Administer Cisco ISE

- Administrator Access Console, on page 1
- Specify Proxy Settings in Cisco ISE, on page 2
- Ports Used by the Admin Portal, on page 3
- Enable External RESTful Services APIs, on page 3
- External RESTful Services SDK, on page 4
- Specify System Time and NTP Server Settings, on page 5
- Changing the System Time Zone, on page 6
- Configure SMTP Server to Support Notifications, on page 6
- Cisco ISE Deployment Upgrade, on page 7
- Cisco ISE Software Patches, on page 10
- Roll Back Software Patches, on page 12
- View Patch Install and Rollback Changes, on page 13
- FIPS Mode Support, on page 13
- Securing SSH Key Exchange Using Diffie-Hellman Algorithm, on page 18
- Configure Cisco ISE to Send Secure Syslog, on page 18
- Default Secure Syslog Collector, on page 20
- Offline Maintenance, on page 20

Administrator Access Console

The following steps describe how to log into the Administrative portal.

**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 case-sensitive password, that was 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 Login page and follow the instructions.

---

**Related Topics**

Administrator Login Browser Support, on page 2
Administrator Login Browser Support

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

- Mozilla Firefox 69 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 77 and earlier versions
- Microsoft Edge beta 77 and earlier versions
- Microsoft Internet Explorer 10.x and 11.x

If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).

ISE Community Resource

ISE Pages Fail to Fully Load When Adblock Plus is Used

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for an administrator user ID enough times, the account would either be suspended for a specified time or locked out (as configured). If you choose to get locked out, the Admin 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. You can reset the password for that administrator ID, as described in the "Reset a Disabled Password Due to Administrator Lockout" section in the Cisco Identity Services Engine Installation Guide. The number of allowed failed attempts before disabling the administrator account is configurable and is described in the Administrative Access to Cisco ISE section in the Cisco Identity Services Engine Administrator Guide. After an administrator user account is locked out, Cisco ISE sends e-mail to the associated administrator user, if configured.

Disabled System administrators' status can be enabled by any Super Admin, including Active Directory users.

Specify Proxy Settings in Cisco ISE

If your existing network topology requires you to use a proxy for Cisco ISE, to access external resources (such as the remote download site where you can find client provisioning and posture-related resources), you can use the Admin portal to specify proxy properties.

The proxy settings impact the following Cisco ISE functions:

- Partner Mobile Management
- Endpoint Profiler Feed Service Update
- Endpoint Posture Update
- Endpoint Posture Agent Resources Download
- CRL (Certificate Revocation List) Download
- Guest Notifications

The Cisco ISE proxy configuration supports basic authentication for proxy servers. NT LAN Manager (NTLM) authentication is not supported.
Step 1  Choose Administration > System > Settings > Proxy.
Step 2  Enter the proxy IP address or DNS-resolvable host name and specify the port through which proxy traffic travels to and from Cisco ISE in **Proxy host server : port**.
Step 3  Check **Password required** check box, if required.
Step 4  Enter the user name and password used to authenticate to the proxy servers in the **User Name** and **Password** fields.
Step 5  Enter the IP address or address range of hosts or domains to be bypassed in **Bypass proxy for these hosts and domain**.
Step 6  Click **Save**.

**Ports Used by the Admin Portal**

The Admin portal is set to use HTTP port 80 and HTTPS port 443, and you cannot change these settings. Cisco ISE also prevents you from assigning any of the end-user portals to use the same ports, which reduces the risk to the Admin portal.

**Enable External RESTful Services APIs**

The External RESTful Services APIs are based on HTTPS protocol and REST methodology and uses port 9060.

The External RESTful Services APIs support basic authentication. The authentication credentials are encrypted and are part of the request header.

You can use any REST client like JAVA, curl, linux command, python or any other client to invoke External RESTful Services API calls.

The ISE administrator must assign special privileges to a user to perform operations using the External RESTful Services APIs. To perform operations using the External RESTful Services APIs (except for the Guest API), the users must be assigned to one of the following Admin Groups and must be authenticated against the credentials stored in the Cisco ISE internal database (internal admin users):

- External RESTful Services Admin—Full access to all ERS APIs (GET, POST, DELETE, PUT). This user can Create, Read, Update, and Delete ERS API requests.
- External RESTful Services Operator—Read Only access (GET request only).

**Note**

The Super Admin user can access all ERS APIs.

The External RESTful Services APIs are not enabled by default. If you try to evoke the External RESTful Services API calls before enabling them, you will receive an error response. 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.
Step 1 Choose Administration > Settings > ERS Settings.

Step 2 Choose Enable ERS for Read/Write for the Primary Administration Node.

Step 3 Choose Enable ERS for Read for All Other Nodes if there are any secondary nodes.

