE CA root chain.
2. Obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. This ensures that the secondary PAN can function as the root CA or subordinate CA of an external PKI in case of a Primary PAN failure and you promote the secondary PAN to be the primary PAN.

## Restore History

You can obtain information about all restore operations, log events, and statuses from the **Operations Audit Report** window.

**Note** However, the **Operations Audit Report** window does not provide information about the start times corresponding to the previous restore operations.

For troubleshooting information, you have to run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log file.

While the restore operation is in progress, all Cisco ISE-PIC services are stopped. You can use the **show restore status** CLI command to check the progress of the restore operation.

## Synchronize Primary and Secondary Nodes

the Cisco ISE-PIC database in the primary and secondary nodes are not synchronized automatically after restoring a backup file on the PAN. If this happens, you can manually force a full replication from the PAN to the secondary ISE-PIC nodes. You can force a synchronization only from the PAN to the secondary nodes. During the sync-up operation, you cannot make any configuration changes. Cisco ISE-PIC allows you to navigate to other Cisco ISE-PIC Admin portal pages and make any configuration changes only after the synchronization is complete.

### Procedure

**Step 1** Choose **Administration** > **Deployment**.

**Step 2** Check the check box next to the secondary node if it has an Out of Sync replication status.

**Step 3** Click **Syncup** and wait until the nodes are synchronized with the PAN. You will have to wait until this process is complete before you can access the Cisco ISE-PIC Admin portal again.

## Recovery of Lost Nodes in Standalone and Two-Node Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and two-node deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data.

### Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Two-Node Deployment

#### Scenario

In a two-node deployment, a natural disaster leads to a loss of all the nodes. After recovery, you want to use the existing IP addresses and hostnames.

For example, you have two nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Administration Node or Secondary PAN.) A backup of the N1 node, which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster.

#### Assumption

All Cisco ISE-PIC nodes in the deployment were destroyed. The new hardware was imaged using the same hostnames and IP addresses.

#### Resolution Steps

1. You have to replace both the N1 and N2 nodes. N1 and N2 nodes will now have a standalone configuration.
2. Obtain a license with the UDI of the N1 and N2 nodes and install it on the N1 node.

3. You must then restore the backup on the replaced N1 node. The restore script will try to sync the data on N2, but N2 is now a standalone node and the synchronization fails. Data on N1 will be reset to time T1.
4. You must log in to the N1 Admin portal to delete and reregister the N2 node. Both the N1 and N2 nodes will have data reset to time T1.

## Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Two-Node Deployment

### Scenario

In a two-node deployment, a natural disaster leads to loss of all the nodes. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

For example, you have two ISE-PIC nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Node.) A backup of the N1 node which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster. The Cisco ISE-PIC nodes are replaced at a new location and the new hostnames are N1A (primary PAN) and N2A (secondary Node). N1A and N2A are standalone nodes at this point in time.

### Assumptions

All Cisco ISE-PIC nodes in the deployment were destroyed. The new hardware was imaged at a different location using different hostnames and IP addresses.

### Resolution Steps

1. Obtain the N1 backup and restore it on N1A. The restore script will identify the hostname change and domain name change, and will update the hostname and domain name in the deployment configuration based on the current hostname.
2. You must generate a new self-signed certificate.
3. Delete the old N2 node.

   Register the new N2A node as a secondary node. Data from the N1A node will be replicated to the N2A node.

## Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment

### Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database was taken at time T1. The N1 node goes down because of a physical failure and must be reimaged or a new hardware is required. The N1 node must be brought back up with the same IP address and hostname.

### Assumptions

This deployment is a standalone deployment and the new or reimaged hardware has the same IP address and hostname.

### Resolution Steps

Once the N1 node is up after a reimage or you have introduced a new Cisco ISE-PIC node with the same IP address and hostname, you must restore the backup taken from the old N1 node. You do not have to make any role changes.

## Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment

### Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database taken at time T1 is available. The N1 node is down because of a physical failure and will be replaced by a new hardware at a different location with a different IP address and hostname.

### Assumptions

This is a standalone deployment and the replaced hardware has a different IP address and hostname.

### Resolution Steps

1. Replace the N1 node with a new hardware. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. No role changes are required.

## Configuration Rollback

### Problem

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. In this case, you can revert to the original configuration by restoring a backup that was taken before you made the changes.

### Possible Causes

There are two nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Policy Administration Node or secondary PAN) and a backup of the N1 node is available. You made some incorrect configuration changes on N1 and want to remove the changes.

### Solution

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. The restore script will synchronize the data from N1 to N2.

## Recovery of Primary Node in Case of Failure in a Two-Node Deployment

### Scenario

In a multinode deployment, the PAN fails.

For example, you have two Cisco ISE-PIC nodes, N1 (PAN) and N2 (Secondary Administration Node). N1 fails because of hardware issues.

#### Assumptions

Only the primary node in a two-node deployment has failed.

#### Resolution Steps

1. Log in to the N2 administrator portal. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose  and configure N2 as your primary node.

   The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 administrator portal, register the new N1 node as a secondary node.

   Now, the N2 node becomes your primary node and the N1 node becomes your secondary node.

If you wish to make the N1 node the primary node again, log in to the N1 administrator portal and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

### Recovery of Secondary Node in Case of Failure in a Two-Node Deployment

#### Scenario

In a multinode deployment, a single secondary node has failed. No restore is required.

#### Resolution Steps

1. Reimage the secondary node to the default standalone state.
2. Log in to the Admin portal from the primary node and delete the secondary node.
3. Reregister the secondary node.

   Data is replicated from the primary to the secondary node. No restore is required.

## Database Purge

The purging process allows you to manage the size of the database by specifying the number of months to retain the data during a purge. The default is three months. This value is utilized when the disk space usage threshold for purging (80 percentage of the total disk space) is met. For this option, each month consists of 30 days. A default of three months equals 90 days.

### Guidelines for Purging the Database

Follow these guidelines for optimal Monitoring database disk usage:

- If the database disk usage is greater than 80 percent of the threshold setting, that is 60 percent of total disk space, a critical alarm is generated, indicating that the database size is about to exceed the maximum amount of allocated disk size. If the disk usage is greater than 90 percent of the threshold setting, that is 70 percent of total disk space, another alarm is generated, indicating that the database size has exceeded the maximum amount of allocated disk size.
- Purging is also based on the percentage of consumed disk space for the database. When the consumed disk space for the database is equal to or exceeds the threshold (the default is 80 percentage of the total disk space), the purge process starts. This process deletes only the oldest seven days' monitoring data, irrespective of what is configured in the Admin portal. It continues this process in a loop until the disk space is below 80 percent. Purging always checks the database disk space limit before proceeding.

## Operational Data Purging

Cisco ISE Monitoring Operational database contains information that is generated as Cisco ISE reports. Recent Cisco ISE releases have options to purge the monitoring operational data and reset the monitoring database when the **application configure ise** command is run.

The purge option is used to clean up the data and prompts you to enter the number of days for which to retain the data. The reset option is used to reset the database to the factory default, so that all the data that is backed up is permanently deleted. Specify the database if the files are consuming too much file system space.

**Note** The reset option causes Cisco ISE services to be temporarily unavailable.

### Related Topics

Purge Older Operational Data, on page 131

## Purge Older Operational Data

The operational data is collected in the server over a period of time. It can be purged either instantly or periodically.

### Procedure

**Step 1** Choose **Administration** > **Maintenance** > **Operational Data Purging**.

**Step 2** Do one of the following:

- In the **Data Retention Period** area:
  - **a.** Specify the time period, in days, for which RADIUS and TACACS data should be retained. All the data prior to the specified time period is exported to a repository. While ISE-PIC does not offer RADIUS or TACACS functionality, some of the infrastructure is shared with Cisco ISE and therefore, it may be necessary to purge such information from the database periodically.
  - **b.** In the **Repository** area, check the **Enable Export Repository** check box to choose the repository to save data.
  - **c.** In the **Encryption Key** field, enter the required password.
  - **d.** Click **Save**.

    **Note**
    If the configured retention period is less than the existing retention thresholds corresponding to the diagnostics data, the configured value overrides the existing threshold values. For example, if you configure the retention period as three day,s and this value is less than the existing thresholds in the diagnostics tables (for example, a default of five days), the data is purged according to the value that you configure (three days) in this window.

- In the **Purge Data Now** area:
  - **a.** Choose to purge all the data or to purge the data that is older than the specified number of days. Data is not saved in any repository.

b. Click **Purge**.

# Upgrading ISE-PIC to a Full ISE Installation

Cisco ISE-PIC is displayed in a simple user-intuitive GUI, based on the full Cisco ISE GUI. As a result, the installation of ISE-PIC enables you to easily upgrade to ISE quickly and efficiently. When upgrading from ISE-PIC to the Essential license for ISE, ISE continues to offer all features that were available to you in ISE-PIC prior to upgrade and you will not need to reconfigure any settings that you had already configured if you use the upgraded ISE-PIC node as your primary PAN.

**Note** If you do not use the existing upgraded ISE-PIC node as your primary PAN, then the data on that node will be erased when you upgrade and you will be able to access the data from your existing full ISE deployment from the newly added node.

For more information about the benefits of upgrading to ISE, see Comparing ISE-PIC with Cisco ISE and Cisco Context Directory Agent, on page 5.

# Upgrade to ISE by Registering Licenses

### Before you begin

An ISE-PIC node can be upgraded to a Cisco ISE node by enabling the Essential license. Before enabling the Essential license, you must purchase and enable both ISE-PIC and ISE-PIC Upgrade licenses on the ISE-PIC node. The Essential license is displayed in the Licenses table after you register the license in CSSM. The application services are restarted during the upgrade.

For more information about the licensing model, see ISE-PIC Smart Licensing, on page 10

### Procedure

**Step 1** If you have a secondary node installed, from your Cisco ISE-PIC primary node installation, choose **Administration** > **Deployment** and Deregister the secondary node. Both nodes then become primary nodes and either of them can be upgraded.

**Step 2** Choose **Administration** > **Licensing**.

**Step 3** Click **Import License**.

**Step 4** Click **Choose File**, browse for the Upgrade license file, and click **OK**.

**Step 5**

**Note**
If you are adding this ISE-PIC node to an existing ISE deployment, you have completed the upgrade once you have completed this step and now can add the node by registering it from the primary node in that deployment. For more information, see the Cisco Identity Services Engine Administrator Guide.

From the **Import New License File** screen, click **Import**.

**Step 6** To make this upgraded node the primary node in a full ISE deployment import a Essential license now. Click **Import License** again.

**Step 7** Click **Choose File**, browse for the license that you received from your Cisco representative, and click **OK**.

