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 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 2.
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.

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).

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 • 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 • MACsec • Authentications that are based on Single Sign-On (SSO), Security Assertion Markup Language (SAML), and Open DataBase Connectivity (ODBC) standards • Guest access and sponsor services • Representational State Transfer (REST) APIs for monitoring purposes, and External RESTful Services APIs for CRUD operations • Passive ID services • 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.

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.

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 15 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.