External RESTful Service requests of all types are valid only for the primary ISE node. Secondary nodes have read-access (GET requests).

Step 4 Select one of the following options:

- Use CSRF Check for Enhanced Security—If this option is enabled, the ERS client must send a GET request to fetch the Cross-Site Request Forgery (CSRF) token from Cisco ISE and include the CSRF token in the requests sent to Cisco ISE. Cisco ISE will validate the CSRF token when a request is received from the ERS client. Cisco ISE processes the request only if the token is valid. This option is not applicable for pre ISE 2.3 Clients.

- Disable CSRF for ERS Request—If this option is enabled, CSRF validation is not performed. This option can be used for pre ISE 2.3 Clients.

Step 5 Click Submit.

All REST operations are audited and the logs are logged in the system logs. External RESTful Services APIs have a debug logging category, which you can enable from the debug logging page of the Cisco ISE GUI.

When you disable External RESTful Services in Cisco ISE, port 9060 remains open but no communication is allowed through the port.

Related Topics

External RESTful Services SDK, on page 4

External RESTful Services SDK

You can use the External RESTful Services SDK to start building your own tools. You can access the External RESTful Services SDK from the following URL: https://<ISE-ADMIN-NODE>:9060/ers/sdk. External RESTful Services SDK can be accessed by the External RESTful Services Admin users only.

The SDK consists the following components:

- Quick reference API documentation
- Complete list of all available API operations
- Schema files available for download
- Sample application in Java available for download
- Use cases in curl script format
- Use cases in python script format
- Instructions on using Chrome Postman
Specify System Time and NTP Server Settings

Cisco ISE allows you to configure up to three Network Time Protocol (NTP) servers. You can use the NTP servers to maintain accurate time and synchronize time across different time zones. You can also specify whether or not Cisco ISE should use only authenticated NTP servers, and you can enter one or more authentication keys for that purpose.

Cisco recommends that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone—especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Cisco ISE also supports public-key authentication for NTP servers. NTPv4 uses symmetric-key cryptography and also provides a new Autokey scheme based on public-key cryptography. Public-key cryptography is generally considered more secure than symmetric-key cryptography because the security is based on a private value, which is generated by each server and never revealed. With Autokey, all key distribution and management functions involve only public values, which considerably simplifies key distribution and storage.

You can configure Autokey for NTP server from the Cisco ISE CLI in Configuration Mode. We recommend that you use the IFF (identify Friend or Foe) Identification scheme as this scheme is most widely used.

Before you begin

You must have either the Super Admin or System Admin administrator role assigned.

If you have both a primary and a secondary Cisco ISE node, you must log in to the user interface of the secondary node and configure the system time and NTP server settings on each Cisco ISE node in your deployment individually.

Step 1  Choose Administration > System > Settings > System Time.

Step 2  Enter unique IP addresses (IPv4/IPv6/FQDN) for your NTP servers.

Step 3  Check the Only allow authenticated NTP servers check box if you want to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time.

Step 4  (Optional) If you want 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 requires authentication via an authentication key, as follows:

   a)  Click Add.

   b)  Enter the necessary Key ID and Key Value, specify whether the key in question is trusted by activating or deactivating the Trusted Key option, and click OK. The Key ID field supports numeric values between 1 to 65535 and the Key Value field supports up to 15 alphanumerical characters.

   c)  Return to the NTP Server Configuration tab when you are finished entering the NTP Server Authentication Keys.

Step 5  (Optional) If you want to authenticate the NTP server using public-key authentication, configure Autokey on Cisco ISE from the command-line interface (CLI). See the ntp server and crypto commands in the Cisco Identity Services Engine CLI Reference Guide for your release of ISE for more details.

Step 6  Click Save.
Changing the System Time Zone

Once set, you cannot edit the time zone from the Admin portal. To change the time zone setting, you must enter the following command in the Cisco ISE CLI:

```
clock timezone timezone
```

**Note**
Cisco ISE uses POSIX-style signs in the time zone names and the output abbreviations. Therefore, zones west of Greenwich have a positive sign and zones east of Greenwich have a negative sign. For example, `TZ='Etc/GMT+4'` corresponds to 4 hours behind Universal Time (UT).

**Caution**
Changing the time zone on a Cisco ISE appliance after installation requires ISE services to be restarted on that particular node. Hence we recommend that you perform such changes within a maintenance window. Also, it is important to have all the nodes in a single ISE deployment configured to the same time zone. If you have ISE nodes located in different geographical locations or time zones, you should use a global time zone such as UTC on all the ISE nodes.

For more information on the `clock timezone` command, refer to the *Cisco Identity Services Engine CLI Reference Guide*.