**Step 8** From the **Import New License File** screen, click **Import**.

**Step 9** Click **OK**.
The upgrade to being a primary node of ISE begins and the following message appears: *This node is now being upgraded to ISE in the background. Please wait several minutes and then log in to ISE.*

**Step 10** Click **OK**.

The log in screen appears after several minutes. Log back in and access all menus offered by the Essential license installation.

You have now upgraded your primary ISE-PIC node to be the primary node in a full ISE installation and the former secondary node is now the primary and only node in the ISE-PIC standalone installation. You can now separately upgrade the last ISE-PIC node in the same manner.

# Manage Settings in ISE-PIC

## Role-Based Access Control

Cisco ISE-PIC allows you to define role-based access control (RBAC) policies that allow or deny certain system-operation permissions to an administrator. These RBAC policies are defined based on the identity of individual administrators or the admin group to which they belong.

To further enhance security and control who has access to the Admin portal, you can:

- Configure administrative access settings based on the IP address of remote clients.
- Define strong password policies for administrative accounts.
- Configure session timeouts for administrative GUI sessions.

## Cisco ISE-PIC administrators

Administrators can use the admin portal to:

- Manage deployments node monitoring and troubleshooting.
- Manage Cisco ISE-PIC servicesadministrator accounts, and system configuration and operations.
- Change administrator and user passwords.

A CLI administrator can start and stop the Cisco ISE application, apply software patches and upgrades, reload, or shut down the Cisco ISE appliance, and view all the system and application logs. Because of the special privileges that are granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments.

The username and password that you configure during setup is intended only for administrative access to the CLI. This role is considered to be the CLI admin user, also known as CLI administrator. By default, the

username for a CLI admin user is admin, and the password is defined during setup. There is no default password. This CLI admin user is the default admin user, and this user account cannot be deleted. However, other administrators can edit it, including options to enable, disable, or change password for the corresponding account.

You can either create an administrator, or you can promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges.

Administrators are users who have local privileges to configure and operate the Cisco ISE-PIC system.

Administrators are assigned to one or more admin groups. These admin groups are predefined in the system for your convenience, as described in the following section.



**Note** Use alphanumeric values while creating user accounts in Cisco ISE.

**Related Topics**

Cisco ISE-PIC administrator groups, on page 134

## Cisco ISE-PIC administrator groups

Administrator groups are role-based access control (RBAC) groups in Cisco ISE-PIC. All the administrators who belong to the same group share a common identity and have the same privileges. An administrator's identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

Cisco ISE supports multiple external identity stores for enhanced user access management by admins.

An administrator account with any level of access can be used to modify or delete the objects for which it has permission, on any window it has access to.

The following table lists the admin groups that are predefined in Cisco ISE-PIC, and the tasks that members from these groups can perform. Only these predefined groups are available for defining administrator users in the system.

***Table 22: Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions***

| Admin Group Role | Access Level | Permissions | Restrictions |
|---|---|---|---|
| Super Admin | All Cisco ISE-PIC administrative functions. The default administrator account belongs to this group. | Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE-PIC resources. | |
| External RESTful Services (ERS) Admin | Full access to all ERS API requests such as GET, POST, DELETE, PUT | • Create, Read, Update, and Delete ERS API requests | The role is meant only for ERS authorization supporting Internal Users, Identity Groups, and Endpoints |

## Privileges of a CLI Administrator Versus a Web-Based Administrator

A CLI administrator can start and stop the Cisco ISE-PIC application, apply software patches and upgrades, reload or shut down the Cisco ISE-PIC appliance, and view all the system and application logs. Because of the special privileges granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE-PIC deployments.

## Create a new administrator

Cisco ISE-PIC administrators need accounts with specific roles assigned to them to perform specific administrative tasks. You can create multiple administrator accounts and assign one or more roles to these admins based on the administrative tasks that these admins must perform.

Use the **Admin Users** window to view, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE-PIC administrators.

**Note** We recommend that you configure Active Directory access in the CLI before you join it in the GUI if the admin user's domain is the same in both the CLI and the GUI. Else, you must rejoin the domain from the GUI to avoid authentication failures to that domain.

### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Admin Users** > **Add** > **Create an Admin User**.

**Step 2** Enter values in the fields. The characters supported for the **Name** field are # $ ’ ( ) * + - . / @ _.

The admin username must be unique. If you have entered an existing username, an error pop-up window displays this message:

```
User can't be created. A User with that name already exists.
```

**Step 3** Click **Submit** to create a new administrator in the Cisco ISE-PIC internal database.

### Related Topics

Read-only admin policy
Customize menu access for the read-only administrator

# Administrative access to Cisco ISE-PIC

Cisco ISE-PIC administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical. Grant administrative access only to users who are authorized to administer Cisco ISE-PIC in your network.

**Note** When a Cisco ISE server is added to a network, it is marked to be in Running state after its web interface comes up. However, it might take some more time for all the services to be fully operational because few advanced services, such as posture services, might take longer to be available.

### Administrative access methods

You can connect to the Cisco ISE servers in several ways. The policy administration node (PAN) runs the Administrators portal. An admin password is required to log in. Other ISE persona servers are accessible through SSH or the console, from where you run the CLI. This section describes the process and password options available for each connection type:

- **Admin password**: The Cisco ISE Admin user that you created during installation, times out in 45 days by default. You can prevent that by turning off **Password Lifetime** from **Administration** > **System** > **Admin Settings**. Click the **Password Policy** tab and uncheck the**Administrative passwords expire** check box under **Password Lifetime**.

  If you do not do this, and the password expires, you can reset the admin password in the CLI by running the **application reset-passwd** command. You can reset the admin password by connecting to the console to access the CLI, or by rebooting the ISE image file to access the boot options menu.

- **CLI password**: You must enter a CLI password during installation. If you have a problem logging in to the CLI because of an invalid password, you can reset the CLI password. Connect to the console and run the **password** CLI command to rest the password. See the Cisco Identity Services Engine CLI Reference Guide for more information.

-

## Administrator Access Settings

Cisco ISE-PIC allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define in the Administrator Account Settings in Cisco ISE-PIC applies to all administrator accounts.

Cisco ISE-PIC supports administrator passwords with UTF-8 characters.

### Configure Maximum Number of Concurrent Administrative Sessions and Login Banners

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners are disabled. However, you cannot configure the maximum number of concurrent sessions for individual administrator accounts.

#### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Access Settings** > **Session**.

**Step 2** Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.

**Step 3** If you want Cisco ISE-PIC to display a message before an administrator logs in, check the **Pre-login banner** check box and enter your message in the text box.

**Step 4** If you want Cisco ISE-PIC to display a message after an administrator logs in, check the **Post-login banner** check box and enter your message in the text box.

**Step 5** Click **Save**.

**Note**
The character limit is set at 1500 for the Pre-login banner and 3000 for the Post-login banner. All characters except **%** and **<** are supported. For login banner installation through CLI, the maximum length of the file name used is 256 characters.

## Allow Administrative Access to Cisco ISE-PIC from Select IP Addresses

Cisco ISE-PIC allows you to configure a list of IP addresses from which administrators can access the Cisco ISE-PIC management interfaces.

### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Access Settings** > **IP Access**.

**Step 2** Choose the service for which you want to configure access restriction by clicking the corresponding service tab. You can configure access restriction for the following services:

- **Admin GUI and CLI**
- **Admin Services** (ERS API, OpenAPI, pxGrid, and Data Connect)
- **User Services** (Guest, BYOD, and Posture)

**Step 3** Click the **Allow only Listed IP addresses to Connect** radio button.

**Note**
Connection on Port 161 (SNMP) is used for administrative access. However, when IP access restrictions are configured, the **snmpwalk** fails if the node from which it was performed is not configured for administrative access.

**Step 4** In the **Configure IP List for Access Permission** area, click **Add**.

**Step 5** In the **Add IP CIDR** dialog box, enter the IP addresses in the classless interdomain routing (CIDR) format in the **IP Address** field.

**Note**
This IP address can be an IPv4 or an IPv6 address. You can configure multiple IPv6 addresses for a Cisco ISE node.

**Step 6** Enter the subnet mask in the **Netmask in CIDR format** field.

**Step 7** Click **OK**.

Repeat steps 4 to 7 to add more IP address ranges to this list.

**Step 8** Click **Save** to save the changes.

**Step 9** Click **Reset** to refresh the **IP Access** window.

## Configure a Password Policy for Administrator Accounts

Cisco ISE-PIC also allows you to create a password policy for administrator accounts to enhance security. The password policy that you define here is applied to all the administrator accounts in Cisco ISE-PIC.

**Note**

- Email notifications for internal admin users are sent to root@host. You cannot configure the email address, and many SMTP servers reject this email.

  Follow open defect CSCui5583, which is an enhancement to allow you to change the email address.

- Cisco ISE-PIC supports administrator passwords with UTF-8 characters.

### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Authentication**.

**Step 2** Click the **Password Policy** tab and enter the required values to configure the Cisco ISE GUI and CLI password requirements.

**Step 3** Click **Save** to save the administrator password policy.

**Note**
If you use an external identity store to authenticate administrators at login, note that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator's username and password.

## Configure Account Disable Policy for Administrator Accounts

Cisco ISE-PIC allows you to disable an administrator account if the administrator account is not authenticated for the configured consecutive number of days.

### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Authentication** > **Account Disable Policy**.

**Step 2** Check the **Disable account after *n* days of inactivity** check box, and enter the number of days in the corresponding field.

This option allows you to disable the administrator account if the administrator account was inactive for the specified number of days.

When an administrator account is disabled and enabled later, it does not remain active for more than 24 hours. If you want an administrator account to remain active even when disabled, keep the **Disable account after *n* days of inactivity** checkbox unchecked.

**Attention**
Cisco ISE does not support the **Disable account after *n* days of inactivity** option even if it is enabled, for administrator accounts that have **Collection Filters** (**Work Centers** > **Network Access** > **Settings** > **Collection Filters** > **Filter All**) configured.

**Step 3** Click **Save** to configure the global account disable policy for administrators.

### Configure Session Timeout for Administrators

Cisco ISE-PIC allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE-PIC logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE-PIC Admin portal.

#### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Session Settings** > **Session Timeout**.

**Step 2** Enter the time in minutes that you want Cisco ISE-PIC to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

**Step 3** Click **Save**.

### Terminate an Active Administrative Session

Cisco ISE-PIC displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

#### Procedure

**Step 1** Choose **Administration** > **Admin Access** > **Session Settings** > **Session Info**.

**Step 2** Check the check box next to the session ID that you want to terminate and click **Invalidate**.

## Ports Used by the Administration Portal

The administration portal uses HTTP port 80 and HTTPS port 443 and you cannot change these settings. You cannot configure any of the end user portals to use these ports, to reduce the risk to the administration portal.

## Configure SMTP Server to Support Notifications

Configure a Simple Mail Transfer Protocol (SMTP) server to send email notifications for alarms.

