Getting Started with ISE-PIC

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*.

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 102 and earlier versions from version 82
- Mozilla Firefox ESR 91.3 and earlier versions
- Google Chrome 103 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

Administrator Lockout Because of Login Attempts

If you enter an incorrect password for an administrator user ID enough times, the account is either suspended for a specified time or locked out (as configured). If Cisco ISE is configured to lock you out, the administration portal locks you out of the system. Cisco ISE adds a log entry in the Server Administrator Logins report and suspends the credentials for that administrator ID. Reset the password for that administrator ID as described in the Section "Reset a Disabled Password Due to Administrator Lockout" in the Cisco Identity Services Engine Installation Guide. The number of failed login attempts allowed before an administrator account is disabled is configured as described in the Section Administrative Access to Cisco ISE-PIC of the *Cisco Identity Services Engine Administrator Guide*. After an administrator user account is locked out, Cisco ISE sends an email to the associated user, if this information is configured.

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 Cisco ISE-PIC Licensing, on page 3.
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 5.
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
5. Configure a single or multiple subscribers. For more information, see Subscribers

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

Cisco ISE-PIC Licensing

Cisco ISE-PIC is offered with a 90-day evaluation period. To continue to use Cisco ISE-PIC after the 90-day evaluation license expires, you must obtain and register a license on your system. ISE-PIC will notify you of evaluation license expiration 90, 60 and 30 days in advance.

Each perpetual license is uploaded to a single ISE-PIC node and a separate license is required for the second node, if you have two nodes in the deployment. Generate a separate license for each UDI and then add the licenses to each node separately, once you have completed installation.

Licensing Installation and Registration Flow

1. Install and register your ISE-PIC license. For more information about installing and registering your ISE-PIC license, see Register Licenses, on page 4. You can install the license either:
   - Immediately after ISE-PIC installation.
   - Anytime during the 90-day evaluation period.
2. Easily upgrade to a base ISE deployment by first installing a Cisco ISE-PIC upgrade license and then:
   - Installing a Base ISE license in order to use the former ISE-PIC node as the primary administrative node (PAN) for your deployment.
   - Adding the upgraded PIC ISE-PIC node to an already existing ISE deployment.
3. Easily upgrade your base ISE deployment and upgrade to smart licensing, by installing any other relevant licenses (Plus, Apex, TACACs+, and so on). For more information about installing ISE licenses, see the *Cisco Identity Services Engine Administrator Guide*.

Cisco ISE Licensing Packages

Table 1: All Cisco ISE Licensing Package Options

ISE License Packages	Perpetual/Subscription (Terms Available)	ISE 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	This license allows these options: • Enable additional (up to 300,000) parallel sessions. • Upgrade to full ISE instance	One license per node. Each license supports up to 300,000 parallel sessions. After installing this license, the upgraded node can then join an existing ISE deployment or alternatively, base licenses can then be installed on the node in order to function as the PAN.

Base	Perpetual	• Basic network access: AAA, IEEE-802.1X • Guest services • Link encryption (MACSec) • TrustSec • ISE Application Programming Interfaces	
Evaluation	Temporary (90 days)	Enables full ISE-PIC functionality for 90 days.	

Register Licenses

Before you begin

Once you have installed ISE-PIC, you have a 90-day evaluation period. You must purchase, register and install your ISE-PIC licenses in order to continue working smoothly. If you have not registered and installed licenses prior to expiration, then when you access ISE-PIC after expiration, all ISE-PIC services are disabled and you are automatically navigated to the **Import License** area, from which you can complete the process. Consult your Cisco partner/account team about the ISE-PIC licenses.

Step 1 From the ordering system (Cisco Commerce Workspace - CCW) on Cisco's website www.cisco.com, order the required licenses. You need one ISE-PIC license for each node in the deployment (a maximum of two nodes per deployment).

After about an hour, an email confirmation containing the Product Authorization Key (PAK) is sent.

Step 2 From the Cisco ISE-PIC Administration portal, choose **Administration** > **Licensing**. Make a note of the node information in the **Licensing Details** section: Product Identifier (PID), Version Identifier (VID), and Serial Number (SN).

Step 3

Step 4 Go to www.cisco.com/go/licensing, and where prompted, enter the PAK of the license you received, the node information, and some details about your company.

After one day, Cisco sends you the license file.

Step 5 Save this license file to a known location on your system.

Step 6 From the Cisco ISE-PIC Administration portal, choose **Administration** > **Licensing**.

Step 7 In the **Licenses** section, click the **Import License** button.

Step 8 Click **Choose File** and select the license file you previously stored on your system.

Step 9 Click **Import**.

The new license is now installed on your system.

What to do next

Choose the licensing dashboard, **Administration** > **Licensing**, and verify that the newly-entered license appears with the correct details.

Remove Licenses

Before you begin

Removing expired or unnecessary licenses eliminates popup reminders, and reclaims space on the Licensing dashboard.

Step 1 Choose **Administration** > **Licensing**

Step 2 In the **License Files** section, click the check next to the relevant file name, and click **Delete License**.

Step 3 Click **OK**.

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.

Step 1 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 Check the **Only allow authenticated NTP servers** check box to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time.

Step 4 (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. Specify whether the key in question is trusted by checking or unchecking the **Trusted Key** check box, and click **OK**. The **Key ID** field supports numeric values between 1 to 65535 and the **Key Value** field supports up to 15 alphanumeric characters.

c) Click **OK**.

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

Step 5 (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 6 Click **Save**.

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.