Configure SMTP Server to Support Notifications

Configure a Simple Mail Transfer Protocol (SMTP) server to send email notifications for alarms, to enable sponsors to send email notification to guests with their login credentials and password reset instructions, and to enable guests to automatically receive their login credentials after they successfully register themselves and with actions to take before their guest accounts expire.

Which ISE Nodes Send Email

The following list shows which node in a distributed ISE environment sends email.

<table>
<thead>
<tr>
<th>Email Purpose</th>
<th>Node That Sends the Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest expiration</td>
<td>Primary PAN</td>
</tr>
<tr>
<td>alarms</td>
<td>Active MnT</td>
</tr>
<tr>
<td>sponsor and guest notifications from guest and sponsor portals</td>
<td>PSN</td>
</tr>
<tr>
<td>password expirations</td>
<td>Primary PAN</td>
</tr>
</tbody>
</table>

**Step 1** Choose Administration > System > Settings > SMTP Server.

**Step 2** Choose Settings > SMTP Server.
Step 3  Enter the hostname of the outbound SMTP server in the SMTP server field. This SMTP host server must be accessible from the Cisco ISE server. The maximum length for this field is 60 characters.

Step 4  Choose one of these options:

- Use email address from Sponsor to send guest notification email from the email address of the sponsor and choose Enable Notifications.

- Use the default email address to specify a specific email address from which to send all guest notifications and enter it in the Default email address field.

Step 5  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>.

Cisco ISE Deployment Upgrade

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified and the progress of the upgrade and the status of the nodes are displayed on screen. Refer to the Cisco Identity Services Engine Upgrade Guide for a list of pre and post upgrade tasks.

The Upgrade Overview page lists all the nodes in your deployment, the personas that are enabled on them, the version of ISE installed, and the status (indicates whether a node is active or inactive) of the node. You can begin upgrade only if the nodes are in the Active state.

Different Types of Deployment

- Standalone Node—A single Cisco ISE node assuming the Administration, Policy Service, and Monitoring persona.

- Multi-Node Deployment—A distributed deployment with several ISE nodes. The procedure to upgrade a distributed deployment is discussed in the following listed references.

ISE Community Resource
For information on how to assess the network for ISE deployment readiness, see ISE Deployment Assistant (IDA).

Upgrade a Distributed Deployment

You can upgrade all the nodes in a Cisco ISE deployment using the Admin portal from Release 2.0 onwards, you can also upgrade a Limited Availability Release of Cisco ISE 2.0 or later to the General Availability Release.
Before you begin

**Note**

If you are upgrading a Cisco ISE STANDALONE node or have de-registered a node from an existing deployment and wish to run a STANDALONE upgrade, then prior to starting the upgrade, there is a need to remove all the upgraded db_* .properties files located in the path: "/opt/oracle/base/admin/cpm10/dpdump".

Please contact Cisco TAC for deleting the above mentioned files, as root privilege is required to remove them. See CSCvi87302 for details.

The above workaround is required only if the upgrade file (ise-upgradebundle-2.0.x-2.3.x-to-2.4.0.357.SPA.x86_64.tar.gz) is downloaded before April 13, 2018.

Ensure that you have performed the following tasks before you upgrade:

- Obtain a backup of the ISE configuration and operational data.
- Obtain a backup of the system logs.
- Disable scheduled backups. Reconfigure the backup schedules after deployment upgrade is complete.
- Export the certificates and private keys.
- Configure a repository. Download the upgrade bundle and place it in the repository.
- Make a note of Active Directory join credentials and RSA SecurID node secret, if applicable. You need this information to connect to Active Directory or RSA SecurID server after upgrade.
- Purge the operational data to improve upgrade performance.
- Ensure that your Internet connection to the repository is good.

**Note**

When you download an upgrade bundle from a repository to a node, the download times out if it takes more than 35 minutes to complete. This issue occurs because of poor Internet bandwidth.

---

**Step 1**
Click the Upgrade tab in the Admin portal.

**Step 2**
Click Proceed.

The Review Checklist window appears. Read the given instructions carefully.

**Step 3**
Check the I have reviewed the checklist check box, and click Continue.

The Download Bundle to Nodes window appears.

**Step 4**
Download the upgrade bundle from the repository to the nodes:

a) Check the check box next to the nodes to which you want to download the upgrade bundle.

b) Click Download.

The Select Repository and Bundle window appears.

   - c) Select the repository.
You can select the same repository or different repositories on different nodes, but you must select the same upgrade bundle on all the nodes.

d) Check the check box next to the bundle that you want to use for the upgrade.  
e) Click Confirm.  

Once the bundle is downloaded to the node, the node status changes to Ready for Upgrade.

Step 5  
Click Continue.  

The Upgrade Nodes window appears.  

Figure 1: Upgrade Window Showing the Current Deployment and the New Deployment

Step 6  
Choose the upgrade sequence.  