Which ISE Nodes Send Email

The following list shows which node in a distributed ISE environment sends email.

| Email Purpose | Node That Sends the Email |
|---|---|
| guest expiration | Primary PAN |
| alarms | Active MnT |

| Email Purpose | Node That Sends the Email |
|---|---|
| sponsor and guest notifications from guest and sponsor portals | PSN |
| password expirations | Primary PAN |

### Procedure

**Step 1** Choose **Settings** > **SMTP Server**.

**Step 2** Enter the hostname of the outbound SMTP server in the **SMTP server** field. This SMTP host server must be accessible from the Cisco ISE-PIC server. The maximum length for this field is 60 characters.

**Step 3** Click **Save**.

The recipient of alarm notifications can be any internal admin users with the **Include system alarms in emails** option enabled. The sender's email address for sending alarm notifications is hardcoded as ise@<hostname>.

# Enabling External RESTful Services APIs from the GUI—ERS Settings

### Before you begin

You must enable the Cisco ISE REST API in order for applications developed for a Cisco ISE REST API to be able to access Cisco ISE. The Cisco REST APIs uses HTTPS port 9060, which is closed by default. If the Cisco ISE REST APIs are not enabled on the Cisco ISE admin server, the client application will receive a time-out error from the server for any Guest REST API request.

External RESTful Service requests of all types are valid only for the primary ISE node. Secondary nodes have read-access (GET requests).

### Procedure

**Step 1** Choose **Settings** > **ERS Settings**.

**Step 2** Choose **Enable ERS for Read/Write** and click **Save**.

### What to do next

See the ISE API reference guide for more information and details about API calls and ISE-PIC.

# Configure Security Settings

To configure the security settings:

### Procedure

**Step 1** Choose **Settings > Security Settings**.

**Step 2** In the **Security Settings** window, choose the required options:

**a.** **Allow TLS 1.0**: Allows TLS 1.0 for communication with legacy peers for the following workflows:

- Cisco ISE is configured as an EAP server
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure TCP syslog client
- Cisco ISE is configured as a secure LDAP client
- Cisco ISE is configured as an ERS server

Also allows TLS 1.0 for communication with the following ISE components:

- All portals
- Certificate Authority
- MDM Client
- pxGrid
- PassiveID Agent

**Note**
It is recommended that clients and servers negotiate to use a higher version of TLS for enhanced security.

**b.** **Allow TLS 1.1**: Allows TLS 1.1 for communication with legacy peers for the following workflows:

- Cisco ISE is configured as an EAP server
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure TCP syslog client
- Cisco ISE is configured as a secure LDAP client
- Cisco ISE is configured as an ERS server

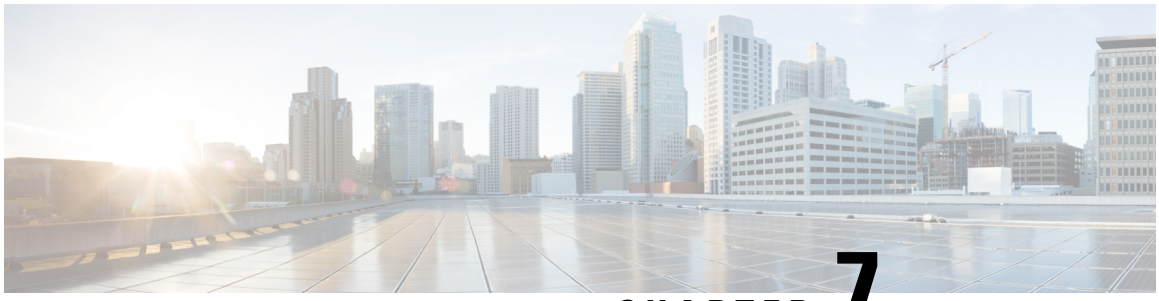
Also allows TLS 1.1 for communication with the following ISE components:

- Admin UI
- All portals
- Certificate Authority
- External RESTful Services (ERS)

- MDM Client
- pxGrid

**Note**
It is recommended that clients and servers negotiate to use a higher version of TLS for enhanced security.

**Step 3** Click **Save**.



CHAPTER 7

# Monitoring and Troubleshooting Service in ISE-PIC

The Monitoring and troubleshooting service is a comprehensive identity solution for all Cisco ISE-PIC run-time services and uses the following components:

- Monitoring—Provides a real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and affect operational conditions.
- Troubleshooting—Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide a resolution in a timely manner.
- Reporting—Provides a catalog of standard reports that you can use to analyze trends and monitor system performance and network activities. You can customize reports in various ways and save them for future use. You can search records using wild cards and multiple values for the Identity, Endpoint ID, and Node fields.

Learn more in this section about how you can manage ISE-PIC with monitoring, troubleshooting and reporting tools.


- Live Sessions, on page 143
- Available Reports, on page 146
- Cisco ISE-PIC Alarms, on page 148
- TCP Dump Utility to Validate Incoming Traffic, on page 158
- Logging Mechanism, on page 160
- Active Directory Troubleshooting , on page 161
- Obtaining Additional Troubleshooting Information, on page 173
- Additional References, on page 178
- Communications, services, and additional information, on page 178


# Live Sessions

This table describes the fields in the **Live Sessions** window, which displays live sessions. From the main menu bar, choose **Live Sessions**.

*Table 23: Live Sessions*

| Field Name | Description |
|---|---|
| **Initiated** | Shows the timestamp when the session was initiated. |
| **Updated** | Shows the timestamp when the session was last updated due to any change. |
| **Account Session Time** | Shows the time span (in seconds) of a user's session. |
| **Session Status** | Shows the current status of the endpoint device. |
| **Action** | Click the Actions icon to open the **Actions** pop-up window. You can do the following:<br>• Clear a session<br>• Check the session status of current user |
| **Endpoint ID** | Shows the unique identifier for an endpoint, usually a MAC or IP address. |
| **Identity** | Shows the username of the endpoint device. |
| **IP Address** | Shows the IP address of the endpoint device. |
| **Server** | Indicates the PIC node from which the log was generated. |
| **Auth Method** | Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and the like. |
| **Session Source** | Indicates whether it is a RADIUS session or PassiveID session. |
| **User Domain Name** | Shows the registered DNS name of the user. |
| **User NetBIOS Name** | Shows the NetBIOS name of the user. |

| Field Name | Description |
|---|---|
| **Provider** | Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers.<br>• Windows Management Instrumentation (WMI)—WMI is a Windows service that provides a common interface and object model to access management information about operating system, devices, applications, and services.<br>• Agent—A program that runs on a client on behalf of the client or another program.<br>• Syslog—A logging server to which a client sends event messages.<br>• REST—A client is authenticated through a terminal server. The TS Agent ID, Source Port Start, Source Port End, and Source First Port values are displayed for this syslog source.<br>• Span—Network information is discovered using span probes.<br>• DHCP—DHCP event.<br>• Endpoint<br>When two events from different providers are learned from an endpoint session, the providers are displayed as comma-separated values in the live sessions page. |
| **MAC Address** | Shows the MAC address of a client. |
| **Endpoint Check Time** | Shows the time at which the endpoint was last checked by the endpoint probe. |
| **Endpoint Check Result** | Shows the result of an endpoint probe. The possible values are:<br>• Unreachable<br>• User Logout<br>• Active User |
| **Source Port Start** | (Values are displayed only for the REST provider) Shows the first port number in a port range. |
| **Source Port End** | (Values are displayed only for the REST provider) Shows the last port number in a port range. |
| **Source First Port** | (Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server (TS) Agent.<br>A Terminal Server (TS) refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address and therefore it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a TS Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port-user mapping. |

| Field Name | Description |
|---|---|
| **TS Agent ID** | (Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server (TS) agent that is installed on an endpoint. |
| **AD User Resolved Identities** | (Values are displayed only for AD user) Shows the potential accounts that matched. |
| **AD User Resolved DNs** | (Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com |

# Available Reports

The following table lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.

| Report Name | Description | Logging Category |
|---|---|---|
| **IDC Reports** | | |
| AD Connector Operations | The AD Connector Operations report provides log of operations performed by AD Connector such as ISE-PIC Server password refresh, Kerberos tickets management, DNS queries, DC discovery, LDAP, and RPC Connections management, etc.<br>If some AD failures are encountered, you can review the details in this report to identify the possible causes. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select AD Connector. |
| Administrator Logins | The Administrator Logins report provides information about all GUI-based administrator login events as well as successful CLI login events. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit. |
| Change Configuration Audit | The Change Configuration Audit report provides details about configuration changes within a specified time period. If you need to troubleshoot a feature, this report can help you determine if a recent configuration change contributed to the problem. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit. |

| Report Name | Description | Logging Category |
|---|---|---|
| Current Active Sessions | The Current Active Sessions report enables you to export a report with details about who was currently on the network within a specified time period.<br><br>If a user isn't getting network access, you can see whether the session is authenticated or terminated or if there is another problem with the session. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Accounting and RADIUS Accounting. |
| Health Summary | The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours, and you can review more historical data using this report.<br><br>You can evaluate this data to see consistent patterns in data. For example, you would expect heavier CPU usage when most employees start their work days. If you see inconsistencies in these trends, you can identify potential problems.<br><br>The CPU Usage table lists the percentage of CPU usage for the different ISE-PIC functions. The output of the **show cpu usage** CLI command is presented in this table and you can correlate these values with the issues in your deployment to identify possible causes. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Administrative and Operational Audit, System Diagnostics, and System Statistics. |
| Operations Audit | The Operations Audit report provides details about any operational changes, such as: running backups, registering a ISE-PIC node, or restarting an application. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit. |
| PassiveID | The Passive ID report enables you to monitor the state of WMI connection to the domain controller and gather statistics related to it (such as amount of notifications received, amount of user login/logouts per second etc.) | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Identity Mapping. |

| Report Name | Description | Logging Category |
|---|---|---|
| pxGrid Administrator Audit | The pxGrid Administrator Audit report provides the details of the pxGrid administration actions such as client registration, client deregistration, client approval, topic creation, topic deletion, publisher-subscriber addition, and publisher-subscriber deletion.<br>Every record has the administrator name who has performed the action on the node.<br>You can filter the pxGrid Administrator Audit report based on the administrator and message criteria. | — |
| System Diagnostic | The System Diagnostic report provides details about the status of the ISE-PIC nodes. If the ISE-PIC node is unable to register, you can review this report to troubleshoot the issue.<br>This report requires that you first enable several diagnostic logging categories. Collecting these logs can negatively impact ISE-PIC performance. So, these categories are not enabled by default, and you should enable them just long enough to collect the data. Otherwise, they are automatically disabled after 30 minutes. | Choose **Administration** > **Logging** > **Logging Categories** and select these logging categories: Internal Operations Diagnostics, Distributed Management, Administrator Authentication and Authorization. |
| User Change Password Audit | The User Change Password Audit report displays verification about employee's password changes. | Choose **Administration** > **System** > **Logging** > **Logging Categories** and select Administrative and Operational audit. |

# Cisco ISE-PIC Alarms

Alarms notify you of conditions on a network and are displayed in the Alarms dashlet. There are three alarm severities: critical, warning and information. They also provide information on system activities, such as data purge events. You can configure how you want to be notified about system activities, or disable them entirely. You can also configure the threshold for certain alarms.

