Administrator Access Console

The following steps describe how to log in to 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 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

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" 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.

Only an administrator with the role of Super Admin (including Microsoft Active Directory users) can configure the disable administrator access option.

Configure Proxy Settings in Cisco ISE

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

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
- Certificate Revocation List (CRL) Download
- Guest Notifications
- SMS Message Transmission
- Social Login
- Microsoft Entra ID
- pxGrid Cloud

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 hostname, and specify the port through which proxy traffic travels to and from Cisco ISE in the **Proxy host server : port** field.

Step 3 Check the **Password required** check box, if necessary.

Step 4 Enter the username and password that are used to authenticate to the proxy servers in the **User Name** and **Password** fields. Reenter the password in the **Confirm Password** field.

Step 5 Enter the IP address or the address range of hosts or domains that must be bypassed in the **Bypass proxy for these hosts and domain** text box.

Step 6 Click **Save**.

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.

Enable External RESTful Services Application Programming Interface

The External RESTful Services application programming interfaces (API) are based on HTTPS protocols and REST methodology and use 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.

Note The ERS APIs support TLS 1.1 and TLS 1.2. ERS APIs do not support TLS 1.0 regardless of enabling TLS 1.0 in the **Security Settings** window (**Administration** > **System** > **Settings** > **Security Settings**). Enabling TLS 1.0 in the **Security Settings** window is related to the EAP protocol only and does not impact ERS APIs.

You must assign special privileges to a user to allow the 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 user must be assigned to either **ERS Admin** or **ERS Operator**administrator group. The user must be authenticated against the credentials that are stored in the Cisco ISE internal database (internal admin users).

- **ERS Admin**: This user can create, read, update, and delete External RESTful Services API requests. They have full access to all External RESTful Services APIs (GET, POST, DELETE, PUT).
- **ERS Operator**: This user has read-only access (GET requests only).

Note A user with the role Super Admin can access all External RESTful Services APIs.

ERS session idle timeout is 60 sec. If several requests are sent during this period, the same session is used with the same Cross-Site Request Forgery (CSRF) token. If the session has been idle for more than 60 sec, the session is reset and a new CSRF token is used.

The External RESTful Services APIs are disabled by default. If you evoke the External RESTful Services API calls before enabling them, you will receive an error response. Enable the Cisco ISE REST API feature for the 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 administration server, the client application receives a timeout error from the server for any Guest REST API requests.

Step 1 Choose **Administration** > **System** > **Settings** > **ERS Settings**.

Step 2 Click the **Enable ERS for Read/Write** radio button to enable External RESTful Services on the Primary Administration node (PAN).

Step 3 Click the **Enable ERS for Read for All Other Nodes** radio button if there are any secondary nodes in your deployment.

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

Step 4 In the **CSRF Check** area, click the radio button for one of the following options:

- **Use CSRF Check for Enhanced Security**: If this option is enabled, the External RESTful Services client must send a GET request to fetch the CSRF token from Cisco ISE and include the CSRF token in the requests that are sent to Cisco ISE. Cisco ISE will validate a CSRF token when a request is received from the External RESTful Services client. Cisco ISE processes the request only if the token is valid. This option is not applicable for External RESTful Services clients earlier than Cisco ISE Release 2.3.

- **Disable CSRF for ERS Request**: If this option is enabled, CSRF validation is not performed. This option can be used for External RESTful Services clients earlier than Cisco ISE 2.3.

Step 5 Click **Save**.

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 window in 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 Software Development Kit , on page 4

External RESTful Services Software Development Kit

Use the External RESTful Services (ERS) software development kit (SDK) to build your own tools. You can access the External RESTful Services SDK with the URL https://<ISE-ADMIN-NODE>:9060/ers/sdk. Only users with the role **ERS Admin** can access the External RESTful Services SDK.

The SDK consists of the following components:

- Quick reference API documentation.
- A 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 Network Time Protocol Server Settings

Cisco ISE 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 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 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 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.