When you move a node to the new deployment, a time estimate for the upgrade is displayed on the Upgrade Nodes window. You can use this information to plan for upgrade and minimize downtime. Use the sequence given below if you have a pair of Administration and Monitoring Nodes, and several Policy Service Nodes.  

a) By default, the Secondary Administration Node is listed first in the upgrade sequence. After upgrade, this node becomes the Primary Administration Node in the new deployment.  
b) The Primary Monitoring Node is the next one in the sequence to be upgraded to the new deployment.  
c) Select the Policy Service Nodes and move them to the new deployment. You can alter the sequence in which the Policy Service Nodes are upgraded.  

You can upgrade the Policy Service Nodes in sequence or in parallel. You can select a set of Policy Service Nodes and upgrade them in parallel.  

d) Select the Secondary Monitoring Node and move it to the new deployment.  
e) Finally, select the Primary Administration Node and move it to the new deployment.  

Step 7  
Check the Continue with upgrade on failure check box if you want to continue with the upgrade even if the upgrade fails on any of the Policy Service Nodes in the upgrade sequence.  

This option is not applicable for the Secondary Administration Node and the Primary Monitoring Node. If any one of these nodes fail, the upgrade process is rolled back. If any of the Policy Service Nodes fail, the Secondary Monitoring Node and the Primary Administration Node are not upgraded and remain in the old deployment.  

Step 8  
Click Upgrade to begin the deployment upgrade.
The upgrade progress is displayed for each node. On successful completion, the node status changes to **Upgrade Complete**.

**Note**  When you upgrade a node from the Admin portal, if the status does not change for a long time (and remains at 80%), you can check the upgrade logs from the CLI or the status of the upgrade from the console. Log in to the CLI or view the console of the Cisco ISE node to view the progress of upgrade. You can use the **show logging application** command to view the upgrade-uibackend-cliconsole.log and upgrade-postosupgrade-yyyyymmdd-xxxxxx.log.

You can view the following upgrade logs from the CLI using the show logging application command:

- DB Data Upgrade Log
- DB Schema Log
- Post OS Upgrade Log

In case you get a warning message: **The node has been reverted back to its pre-upgrade state**, go to the Upgrade window, click the **Details** link. Address the issues that are listed in the **Upgrade Failure Details** window. After you fix all the issues, click **Upgrade** to reinitiate the upgrade.

**Note**  If the posture data update process is running on the Primary Administration Node in the new deployment, you cannot register a node to the Primary Administration Node. You can either wait till the posture update process is over (which might take approximately 20 minutes) or disable the posture auto-update feature from the **Administration > System > Settings > Posture > Updates** page while upgrading or registering a node to the new deployment.

---

**Cisco ISE Software Patches**

Cisco ISE software patches are usually cumulative. Cisco ISE allows you to perform patch installation and rollback from CLI or GUI.

You can install patches on Cisco ISE 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 are installing the patch from the GUI, the patch is automatically installed on the Primary PAN first. The system then installs the patch on the other nodes in the deployment in the order listed in the GUI. You cannot control the order in which the nodes are updated.

If you are installing the patch from the CLI, you can control the order in which the nodes are updated. However, we recommend that you install the patch on the Primary PAN first.

If you want to validate the patch on some of the nodes before upgrading the entire deployment, you can use the CLI to install the patch on selected nodes. Use the following CLI command to install the patch:

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

You can install the required patch version directly. For example, if you are currently using Cisco ISE 2.x and would like to install Cisco ISE 2.x patch 5, you can directly install Cisco ISE 2.x patch 5, without installing the previous patches (in this example, Cisco ISE 2.x patches 1 – 4).

**Related Topics**

- Software Patch Installation Guidelines, on page 11
- Install a Software Patch, on page 12
- Software Patch Installation Guidelines, on page 11
- Software Patch Rollback Guidelines, on page 13
- Install a Software Patch, on page 12
- Roll Back Software Patches, on page 12

---

**Software Patch Installation Guidelines**

When you install a patch on an 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 version that is deployed in your network. Cisco ISE reports any mismatch in versions as well as any errors in the patch file.

You cannot install a patch with a version that is lower than the patch that is currently installed on Cisco ISE. Similarly, you cannot roll back changes of a lower-version patch if a higher version is currently installed on Cisco ISE. For example, if patch 3 is installed on your Cisco ISE 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 distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment. If the patch installation is successful on the Primary PAN, Cisco ISE then continues patch installation on the secondary nodes. If it fails on the Primary PAN, the installation does not proceed to the secondary nodes. However, if the installation fails on any of the secondary nodes for any reason, it still continues with the next secondary node in your deployment.