Most alarms do not have an associated schedule and are sent immediately after an event occurs. At any given point in time, only the latest 15,000 alarms are retained.

If the event re-occurs, then the same alarms are suppressed for about an hour. During the time that the event re-occurs, depending up on the trigger, it may take about an hour for the alarms to re-appear.

The following table lists all the Cisco ISE-PIC alarms, descriptions and their resolution.

***Table 24: Cisco ISE-PIC Alarms***

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Administrative and Operational Audit Management | | |
| Deployment Upgrade Failure | An upgrade has failed on an ISE PIC node. | Check the ADE.log on the failed node for upgrade failure reason and corrective actions. |
| Upgrade Bundle Download failure | An upgrade bundle download has failed on an ISE-PIC node. | Check the ADE.log on the failed node for upgrade failure reason and corrective actions. |
| Secure LDAP connection reconnect due to CRL found revoked certificate | CRL check result is that the certificate used for LDAP connection is revoked. | Check the CRL configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on LDAP server. |
| Secure LDAP connection reconnect due to OCSP found revoked certificate | OCSP check result is that the certificate used for LDAP connection is revoked. | Check the OCSP configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on LDAP server. |
| Secure syslog connection reconnect due to CRL found revoked certificate | CRL check result is that the certificate used for syslog connection is revoked. | Check the CRL configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on syslog server. |
| Secure syslog connection reconnect due to OCSP found revoked certificate | OCSP check result is that the certificate used for syslog connection is revoked. | Check the OCSP configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on syslog server. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Administrator account Locked/Disabled | Administrator account is locked or disabled due to password expiration or incorrect login attempts. For more details, refer to the administrator password policy. | Administrator password can be reset by another administrator using the GUI or CLI. |
| ERS identified deprecated URL | ERS identified deprecated URL | The request URL is deprecated and it is recommended to avoid using it. |
| ERS identified out-dated URL | ERS identified out-dated URL | The requested URL is out-dated and it is recommended to use a newer one. This URL will not be removed in future releases. |
| ERS request content-type header is out-dated | ERS request content-type header is out-dated. | 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 attributes may have been added or removed. To overcome that with the outdated schema, the ERS Engine will use default values. |
| ERS XML input is a suspect for XSS or Injection attack | ERS XML input is a suspect for XSS or Injection attack. | Please review your xml input. |
| Backup Failed | The Cisco ISE-PIC backup operation failed. | Check the network connectivity between Cisco ISE-PIC and the repository. Ensure that:<br>• The credentials used for the repository is correct.<br>• There is sufficient disk space in the repository.<br>• The repository user has write privileges. |
| CA Server is down | CA server is down. | Check to make sure that the CA services are up and running on the CA server. |
| CA Server is Up | CA server is up. | A notification to inform the administrator that the CA server is up. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Certificate Expiration | This certificate will expire soon. When it expires, Cisco ISE-PIC may fail to establish secure communication with clients. | Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE-PIC to extend the expiration date. You can delete the certificate if it is no longer used. |
| Certificate Revoked | Administrator has revoked the certificate issued to an Endpoint by the Internal CA. | Go through the ISE-PIC flow from the beginning to be provisioned with a new certificate. |
| Certificate Provisioning Initialization Error | Certificate provisioning initialization failed | More than one certificate found with the same value of CN (CommonName) attribute in the subject, cannot build certificate chain. Check all the certificates in the system. |
| Certificate Replication Failed | Certificate replication to secondary node failed | The certificate is not valid on the secondary node, or there is some other permanent error condition. Check the secondary node for a pre-existing, conflicting certificate. If found, delete the pre-existing certificate on the secondary node, and export the new certificate on the primary, delete it, and import it in order to re-attempt replication. |
| Certificate Replication Temporarily Failed | Certificate replication to secondary node temporarily failed | The certificate was not replicated to a secondary node due to a temporary condition such as a network outage. The replication will be retried until it succeeds. |
| Certificate Expired | This certificate has expired. Cisco ISE-PIC may fail to establish secure communication with clients.<br>Node-to-node communication may also be affected. | Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE-PIC to extend the expiration date. You can delete the certificate if it is no longer used. |
| Certificate Request Forwarding Failed | Certificate request forwarding failed. | Make sure that the certification request coming in matches with attributes from the sender. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Configuration Changed | Cisco ISE configuration is updated. This alarm is not triggered for any configuration change in users and endpoints. | Check if the configuration change is expected. |
| CRL Retrieval Failed | Unable to retrieve CRL from the server. This could occur if the specified CRL is unavailable. | Ensure that the download URL is correct and is available for the service. |
| DNS Resolution Failure | DNS resolution failed on the node. | Check if the DNS server configured by the command **ip name-server** is reachable.<br>If you get the alarm as 'DNS Resolution failed for CNAME <hostname of the node>', then ensure that you create CNAME RR along with the A record for each Cisco ISE node. |
| Firmware Update Required | A firmware update is required on this host. | Contact Cisco Technical Assistance Center (TAC) to obtain firmware update |
| Insufficient Virtual Machine Resources | Virtual Machine (VM) resources such as CPU, RAM, Disk Space, or IOPS are insufficient on this host. | Ensure that a minimum requirements for the VM host, as specified in the Cisco ISE Hardware Installation Guide. |
| NTP Service Failure | The NTP service is down on this node. | This could be because there is a large time difference between NTP server and Cisco ISE-PIC node (more than 1000s). Ensure that your NTP server is working properly and use the **ntp server <servername>** CLI command to restart the NTP service and fix the time gap. |
| NTP Sync Failure | All the NTP servers configured on this node are unreachable. | Execute **show ntp** command from the CLI for troubleshooting. Ensure that the NTP servers are reachable from Cisco ISE-PIC. If NTP authentication is configured, ensure that the key ID and value matches with that of the server. |
| No Configuration Backup Scheduled | No Cisco ISE-PIC configuration backup is scheduled. | Create a schedule for configuration backup. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Operations DB Purge Failed | Unable to purge older data from the operations database. This could occur if M&T nodes are busy. | Check the Data Purging Audit report and ensure that the used_space is lesser than the threshold_space. Login to M&T nodes using CLI and perform the purge operation manually. |
| Replication Failed | The secondary node failed to consume the replicated message. | Login to the Cisco ISE-PIC GUI and perform a manual syncup from the deployment page. De-register and register back the affected Cisco ISE-PIC node. |
| Restore Failed | Cisco ISE-PIC restore operation failed. | Ensure the network connectivity between Cisco ISE-PIC and the repository. Ensure that the credentials used for the repository is correct. Ensure that the backup file is not corrupted. Execute the **reset-config** command from the CLI and restore the last known good backup. |
| Patch Failure | A patch process has failed on the server. | Re-install the patch process on the server. |
| Patch Success | A patch process has succeeded on the server. | - |
| Replication Stopped | ISE-PIC node could not replicate configuration data from the primary node. | Login to the Cisco ISE-PIC GUI to perform a manual syncup from the deployment page or de-register and register back the affected Cisco ISE-PIC node with required field. |
| Endpoint certificates expired | Endpoint certificates were marked expired by daily scheduled job. | Please re-enroll the endpoint device to get a new endpoint certificate. |
| Endpoint certificates purged | Expired endpoint certificates were purged by daily scheduled job. | No action needed - this was an administrator-initiated cleanup operation. |
| Slow Replication Error | Slow or a stuck replication is detected. | Please verify that the node is reachable and part of the deployment. |
| Slow Replication Info | Slow or a stuck replication is detected. | Please verify that the node is reachable and part of the deployment. |
| Slow Replication Warning | Slow or a stuck replication is detected . | Please verify that the node is reachable and part of the deployment. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| EST Service is down | EST Service is down. | Make sure that the CA and EST services are up and running and Certificate services endpoint Sub CA certificate chain is complete. |
| EST Service is up | EST Service is up. | A notification to inform the administrator that the EST service is up. |
| Smart Call Home Communication Failure | Smart Call Home messages were not sent successfully. | Ensure that there is network connectivity between Cisco ISE-PIC and Cisco systems. |
| Telemetry Communication Failure | Telemetry messages were not sent successfully. | Ensure that there is network connectivity between Cisco ISE and Cisco systems. |
| ISE Services | | |
| AD Connector had to be restarted | AD Connector stopped unexpectedly and had to be restarted. | If this issue persists, contact the Cisco TAC for assistance. |
| Active Directory forest is unavailable | Active Directory forest GC (Global Catalog) is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval. | Check DNS configuration, Kerberos configuration, error conditions, and network connectivity. |
| Authentication domain is unavailable | Authentication domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval. | Check DNS configuration, Kerberos configuration, error conditions, and network connectivity. |
| ID Map. Authentication Inactivity | No User Authentication events were collected by the Identity Mapping service in the last 15 minutes. | If this is a time when User Authentications are expected (e.g. work hours), then check the connection to Active Directory domain controllers. |
| Configured nameserver is down | Configured nameserver is down or unavailable. | Check DNS configuration and network connectivity. |
| AD: Machine TGT refresh failed | ISE-PIC server TGT (Ticket Granting Ticket) refresh has failed; it is used for AD connectivity and services. | Check that the Cisco ISE-PIC machine account exists and is valid. Also, check for possible clock skew, replication, Kerberos configuration and/or network errors. |
| AD: ISE account password update failed | ISE-PIC server has failed to update it's AD machine account password. | Check that the Cisco ISE-PIC machine account password is not changed and that the machine account is not disabled or restricted. Check the connectivity to KDC. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Joined domain is unavailable | Joined domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval. | Check DNS configuration, Kerberos configuration, error conditions, and network connectivity. |
| Identity Store Unavailable | Cisco ISE-PIC policy service nodes are unable to reach the configured identity stores. | Check the network connectivity between Cisco ISE-PIC and identity store. |
| AD: ISE machine account does not have the required privileges to fetch groups | Cisco ISE-PIC machine account does not have the required privileges to fetch groups. | Check if the Cisco ISE-PIC machine account has rights to fetch user groups in Active Directory. |
| System Health | | |
| High Disk I/O Utilization | Cisco ISE-PIC system is experiencing high disk I/O utilization. | Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load. |
| High Disk Space Utilization | Cisco ISE-PIC system is experiencing high disk space utilization. | Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load. |
| High Load Average | Cisco ISE-PIC system is experiencing high load average. | Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load. |
| High Memory Utilization | Cisco ISE-PIC system is experiencing high memory utilization. | Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load. |
| High Operations DB Usage | Cisco ISE-PIC monitoring nodes are experiencing higher volume of syslog data than expected. | Check and reduce the purge configuration window for the operations data. |
| Health Status Unavailable | The monitoring node has not received health status from the Cisco ISE-PIC node. | Ensure that Cisco ISE-PIC nodes are up and running. Ensure that Cisco ISE-PIC nodes are able to communicate with the monitoring nodes. |

| Alarm Name | Alarm Description | Alarm Resolution |
|---|---|---|
| Process Down | One of the Cisco ISE-PIC processes is not running. | Restart the Cisco ISE-PIC application. |
| OCSP Transaction Threshold Reached | The OCSP transaction threshold has been reached. This alarm is triggered when internal OCSP service reach high volume traffic. | Please check if the system has sufficient resources. |
| Licensing | | |
| PIC License Expired | License installed on the Cisco ISE-PIC nodes has expired. | Contact Cisco Accounts team to purchase new licenses. |
| PIC Licence expiring within 30 Days | License installed on the Cisco ISE-PIC nodes will be expiring in 30 days. | Contact Cisco Sales team for extension of the ISE-PIC license. |
| PIC Licence expiring within 60 Days | License installed on the Cisco ISE-PIC nodes will be expiring in 60 days. | Contact Cisco Sales team for extension of the ISE-PIC license. |
| PIC Licence expiring within 90 Days | License installed on the Cisco ISE-PIC nodes will be expiring in 90 days. | Contact Cisco Sales team for extension of the ISE-PIC license. |
| System Error | | |
| Log Collection Error | Cisco ISE-PIC monitoring collector process is unable to persist the audit logs generated from the policy service nodes. | This will not impact the actual functionality of the Policy Service nodes. Contact TAC for further resolution. |
| Scheduled Report Export Failure | Unable to copy the exported report (CSV file) to configured repository. | Verify the configured repository. If it has been deleted, add it back. If it is not available or not reachable, reconfigure the repository to a valid one. |

Alarms are not triggered when you add users or endpoints to Cisco ISE-PIC.

# Alarm Settings

The following table describes the fields in the **Alarm Settings** window(**Settings** > **Alarm Settings**).

| Field Name | Description |
|---|---|
| **Alarm Type** | Alarm type. |
| **Alarm Name** | Name of the alarm. |
| **Description** | Description for the alarm. |
| **Suggested Actions** | Action to be performed when the alarm is triggered. |
| **Status** | Enable or disable the alarm rule. |

| Field Name | Description |
|---|---|
| **Severity** | Select the severity level for your alarm. Valid options are:<br>• Critical: Indicates a critical error condition.<br>• Warning: Indicates a normal but significant condition. This is the default condition.<br>• Info: Indicates an informational message. |
| **Send Syslog Message** | Send a syslog message for each system alarm that Cisco ISE-PIC generates. |
| **Enter multiple e-mails separated with comma** | List of e-mail addresses or ISE-PIC administrator names or both. |
| **Notes in Email (0 to 4000 characters)** | Custom text messages that you want associated with your system alarm. |

# Add Custom Alarms

Cisco ISE-PIC contains 5 default alarm types, such as Configuration Changed, High Disk I/O Utilization, High Disk Space Utilization, High Memory Utilization and ISE Authentication Inactivity. Cisco-defined system alarms are listed in the Alarms Settings page (Settings > Alarms Settings). You can only edit the system alarms.

In addition to the existing system alarms, you can add, edit, or delete custom alarms under the existing alarm types.

For each alarm type, you can create a maximum of 5 alarms and the total number of alarms is limited to 200.

To add an alarm:

### Procedure

**Step 1** Choose **Settings > Alarm Settings**.

**Step 2** In the **Alarm Configuration** tab, click **Add**.

**Step 3** Enter the required details. Refer to the Alarm Settings section for more information.

Based on the alarm type, additional attributes are displayed in the Alarm Configuration page. For example, Object Name, Object Type, and Admin Name fields are displayed for Configuration Changed alarms. You can add multiple instances of same alarm with different criteria.

**Step 4** Click **Submit**.

# TCP Dump Utility to Validate Incoming Traffic

The TCP Dump Utility sniffs packets that you can use to verify if the expected packet has reached a node. For example, when there is no incoming authentication or log indicated in the report, you may suspect that there is no incoming traffic, or that the incoming traffic cannot reach Cisco ISE. In such cases, you can run this tool to validate.

You can configure the TCP dump options and then collect data from the network traffic to help you troubleshoot a network issue.

## Use TCP Dump to Monitor Network Traffic

The TCP Dump window lists TCP dump process files that you create. You can create different files for different purposes, run them as needed, and delete them when you don't need them.

You can control the data that is collected by specifying size, number of files, and how long the process runs. If the process finishes before the time limit, and the file is less than the maximum size, and you enabled more than one file, then the process continues and creates another dump file.

You can run TCP dump on more interfaces, including bonded interfaces.

**Note** Human-readable format is no longer an option; the dump file is always in raw format.

### Before you begin

The **Network Interface** drop-down list in the **TCP Dump** window displays only the network interface cards (NICs) that have an IPv4 or IPv6 address configured. By default in VMware, all the NICs are connected, which means that all the NICs have an IPv6 address and are displayed in the **Network Interface** drop-down list.

### Procedure

**Step 1** From the **Host Name** drop-down list, choose the source for the TCP Dump utility.

**Step 2** From the **Network Interface** drop-down list, choose an interface to monitor.

**Step 3** In the **Filter** field, enter a boolean expression on which to filter.

The following are supported standard TCP dump filter expressions:

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

**Step 4** Enter a **File Name** for this TCP dump process.

**Step 5** From the **Repository** drop-down list, choose a repository to store TCP dump log files in.

**Step 6** From the **File Size** drop-down list—Select a maximum file size.

If the dump exceeds this file size, a new file opens to continue the dump. The number of times the dump can continue to a new file is limited by the **Limit to** setting.

**Step 7** The **Limit to** option can be used to limit the number of files that the dump can expand into.

**Step 8** The **Time Limit** option can be used to configure how long a dump runs before ending.

**Step 9** Set **Promiscuous Mode** by clicking **On** or **Off**. The default is **On**.

Promiscuous mode is the default packet sniffing mode in which the network interface passes all traffic to the system's CPU. We recommend that you leave it set to On.

# Save a TCP Dump File

### Before you begin

You should have successfully completed the task, as described in Using TCP Dump to Monitor network Traffic section.

**Note** You can also access TCP Dump through the Cisco ISE CLI. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

### Procedure

**Step 1** Click **Download**, corresponding to the desired location, and then click **Save**.

**Step 2** (Optional) To get rid of the previous dump file without saving it, click **Delete**.

# TCP Dump Settings

The following table describes the fields on the **tcpdump** utility page, which you use to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear. The navigation path for this page is: **Troubleshoot**.

***Table 25: TCP Dump Settings***

| Option | Usage Guidelines |
|---|---|
| Status | • Stopped—the tcpdump utility is not running<br>• Start—Click to start the tcpdump utility monitoring the networ<br>• Stop—Click to stop the tcpdump utility |
| Host Name | Choose the name of the host to monitor from the drop-down list. |

| Option | Usage Guidelines |
|---|---|
| Network Interface | Choose the network interface to monitor from the drop-down list.<br>**Note**<br>You must configure all network interface cards (NICs) with an IPv4 or IPv so that they are displayed in the Cisco ISE Admin portal. |
| Promiscuous Mode | • On—Click to turn on promiscuous mode (default).<br>• Off—Click to turn off promiscuous mode.<br>Promiscuous mode is the default packet sniffing mode. It is recommende leave it set to On. In this mode the network interface is passing all traffi system's CPU. |
| Filter | Enter a boolean expression on which to filter. Supported standard tcpdu expressions:<br>ip host 10.77.122.123<br>ip host 10.77.122.123 and not 10.177.122.119<br>ip host ISE123 |
| Format | Select a format for the tcpdump file. |
| Dump File | Displays data on the last dump file, such as the following:<br>Last created on Wed Apr 27 20:42:38 UTC 2011 by admin<br>`File size: 3,744 bytes`<br>`Format: Raw Packet Data`<br>`Host Name: Positron`<br>`Network Interface: GigabitEthernet 0`<br>`Promiscuous Mode: On`<br>• Download—Click to download the most recent dump file.<br>• Delete—Click to delete the most recent dump file. |

# Logging Mechanism

## Cisco ISE-PIC Logging Mechanism

### Configure Syslog Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

# Active Directory Troubleshooting

## Prerequisites for Integrating Active Directory and Cisco ISE-PIC

This section describes the manual steps required to configure Active Directory for integration with Cisco ISE-PIC. However, in most cases, you can enable Cisco ISE-PIC to automatically configure Active Directory. The following are the prerequisites to integrate Active Directory with Cisco ISE-PIC.

- Ensure you have Active Directory Domain Admin credentials, required to make changes to any of the AD domain configurations.
- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE-PIC server and Active Directory. You can configure NTP settings from Cisco ISE-PIC CLI.
- You must have at least one global catalog server operational and accessible by Cisco ISE-PIC, in the domain to which you are joining Cisco ISE-PIC.

### Active Directory Account Permissions Required to Perform Various Operations

| Join Operations | Leave Operations | Cisco ISE-PIC Machine Accounts |
|---|---|---|
| The join operation requires the following account permissions:<br>• Search Active Directory (to see if a Cisco ISE-PIC machine account exists)<br>• Create Cisco ISE-PIC machine account to domain (if the machine account does not already exist)<br>• Set attributes on the new machine account (for example, CiscoISE-PIC machine account password, SPN, dnsHostname) | The leave operation requires the following account permissions:<br>• Search Active Directory (to see if a Cisco ISE-PIC machine account exists)<br>• Remove the Cisco ISE-PIC machine account from the domain<br>If you perform a force leave (leave without the password), it will not remove the machine account from the domain. | The ISE-PIC machine account that communicates to the Active Directory connection requires the following permissions:<br>• Change password<br>• Read the user and machine objects corresponding to users and machines that are contacted<br>• Query Active Directory to get information (for example, trusted domains, alternative UPN suffixes, and so on)<br>• Read the tokenGroups attribute<br>You can precreate the machine account in Active Directory. If the SAM name matches the Cisco ISE-PIC appliance hostname, it is located during the join operation and re-used.<br>If there are multiple join operations, multiple machine accounts are maintained inside Cisco ISE-PIC, one for each join. |

**Note** The credentials that are used for the join or leave operation are not stored in Cisco ISE-PIC. Only the newly created Cisco ISE-PIC machine account credentials are stored.