When you install a patch from the Primary PAN that is part of a two-node deployment, Cisco installs the patch on the primary node and then on the secondary node. If the patch installation is successful on the Primary PAN, Cisco then continues patch installation on the secondary node. If it fails on the Primary PAN, the installation does not proceed to the secondary node.
# Install a Software Patch

**Before you begin**

- You must have the Super Admin or System Admin administrator role assigned.
- Go to Administration > System > Deployment > PAN Failover, and ensure that the Enable PAN Auto Failover check box is unchecked. The PAN auto-failover configuration must be disabled for the duration of this task.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Maintenance &gt; Patch Management &gt; Install.</td>
</tr>
<tr>
<td>2</td>
<td>Click Browse and choose the patch that you downloaded from Cisco.com.</td>
</tr>
<tr>
<td>3</td>
<td>Click Install to install the patch. After the patch is installed on the PAN, Cisco ISE logs you out and you have to wait for a few minutes before you can log in again. <strong>Note</strong> When patch installation is in progress, Show Node Status is the only function that is accessible on the Patch Management page.</td>
</tr>
<tr>
<td>4</td>
<td>Choose Administration &gt; System &gt; Maintenance &gt; Patch Management to return to the Patch Installation page.</td>
</tr>
<tr>
<td>5</td>
<td>Click the radio button next to the patch that you have installed on any secondary node and click Show Node Status to verify whether installation is complete.</td>
</tr>
</tbody>
</table>

**What to do next**

If you need to install the patch on one or more secondary nodes, ensure that the nodes are up and repeat the process to install the patch on the remaining nodes.

# Roll Back Software Patches

When you roll back a patch from the PAN that is part of a deployment with multiple nodes, Cisco ISE rolls back the patch on the primary node and then all the secondary nodes in the deployment.

**Before you begin**

- You must have either the Super Admin or System Admin administrator role assigned.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Maintenance &gt; Patch Management.</td>
</tr>
<tr>
<td>2</td>
<td>Click the radio button for the patch version whose changes you want to roll back and click Rollback. <strong>Note</strong> When a patch rollback is in progress, Show Node Status is the only function that is accessible on the Patch Management page. After the patch is rolled back from the PAN, Cisco ISE logs you out and you have to wait a few minutes before you can log in again.</td>
</tr>
</tbody>
</table>
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 Choose Administration > System > Maintenance > Patch Management.

Step 5 To view the progress of the patch rollback, choose the patch in the Patch Management page and click Show Node Status.

Step 6 Click the radio button for the patch and click Show Node Status on a secondary node to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process to roll back the changes from the remaining nodes. Cisco ISE only rolls back the patch from the nodes that still have this version of the patch installed.

**Related Topics**

Software Patch Rollback Guidelines, on page 13

**Software Patch Rollback Guidelines**

To roll back a patch from Cisco ISE 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 nodes. If the rollback process fails on the PAN, the patches are not rolled back from the secondary nodes. However, if the patch rollback fails on any secondary node, it still continues to roll back the patch from the next secondary node in your deployment.

While Cisco ISE rolls back the patch from the secondary nodes, you can continue to perform other tasks from the PAN GUI. The secondary nodes will be restarted after the rollback.

**View Patch Install and Rollback Changes**

To view reports related to installed patches, perform the following steps.

**Before you begin**

You must have either the Super Admin or System Admin administrator role assigned. You can install or rollback patches in the Administration > System > Maintenance > Patch Management page. You can also view the status (installed/in-progress/not installed) of a particular patch on each node in the deployment, by selecting a specific patch and clicking the Show Node Status button.

**Related Topics**

Software Patch Rollback Guidelines, on page 13

**FIPS Mode Support**

ISE FIPS 140 mode initializes the Cisco FIPS Object Module cryptographic module into FIPS 140-2 mode. Cisco Identity Services Engine uses embedded FIPS 140-2 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.
When the FIPS mode is enabled, the Cisco ISE administrator interface displays a FIPS mode icon at the left of the node name in the upper-right corner of the page.

If Cisco ISE detects the use of a protocol or certificate that is not supported by the FIPS 140-2 standard, it displays a warning with the name of the protocol or certificate that is noncompliant, and the FIPS mode is not enabled. Ensure that you choose only FIPS-compliant protocols and replace non-FIPS compliant certificates before you enable the FIPS mode.

The FIPS standard places limitations on the use of certain algorithms. Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. When the FIPS mode is enabled, any function that uses non-FIPS compliant algorithms will fail.

The certificates installed in Cisco ISE must be re-issued if the encryption method used in the certificates is not supported by FIPS.