The **Network access: Restrict clients allowed to make remote calls to SAM** security policy in Microsoft Active Directory has been revised. Hence, Cisco ISE might not able to update its machine account password every 15 days. If the machine account password is not updated, Cisco ISE will no longer authenticate users through Microsoft Active Directory. You will receive the **AD: ISE password update failed** alarm on your Cisco ISE dashboard to notify you of this event.

**Note** This issue happens in Windows Server 2016 Active Directory or later and Windows 10 version 1607 due to the restriction in them. To overcome this restriction, when you are integrating Windows Server 2016 Active Directory or later or Windows 10 version 1607 with Cisco ISE, you much set the registry value in the following registry from non-zero to blank to give access to all: Registry:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam This allows Cisco ISE to update its machine account password.

The security policy allows users to enumerate users and groups in the local Security Accounts Manager (SAM) database and in Microsoft Active Directory. To ensure Cisco ISE can update its machine account password, check that your configurations in Microsoft Active Directory are accurate. For more information on the Windows operating systems and Windows Server versions affected, what this means for your network, and what changes may be needed, see:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

## Network Ports that Must Be Open for Communication

| Protocol | Port (remote-local) | Target | Notes |
|---|---|---|---|
| DNS (TCP/UDP) | Random number greater than or equal to 49152 | DNS Servers/AD Domain Controllers | — |
| MSRPC | 445 | Domain Controllers | — |
| Kerberos (TCP/UDP) | 88 | Domain Controllers | MS AD/KDC |
| LDAP (TCP/UDP) | 389 | Domain Controllers | — |
| LDAP (GC) | 3268 | Global Catalog Servers | — |
| NTP | 123 | NTP Servers/Domain Controllers | — |
| IPC | 80 | For the secondary ISE-PIC node | — |

# Active Directory Requirements to Support ISE-PIC

ISE-PIC uses Active Directory login audit events generated by the Active Directory domain controller to gather user login information. The Active Directory server must be configured properly so the ISE user can connect and fetch the user login information. The following sections show how to configure the Active Directory domain controller (configurations from the Active Directory side) to support ISE-PIC.

To configure Active Directory domain controllers (configurations from the Active Directory side) to support , follow these steps:

**Note** You must configure all the domain controllers in all the domains.

1. Set up Active Directory join points and domain controllers from ISE-PIC (see Add an Active Directory Join Point and Join Cisco ISE-PIC Node to the Join Point, on page 20).
2. Perform the following steps from Active Directory:
   - Configure Active Directory for Passive Identity service, on page 163
3. (Optional) Troubleshoot automatic configurations performed by ISE on Active Directory with these steps:
   - Set Permissions when Microsoft Active Directory Users are in Domain Admin Group, on page 166
   - Permissions for Microsoft Active Directory Users Not in Domain Admin Group, on page 167
   - Permissions to Use DCOM on the Domain Controller, on page 168

## Configure Active Directory for Passive Identity service

ISE-PIC Active Directory login audit events generated by the Active Directory domain controller to gather user login information. ISE-PIC connects to Active Directory and fetches the user login information.

The following steps should be performed from the Active Directory domain controller:

### Procedure

**Step 1** Make sure relevant Microsoft patches are installed on the Active Directory domain controllers.

**Step 2** Make sure the Active Directory logs the user login events in the Windows Security Log.

Verify that the Audit Policy settings (part of the Group Policy Management settings) allows successful logons to generate the necessary events in the Windows Security Log (this is the default Windows setting, but you must explicitly ensure that this setting is correct).

**Step 3** You must have an Active Directory user with sufficient permissions for ISE-PIC to connect to the Active Directory. The following instructions show how to define permissions either for admin domain group user or none admin domain group user:

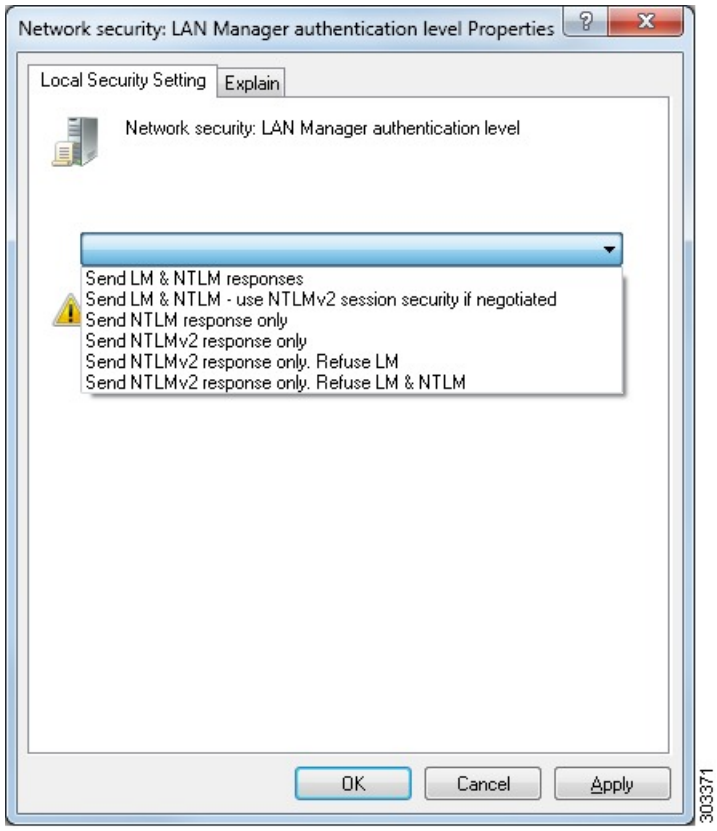
- Permissions Required when an Active Directory User is a Member of the Domain Admin Group
- Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group

**Step 4** The Active Directory user used by ISE-PIC can be authenticated either by NT Lan Manager (NTLM) v1 or v2. You need to verify that the Active Directory NTLM settings are aligned with ISE-PIC NTLM settings to ensure successful authenticated connection between ISE-PIC and the Active Directory Domain Controller. The following table shows all Microsoft NTLM options, and which ISE-PIC NTLM actions are supported. If ISE-PIC is set to NTLMv2, all six options described in are supported. If ISE-PIC is set to support NTLMv1, only the first five options are supported.

*Table 26: Supported Authentication Types Based on ISE-PIC and AD NTLM Version Settings*

| ISE-PIC NTLM Setting Options / Active Directory (AD) NTLM Setting Options NTLMv1 NTLMv2 | NTLMv1 | NTLMv2 |
|---|---|---|
| Send LM & NTLM responses connection is allowed connection is allowed | Connection is allowed | Connection is allowed |
| Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed | Connection is allowed | Connection is allowed |
| Send NTLM response only connection is allowed connection is allowed | Connection is allowed | Connection is allowed |
| Send NTLMv2 response only connection is allowed connection is allowed | Connection is allowed | Connection is allowed |
| Send NTLMv2 response only. Refuse LM connection is allowed connection is allowed | Connection is allowed | Connection is allowed |
| Send NTLMv2 response only. Refuse LM & NTLM connection is refused connection is allowed | Connection is refused | Connection is allowed |

*Figure 6: MS NTLM Authentication Type Options*




**Step 5** Make sure that you have created a firewall rule to allow traffic to `dllhost.exe` on Active Directory domain controllers.

You can either turn the firewall off, or allow access on a specific IP (ISE-PIC IP address) to the following ports:

- TCP 135: General RPC Port. When doing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- UDP 137: Netbios Name Resolution
- UDP 138: Netbios Datagram Service
- TCP 139: Netbios Session Service
- TCP 445: SMB

Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dllhost.exe as a target. This program manages ports dynamically.

All firewall rules can be assigned to specific IP (ISE-PIC IP).

## Set the Windows Audit Policy

Ensure that the **Audit Policy** (part of the **Group Policy Management** settings) allows successful logons. This is required to generate the necessary events in the Windows Security Log of the AD domain controller machine. This is the default Windows setting, but you must verify that this setting is correct.

### Procedure

**Step 1** Choose **Start** > **Programs** > **Administrative Tools** > **Group Policy Management**.

**Step 2** Navigate under Domains to the relevant domain and expand the navigation tree.

**Step 3** Choose **Default Domain Controller Policy**, right click and choose **Edit**.

The Group Policy Management Editor appears.

**Step 4** Choose **Default Domain Controllers Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.

- For Windows Server 2003 or Windows Server 2008 (non-R2), choose **Local Policies** > **Audit Policy**. For the two Policy items, **Audit Account Logon Events** and **Audit Logon Events**, ensure that the corresponding **Policy Setting** either directly or indirectly includes the **Success** condition. To include the Success condition indirectly, the **Policy Setting** must be set to **Not Defined**, indicating that the effective value will be inherited from a higher level domain, and the **Policy Setting** for that higher level domain must be configured to explicitly include the **Success** condition.
- For Windows Server 2008 R2 and Windows 2012, choose **Advanced Audit Policy Configuration** > **Audit Policies** > **Account Logon**. For the two Policy items, **Audit Kerberos Authentication Service** and **Audit Kerberos Service Ticket Operations**, ensure that the corresponding Policy Setting either directly or indirectly includes the Success condition, as described above.

  **Note**
  Cisco ISE uses RC4 cipher in Kerberos protocol while communicating with Active Directory, unless this encryption type is disabled in Active Directory Domain Controller configuration. You can use the **Network Security: Configure Encryption Types Allowed for Kerberos** option in Active Directory to configure the allowed encrytion types for Kerberos protocol.

**Step 5** If any Audit Policy item settings have been changed, you should then run `gpupdate /force` to force the new settings to take effect.

## Set Permissions when Microsoft Active Directory Users are in Domain Admin Group

For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the Domain Admin group does not have full control of certain registry keys in the Windows operating system by default. The Microsoft Active Directory administrator must give the Microsoft Active Directory user full control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following Microsoft Active Directory versions require no registry changes:

- Windows 2003

- Windows 2003R2
- Windows 2008

To grant full control, the Microsoft Active Directory admin must first take ownership of the key:

**Procedure**

**Step 1** Right-click the key icon and choose the **Owner** tab.

**Step 2** Click **Permissions**.

**Step 3** Click **Advanced**.

### Permissions for Microsoft Active Directory Users Not in Domain Admin Group

For Windows Server 2012 R2, give the Microsoft AD user full control permissions on the following registry keys:

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Use the following commands in Windows PowerShell to check if full permission is given to the registry keys:

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

The following permissions are required when a Microsoft AD user is not in the Domain Admin group, but is in the Domain Users group:

- Add registry keys to allow ISE-PIC to connect to the domain controller.
- Permissions to Use DCOM on the Domain Controller, on page 168
- Set Permissions for Access to WMI Root and CIMv2 Namespace, on page 170

These permissions are only required for the following Microsoft AD versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2

- Windows 2016

### Add Registry Keys to Allow ISE-PIC to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow ISE-PIC to connect as a domain user, and retrieve login authentication events. An agent is not required on the domain controllers or on any machines in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

Make sure that you include two spaces in the value of the DllSurrogate key. If the registry is manually updated, you must include only the two spaces and do not include the quotes. While updating the registry manually, ensure that quotes are not included for AppID, DllSurrogate, and its values.

Retain the empty lines as shown in the preceding script, including the empty line at the end of the file.

Use the following commands in the Windows command prompt to confirm if the registry keys are created and have the correct values:

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

## Permissions to Use DCOM on the Domain Controller

The Microsoft Active Directory user who is used for ISE-PIC Passive Identity service must have the permissions to use DCOM on the domain controller server. Configure permissions with the **dcomcnfg** command line tool.

### Procedure

**Step 1** Run the **dcomcnfg** tool from the command line.

**Step 2** Expand **`Component Services`**.

**Step 3** Expand **Computers** > **My Computer**.

**Step 4** Choose **Action** from the menu bar, click **Properties**, and click **COM Security**.

**Step 5** The account that Cisco ISE uses for both access and launch must have Allow permissions. Add the Microsoft Active Directory user to all the four options, **Edit Limits** and **Edit Default** for both **Access Permissions** and **Launch and Activation Permissions**.

**Step 6** Allow all local and remote accesses for both **Access Permissions** and **Launch and Activation Permissions**.

***Figure 7: Local and Remote Accesses for Access Permissions***

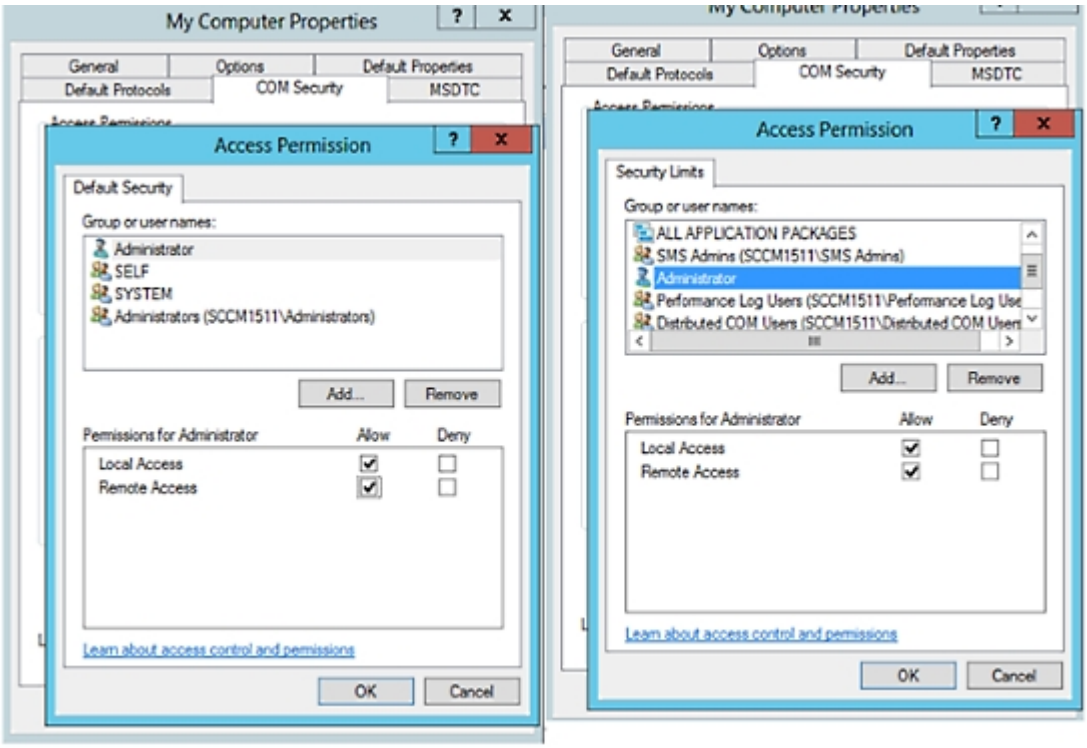
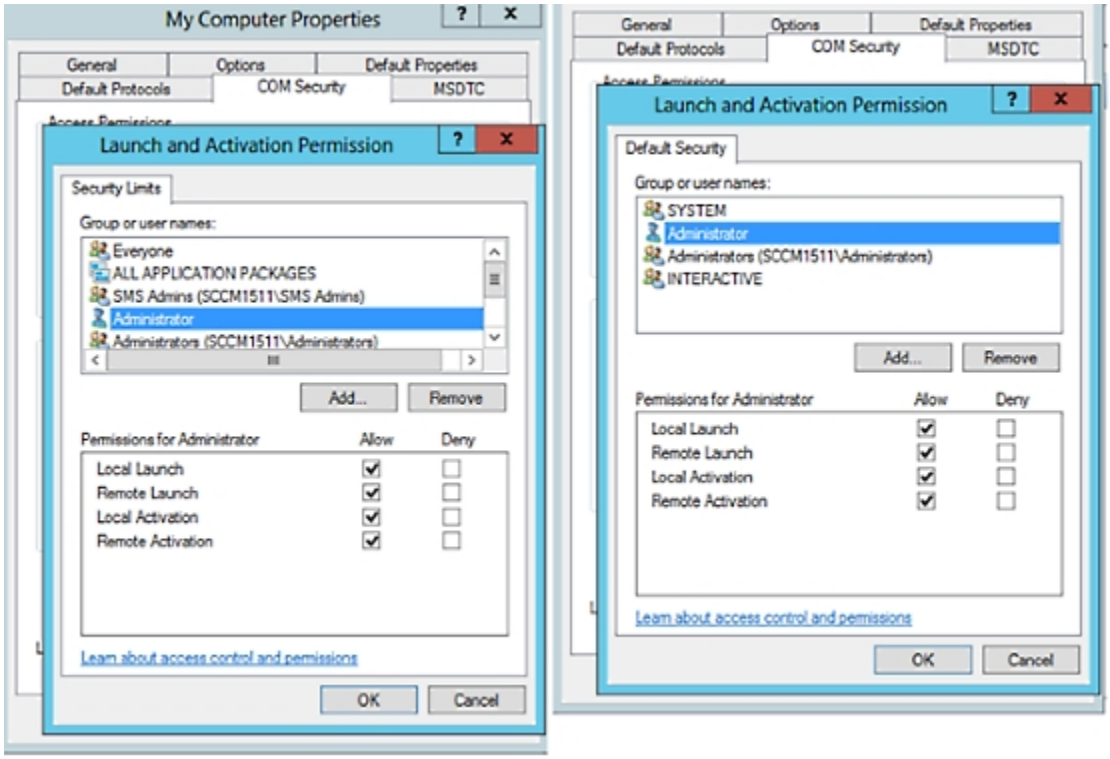


*Figure 8: Local and Remote Accesses for Launch and Activation Permissions*




## Set Permissions for Access to WMI Root and CIMv2 Namespace

By default, Microsoft Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmimgmt.msc MMC console.

### Procedure

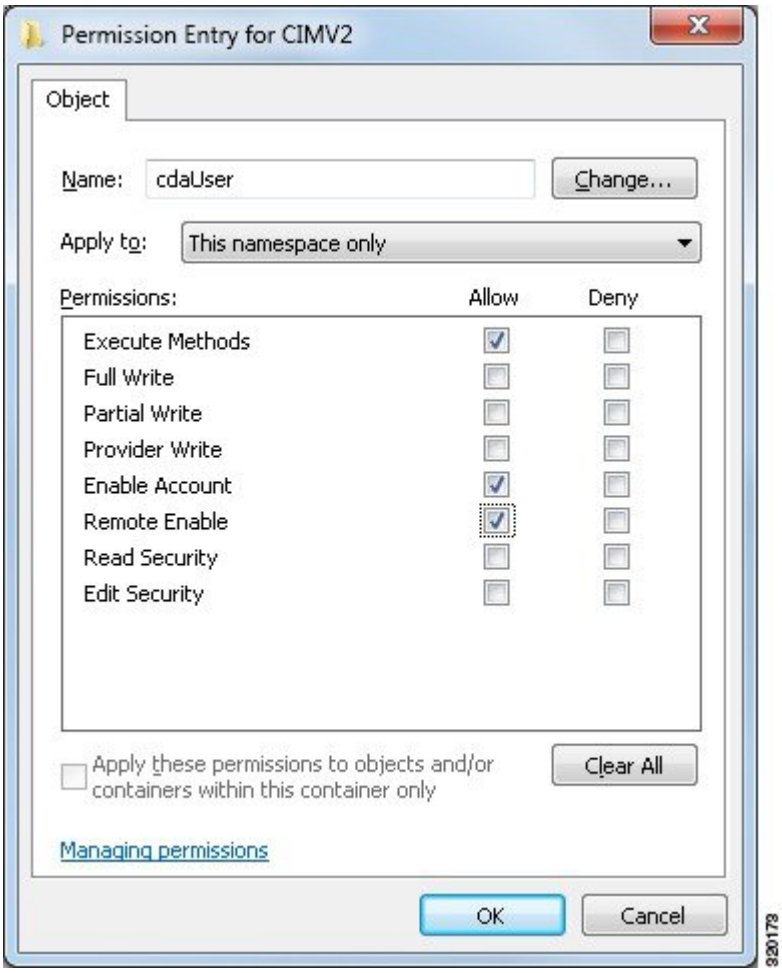
**Step 1** Choose **Start** > **Run** and enter `wmimgmt.msc`.

**Step 2** Right-click **WMI Control** and click **Properties**.

**Step 3** Under the **Security** tab, expand **Root** and choose **CIMV2**.

**Step 4** Click **Security**.

**Step 5** Add the Microsoft Active Directory user, and configure the required permissions as shown in the following image.




## Grant Access to the Security Event Log in the AD Domain Controller

On Windows 2008 and later, you can grant access to the AD Domain controller logs by adding the ISE-PIC ID Mapping user to a group called Event Log Readers.

On all older versions of Windows, you must edit a registry key, as shown below.