When you enable the FIPS mode, the following functions are affected:

- IEEE 802.1X environment
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-Transport Layer Security (EAP-TLS)
  - PEAP
  - RADIUS

  **Note**
  Other protocols like EAP-Message Digest 5 (EAP-MD5), Lightweight Extensible Authentication Protocol (LEAP), and PAP are not compatible with FIPS 140-2 standards and are disabled when the FIPS mode is enabled. Local Web Authentication (LWA), a legacy method of guest access uses PAP and will not work when the FIPS mode is enabled. However, if Host Lookup is used in Allowed Protocols for MAC Authentication Bypass (MAB), guess access with Central Web Authentication (CWA) will work.

- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)
- Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. When the FIPS mode is enabled, any function that uses non-FIPS compliant algorithm will fail.

Guest is not supported in FIPS mode. Enabling FIPS mode also automatically disables Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) protocols, which the guest login function of Cisco ISE requires.

Once the FIPS Mode is enabled, all the nodes in the deployment are rebooted automatically. Cisco ISE performs a rolling restart by first restarting the Primary PAN and then restarting each of the secondary node, one at a time. Hence, it is recommended that you plan for the downtime before changing the configuration.

**Tip**
We recommend that you do not enable FIPS mode before completing any database migration process.
Enable FIPS Mode in Cisco ISE

To enable the FIPS mode:

**Step 1** Choose **Administration > System > Settings > FIPS Mode**.

**Step 2** Choose the **Enabled** option from the **FIPS Mode** drop-down list.

**Step 3** Click **Save** and restart your machine.

### What to do next

After you enable FIPS mode, enable and configure the following FIPS 140-2 compliant functions:

- Generate a Self-Signed Certificate
- Create a Certificate Signing Request and Submit the CSR to a Certificate Authority
- See the Network Device Definition Settings section in
- Configure RADIUS authentication settings under Network Device Definition Settings

In addition, you may want to enable administrator account authorization using a Common Access Card (CAC) function. Although using CAC functions for authorization is not strictly a FIPS 140-2 requirement, it is a well-known secure-access measure that is used in a number of environments to bolster FIPS 140-2 compliance.

### Configure Cisco ISE for Administrator CAC Authentication

#### Before you begin

Before beginning configuration, do the following:

- (Optional) Turn on FIPS mode. FIPS mode is not required for certificate-based authentication, but the two security measures often go hand-in-hand. If you do plan to deploy Cisco ISE in a FIPS 140-2 compliant deployment and to use CAC certificate-based authorization as well, be sure to turn FIPS mode on and specify the appropriate private keys and encryption/decryption settings first.

- Ensure that the domain name server (DNS) in Cisco ISE is set for Active Directory.

- Ensure that Active Directory user and user group membership has been defined for each administrator certificate.

To ensure that Cisco ISE can authenticate and authorize an administrator based on the CAC-based client certificate that is submitted from the browser, be sure that you have configured the following:

- The external identity source (Active Directory in the following example)
- The user groups in Active Directory to which the administrator belongs
- How to find the user's identity in the certificate
- Active Directory user groups to Cisco ISE RBAC permissions mapping
- The Certificate Authority (trust) certificates that sign the client certificates
Configure Cisco ISE for Administrator CAC Authentication

- A method to determine if a client certificate has been revoked by the CA

You can use a Common Access Card (CAC) to authenticate credentials when logging into Cisco ISE.

---

**Step 1**
Enable FIPS mode. You will be prompted to restart your system after you enable the FIPS mode. You can defer the restart if you are going to import CA certificates as well.

**Step 2**
Configure an Active Directory identity source in Cisco ISE and join all Cisco ISE nodes to Active Directory.

**Step 3**
Configure a certificate authentication profile according to the guidelines.

Be sure to select the attribute in the certificate that contains the administrator user name in the Principal Name X.509 Attribute field. (For CAC cards, the Signature Certificate on the card is normally used to look up the user in Active Directory. The Principal Name is found in this certificate in the "Subject Alternative Name" extension, specifically in a field in that extension that is called "Other Name." So the attribute selection here should be "Subject Alternative Name - Other Name.")

If the AD record for the user contains the user's certificate, and you want to compare the certificate that is received from the browser against the certificate in AD, check the Binary Certificate Comparison check box, and select the Active Directory instance name that was specified earlier.

**Step 4**
Enable Active Directory for Password-Based Admin Authentication. Choose the Active Directory instance name that you connected and joined to Cisco ISE earlier.

*Note* You must use password-based authentication until you complete other configurations. Then, you can change the authentication type to client certificate based at the end of this procedure.

**Step 5**
Create an External Administrator Group and map it to an Active Directory Group. Choose Administration > System > Admin Access > Administrators > Admin Groups. Create an external system administrator group.

**Step 6**
Configure an admin authorization policy to assign RBAC permissions to the external admin groups.

*Caution* We strongly recommend that you create an external Super Admin group, map it to an Active Directory group, and configure an admin authorization policy with Super Admin permissions (menu access and data access), and create at least one user in that Active Directory Group. This mapping ensures that at least one external administrator has Super Admin permissions once Client Certificate-Based Authentication is enabled. Failure to do this may lead to situations where the Cisco ISE administrator is locked out of critical functionality in the Admin Portal.