### Procedure

**Step 1** To delegate access to the Security event logs, find the SID for the account .

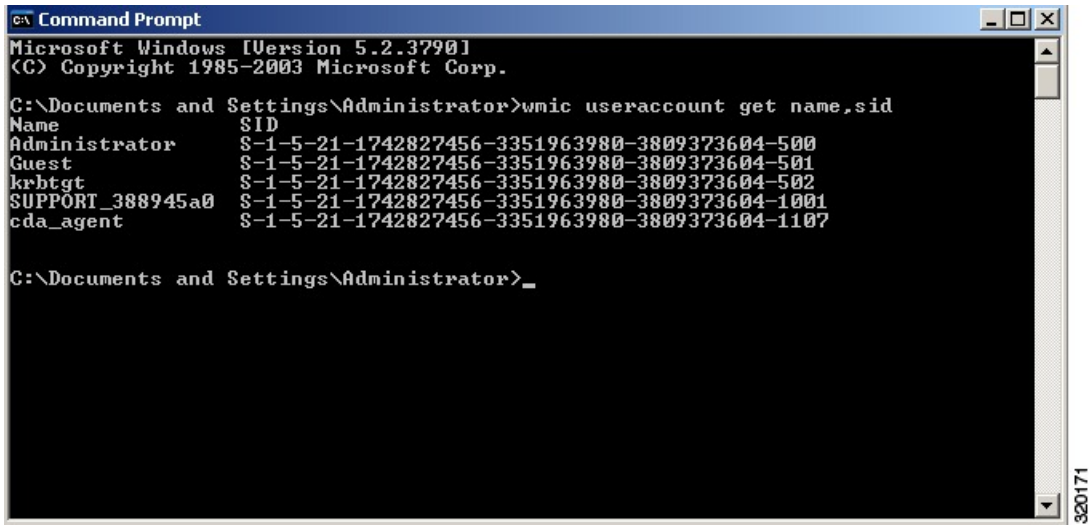
**Step 2** Use the following command from the command line, also shown in the diagram below, to list all the SID accounts.

```
wmic useraccount get name,sid
```

You can also use the following command for a specific username and domain:

```
wmic useraccount where name="iseUser" get domain,name,sid
```

*Figure 9: List All the SID Accounts*



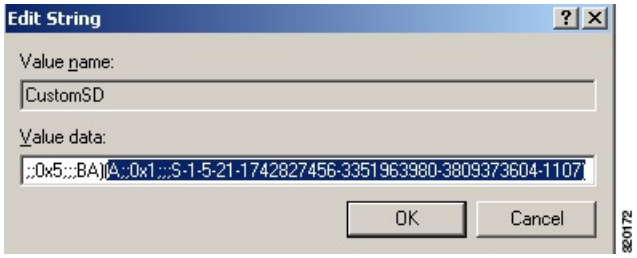

**Step 3** Find the SID, open the Registry Editor, and browse to the following location:

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

**Step 4** Click on **Security**, and double click **CustomSD**.

For example, to allow read access to the ise_agent account `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`, enter `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`.

*Figure 10: Edit CustomSD String*




**Step 5** Restart the WMI service on the Domain Controller. You can restart the WMI services in the following two ways:

a) Run the following commands from the CLI:

**net stop winmgmt**

**net start winmgmt**

b) Run `Services.msc`, which opens the Windows Services Management tool. In the Windows Services Management window, locate the **Windows Management Instrumentation** service, right click, and select **Restart**.

# Obtaining Additional Troubleshooting Information

Cisco ISE-PIC allows you to download support and troubleshooting information from the Admin portal. You can use the support bundles to prepare diagnostic information for the Cisco Technical Assistance Center (TAC) to troubleshoot problems with Cisco ISE-PIC.

**Note** The support bundles and debug logs provide advanced troubleshooting information for TAC and are difficult to interpret. You can use the various reports and troubleshooting tools that Cisco ISE-PIC provides to diagnose and troubleshoot issues that you are facing in your network.

## Cisco ISE-PIC Support Bundle

You can configure the logs that you want to be a part of your support bundle. For example, you can configure logs from a particular service to be a part of your debug logs. You can also filter the logs based on dates.

The logs that you can download are categorized as follows:

- Full configuration database: Contains the Cisco ISE-PIC configuration database in a human-readable XML format. When you troubleshoot issues, you can import this database configuration into another Cisco ISE node to re-create the scenario.
- Debug logs: Captures bootstrap, application configuration, run-time, deployment, public key infrastructure (PKI) information, and monitoring and reporting.

  Debug logs provide troubleshooting information for specific Cisco ISE components. To enable debug logs, see chapter 11 on *Logging*. If you do not enable the debug logs, all the informational messages (INFO) will be included in the support bundle. For more information, see Cisco ISE-PIC Debug Logs, on page 175.
- Local logs: Contains syslog messages from the various processes that run on Cisco ISE.
- Core files: Contains critical information that helps identify the cause of a crash. These logs are created when the application crashes, and includes heap dumps.
- Monitoring and reporting logs: Contains information about alerts and reports.
- System logs: Contains Cisco Application Deployment Engine-related (ADE-related) information.
- Policy configuration: Contains policies configured in Cisco ISE in human-readable format.

You can download these logs from the Cisco ISE CLI by using the **backup-logs** command. For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

If you choose to download these logs from the Admin portal, you can do the following:

- Download only a subset of logs based on the log type, such as debug logs or system logs.
- Download only the latest *n* number of files for the selected log type. This option allows you to control the size of the support bundle and the time taken for download.

Monitoring logs provide information about the monitoring, reporting, and troubleshooting features. For more information about downloading logs, see Download Cisco ISE-PIC Log Files, on page 174.

# Support Bundle

You can download the support bundle to your local computer as a simple tar.gpg file. The support bundle will be named with the date and time stamps in the format ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg. The browser prompts you to save the support bundle to an appropriate location. You can extract the content of the support bundle and view the README.TXT file, which describes the contents of the support bundle, as well as how to import the contents of the ISE database if it is included in the support bundle.

# Download Cisco ISE-PIC Log Files

You can download the Cisco ISE-PIC log files to look for more information while troubleshooting issues in your network.

You can also download system logs that include ADE-OS and other log files to troubleshoot installation and upgrade issues.

### Before you begin

- You should have configured the debug logs and debug log levels.

### Procedure

**Step 1** Choose **Administration** > **Logging** > **Download Logs** > **Appliance node list**.

**Step 2** Click the node from which you want to download the support bundles.

**Step 3** In the **Support Bundle** tab, choose the parameters that you want to be populated in your support bundle.

If you include all the logs, your support bundle will be excessively large and the download will take a long time. To optimize the download process, choose to download only the most recent *n* number of files.

**Step 4** Enter the **From** and **To** dates for which you want to generate the support bundle.

**Step 5** Choose one of the following:

- **Public Key Encryption**: Choose this option if you want to provide the support bundle to Cisco TAC for troubleshooting purposes.
- **Shared Key Encryption**: Choose this option if you want to troubleshoot the issues locally on premise. If you choose this option, you must enter the encryption key for the support bundle.

**Step 6** Click **Create Support Bundle**.

**Step 7** Click **Download** to download the newly-created support bundle.

The support bundle is a tar.gpg file that is downloaded to the client system that is running your application browser.

### What to do next

Download debug logs for specific components.

# Cisco ISE-PIC Debug Logs

Debug logs provide troubleshooting information for various Cisco ISE-PIC components. Debug logs contain critical and warning alarms generated over the last 30 days, and information alarms generated over the last seven days. While reporting problems, you might be asked to enable these debug logs and send them for diagnosis and resolution of your problems.

**Note** Enabling debug logs with heavy load (such as monitoring debug logs) will generate alarms about high load.

## Obtain Debug Logs

**Procedure**

**Step 1** Configure the components for which you want to obtain debug logs. See Cisco ISE-PIC Components and Corresponding Debug Logs, on page 175.

**Step 2** Download the debug logs.

## Cisco ISE-PIC Components and Corresponding Debug Logs

**Note**
The list below is a complete list of components available in Cisco ISE. Some of the components listed in the table may not be relevant for ISE-PIC

*Table 27: Components and Corresponding Debug Logs*

| Component | Debug Log |
|---|---|
| Active Directory | ad_agent.log |
| Cache Tracker | tracking.log |
| Entity Definition Framework (EDF) | edf.log |
| JMS | ise-psc.log |
| License | ise-psc.log |
| Notification Tracker | tracking.log |
| Replication-Deployment | replication.log |
| Replication-JGroup | replication.log |
| Replication Tracker | tracking.log |
| RuleEngine-Attributes | ise-psc.log |
| RuleEngine-Policy-IDGroups | ise-psc.log |
| accessfilter | ise-psc.log |

| Component | Debug Log |
|---|---|
| admin-infra | ise-psc.log |
| boot-strap wizard | ise-psc.log |
| cellular-config | ise-psc.log |
| cellular-config-api | api-service.log |
| cellular-config-ui | ise-psc.log |
| cellular-mnt | collector.log |
| cisco-mnt | ise-psc.log |
| client | ise-psc.log |
| cpm-clustering | ise-psc.log |
| cpm-mnt | ise-psc.log |
| epm-pdp | ise-psc.log |
| epm-pip | ise-psc.log |
| anc | ise-psc.log |
| anc | ise-psc.log |
| ers | ise-psc.log |
| guest | ise-psc.log |
| Guest Access Admin | guest.log |
| Guest Access | guest.log |
| MyDevices | guest.log |
| Portal | guest.log |
| Portal-Session-Manager | guest.log |
| Portal-web-action | guest.log |
| guestauth | ise-psc.log |
| guestportal | ise-psc.log |
| identitystore-AD | ise-psc.log |
| infrastructure | ise-psc.log |
| ipsec | ise-psc.log |
| ipsec-api | api-service.log |
| ipsec-ui | ise-psc.log |
| mdm | ise-psc.log |
| mdm-pip | ise-psc.log |

| Component | Debug Log |
|---|---|
| mnt-report | reports.log |
| mydevices | ise-psc.log |
| nsf | ise-psc.log |
| nsf-session | ise-psc.log |
| org-apache | ise-psc.log |
| org-apache-cxf | ise-psc.log |
| org-apache-digester | ise-psc.log |
| posture | ise-psc.log |
| profiler | profiler.log |
| provisioning | ise-psc.log |
| policy-engine | ise-psc.log |
| policy-engine-timelog | policy-eval-time.log |
| prrt-JNI | prrt-management.log |
| runtime-AAA | prrt-management.log |
| runtime-config | prrt-management.log |
| runtime-logging | prrt-management.log |
| sponsorportal | ise-psc.log |
| swiss | ise-psc.log |
| telemetry | sch.log |

# Download Debug Logs

**Procedure**

**Step 1** Choose **Administration** > **Logging** > **Download Logs**.

**Step 2** From the Appliance node list, click the node for which you want to download the debug logs.

**Step 3** Click the **Debug Logs** tab.

A list of debug log types and debug logs is displayed. This list is based on your debug log configuration.

**Step 4** Click the log file that you want to download and save it to the system that is running your client browser.

You can repeat this process to download other log files as needed. The following are the additional debug logs that you can download from the **Debug Logs** window:

- isebootstrap.log: Provides bootstrapping log messages
- monit.log: Provides watchdog messages

- pki.log: Provides third-party crypto library logs
- iseLocalStore.log: Provides logs about the local store files
- ad_agent.log: Provides Microsoft Active Directory third-party library logs
- catalina.log: Provides third-party logs

# Additional References

The following link contains additional resources that you can use when working with Cisco ISE:
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

# Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact 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 DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.