**Step 7**
Choose Administration > System > Certificates > Certificate Store to import certificate authority certificates into the Cisco ISE certificate trust store.

Cisco ISE does not accept a client certificate unless the CA certificates in the client certificate’s trust chain are placed in the Cisco ISE Certificate Store. You must import the appropriate CA certificates in to the Cisco ISE Certificate Store.

a) Click **Browse** to choose the certificate.
b) Check the Trust for client authentication check box.
c) Click **Submit**.

Cisco ISE prompts you to restart all the nodes in the deployment after you import a certificate. You can defer the restart until you import all the certificates. However, after importing all the certificates, you must restart Cisco ISE before you proceed.

**Step 8**
Configure the certificate authority certificates for revocation status verification.

a) Choose Administration > System > Certificates > OSCP Services.
b) Enter the name of an OSCP server, an optional description, and the URL of the server.

c) Choose Administration > System > Certificates > Certificate Store.

d) For each CA certificate that can sign a client certificate, specify how to do the revocation status check for that CA. Choose a CA certificate from the list and click Edit. On the edit page, choose OCSP and/or CRL validation. If you choose OCSP, choose an OCSP service to use for that CA. If you choose CRL, specify the CRL Distribution URL and other configuration parameters.

Step 9 Enable client certificate-based authentication. Choose Administration > System > Admin Access > Authentication.

a) Choose Client Certificate Based authentication type on the Authentication Method tab.

b) Choose the certificate authentication profile that you configured earlier.

c) Select the Active Directory instance name.

d) Click Save.

Here, you switch from password-based authentication to client certificate-based authentication. The certificate authentication profile that you configured earlier determines how the administrator’s certificate is authenticated. The administrator is authorized using the external identity source, which in this example is Active Directory.

The Principal Name attribute from the certificate authentication profile is used to look up the administrator in Active Directory.

You have now configured Cisco ISE for administrator CAC authentication.

---

Related Topics

- Supported Common Access Card Standards, on page 17
- Common Access Card Operation in Cisco ISE, on page 17

---

Supported Common Access Card Standards

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee. Access via the CAC requires a card reader into which you insert the card and enter a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Windows Internet Explorer Version 8 and 9 users running the Windows 7 operating system must install the ActiveIdentity ActivClient Version 6.2.0.133 third-party middleware software product for Cisco ISE to interoperate with CAC. For more information on ActiveIdentity security client products, refer to ActivID ActivClient Security Software Datasheet.

Common Access Card Operation in Cisco ISE

The Admin portal can be configured so that your authentication with Cisco ISE is permitted only by using a client certificate. Credentials-based authentication—such as providing a user ID and password—is not permitted. In client certificate authentication, you insert a Common Access Card (CAC) card, enter a PIN and then enter the Cisco ISE Admin portal URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes your login session, based on the contents of the certificate. If this process is successful, you are presented with the Cisco ISE Monitoring and Troubleshooting home page and given the appropriate RBAC permissions.
Securing SSH Key Exchange Using Diffie-Hellman Algorithm

You can configure Cisco ISE to only allow Diffie-Hellman-Group14-SHA1 SSH key exchanges. To do this, you must enter the following commands from the Cisco ISE Command-Line Interface (CLI) Configuration Mode:

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

Here’s an example:

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

Configure Cisco ISE to Send Secure Syslog

To configure Cisco ISE to send only TLS-protected secure syslog between the Cisco ISE nodes and to the Monitoring nodes, you must perform the following tasks:

**Before you begin**

- Ensure that all the Cisco ISE nodes in your deployment are configured with appropriate server certificates. If you want your setup to be FIPS 140-2 compliant, the certificate keys must have a key size of 2048 bits or greater.

- Enable the FIPS mode in the Admin portal.

- Ensure that the default network access authentication policy does not allow any version of the SSL protocol. Use the TLS protocol in the FIPS mode along with FIPS-approved algorithms.

- Ensure that all the nodes in your deployment are registered with the Primary PAN. Also, ensure that at least one node in your deployment has the Monitoring persona enabled to function as the secure syslog receiver (TLS server).

**Step 1** Configure secure syslog remote logging target.

**Step 2** Enable Logging Categories to send auditable events to the secure syslog remote logging target.

**Step 3** Disable TCP Syslog and UDP syslog collectors. Only TLS-protected syslog collectors should be enabled.

**Related Topics**

- Configure Secure Syslog Remote Logging Target, on page 18
- Enable Logging Categories to Send Auditable Events to the Secure Syslog Target, on page 19
- Disable the TCP Syslog and UDP Syslog Collectors, on page 20

Configure Secure Syslog Remote Logging Target

Cisco ISE system logs are collected and stored by log collectors for various purposes. You must choose the Cisco ISE Monitoring node as your log collector for configuring a secure syslog target.
Step 1 Log into the Admin portal.
Step 2 Choose Administration > System > Logging > Remote Logging Targets.
Step 3 Click Add.
Step 4 Enter a name for the secure syslog server.
Step 5 Choose Secure Syslog from the Target Type drop-down list.
Step 6 Choose Enabled from the Status drop-down list.
Step 7 Enter the IP address of the Cisco ISE Monitoring node in your deployment.
Step 8 Enter 6514 as the port number. The secure syslog receiver listens on TCP port 6514.
Step 9 Choose the syslog facility code. The default is LOCAL6.
Step 10 Check the Buffer Messages When Server is Down check box. If this option is checked, Cisco ISE stores the logs if the secure syslog receiver is unreachable, periodically checks the secure syslog receiver, and forwards them when the secure syslog receiver comes up.
   a) Enter the buffer size.
   b) Enter the Reconnect Timeout in seconds for Cisco ISE to periodically check the secure syslog receiver.
Step 11 Select a CA certificate that you want Cisco ISE to present to the secure syslog server.
Step 12 Uncheck the Ignore Server Certificate validation check box. You must not check this option.
Step 13 Click Submit.

Enable Logging Categories to Send Auditable Events to the Secure Syslog Target

You must enable logging categories for Cisco ISE to send auditable events to the secure syslog target.

Step 1 Log in to the Admin portal.
Step 2 Choose Administration > System > Logging > Logging Categories.
Step 3 Click the radio button next to the AAA Audit logging category, then click Edit.
Step 4 Choose WARN from the Log Severity Level drop-down list.
Step 5 Move the secure syslog remote logging target that you created earlier to the Selected box.
Step 6 Click Save.
Step 7 Repeat this procedure to enable the following logging categories:
   • Administrative and Operational Audit
   • Posture and Client Provisioning Audit
Disable the TCP Syslog and UDP Syslog Collectors

For Cisco ISE to send only secure syslog between the ISE nodes, you must disable the TCP and UDP syslog collectors, and enable only the secure syslog collector.

**Step 1**
Log in to the Admin portal.

**Step 2**
Choose *Administration > System > Logging > Remote Logging Targets*.

**Step 3**
Click the radio button next to the TCP or UDP syslog collector.

**Step 4**
Click *Edit*.

**Step 5**
Choose Disabled from the Status drop-down list.

**Step 6**
Click *Save*.

**Step 7**
Repeat this process until you disable all the TCP or UDP syslog collectors.

---

Default Secure Syslog Collector

Cisco ISE provides default secure syslog collectors for the MnT nodes. By default, no logging categories are mapped to these default secure syslog collectors. The default secure syslog collectors are named as follows:

- Primary MnT node—SecureSyslogCollector
- Secondary MnT node—SecureSyslogCollector2

You can view this information on the Remote Logging Targets page (Administration > System > Logging). You cannot delete the default syslog collectors and cannot update the following fields for the default syslog collectors: Name, Target type, IP/Host address, and Port.

During a fresh Cisco ISE installation, "Default Self-signed Server Certificate" from the system will be added to the Trust Store and marked for “Trust for Client authentication and Syslog” usage, thereby making it available for secure syslog usage. While configuring your deployment or updating the certificates, you must assign relevant certificates to the secure syslog targets.

During upgrade if there are any existing secure syslog targets pointing to MnT nodes on port 6514, the same name and configuration will be retained, but after upgrade you cannot delete these syslog targets and cannot edit the following fields: Name, Target type, IP/Host address, and Port. If no such targets exist at the time of upgrade, default secure syslog targets will be created similar to fresh installation scenario without any certificate mapping. You can assign relevant certificates to these syslog targets. If you try to map a secure syslog target that is not mapped to any certificate, to a logging category, the following message will be displayed:

> Please configure the certificate for *log_target_name*

Offline Maintenance

If the maintenance time period is less than an hour, take the ISE node offline and perform the maintenance task. When you bring the node back online, PAN will automatically synchronize all the changes that happened
during maintenance time period. If the changes are not synchronized automatically, you can manually synchronize it with the PAN.

If the maintenance time period is more than an hour, de-register the node at the time of maintenance and re-register the node when you add the node back to deployment.

We recommend that you schedule the maintenance at a time period during which the activity is low.

1. Data replication issue may occur if the queue contains more than 1,000,000 messages or if the ISE node is offline for more than 6 hours.
2. If you are planning to perform maintenance on primary MnT node, we recommend that you take operational backup of the MnT node before performing maintenance activities.