Before you begin

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

If you have both primary and secondary Cisco ISE nodes in your deployment, log in to the user interface of each node and configure the system time and Network Time Protocol (NTP) server settings.

Step 1 Choose **Administration** > **System** > **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**.

Change the System Time Zone

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

clock timezone *timezone*

For more information about the **clock timezone** command, see Cisco Identity Services Engine CLI Reference Guide.

Note Cisco ISE uses Portable Operating System Interface (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 When you change the time zone on a Cisco ISE appliance after installation, Cisco ISE services restart on that particular node. We recommend that you perform such changes within a maintenance window. Also, it is important to have all the nodes in a single Cisco ISE deployment that is configured to the same time zone. If you have Cisco ISE nodes located in different geographical locations or time zones, you should use a global time zone such as UTC on all the Cisco ISE nodes.

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.

Email Purpose	Node That Sends the Email
guest expiration	Primary PAN
alarms	Active MnT
sponsor and guest notifications from guest and sponsor portals	PSN
password expirations	Primary PAN

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>.

Federal Information Processing Standards Mode Support

Cisco ISE uses embedded Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules Cisco Common Cryptographic Module (Certificate #1643 and Certificate #2100). For details of the FIPS compliance claims, see 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 top-right corner of the window.

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 fail.

The certificates that are installed in Cisco ISE must be re-issued if the cryptographic algorithms or their parameters that are used in the certificates are 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
- Lightweight Directory Access Protocol (LDAP) over 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 a non-FIPS-compliant algorithm fails.

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 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 the database migration process.

Enable Federal Information Processing Standards Mode in Cisco ISE

To enable the FIPS mode in Cisco ISE:

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

Step 2 Choose **Enabled** 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 compliant functions:

- Generate a Self-Signed Certificate.
- Create a Certificate-Signing Request and Submit it to a Certificate Authority.
- Configure RADIUS authentication settings as mentioned under Network Device Definition Settings.

You may want to enable administrator account authorization using a Common Access Card function. Although using Common Access Card functions for authorization is not strictly a FIPS 140 requirement, it is a well-known secure-access measure that is used in several environments to bolster FIPS 140 compliance.

Configure Cisco ISE for Administrator Common Access Card Authentication

Before you begin

- (Optional) Enable the FIPS mode in Cisco ISE. FIPS mode is not required for certificate-based authentication, but the two security measures often go hand-in-hand. If you plan to deploy Cisco ISE in a FIPS 140 compliant deployment and use Common Access Card certificate-based authorization, enable the FIPS mode 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 memberships have been defined for each administrator certificate.

To ensure that Cisco ISE can authenticate and authorize an administrator based on the Common Access Card-based client certificate that is submitted from the browser, configure the following:

- The external identity source (Active Directory in the following example).
- The Active Directory user groups 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.
- A method to determine if a client certificate has been revoked by the certificate authority.

You can use a Common Access Card to authenticate credentials when logging in to Cisco ISE.

Step 1 When you enable FIPS mode, you are prompted to restart your system. You can defer the restart if you are going to import certificate authority 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 username in the **Principal Name X.509 Attribute** field. For Common Access 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 the **Other Name** area of the extension. So the attribute selection here should be **Subject Alternative Name - Other Name**.

If the Active Directory 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 Active Directory, 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 administrator 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 administrator authorization policy to assign RBAC permissions to the external administrator groups.

Caution We strongly recommend that you create an external Super Admin group, map it to an Active Directory group, and configure an administrator 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 administration portal.

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

Cisco ISE does not accept a client certificate unless the certificate authority certificates in the client certificate's trust chain are placed in the Cisco ISE Certificates store. You must import the appropriate certificate authority certificates in to the Cisco ISE Certificates store.

a) Click **Import** and click **Choose File** in the **Certificate File** area.
b) Check the **Trust for client authentication and Syslog** 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 Client Profile**.
b) Click **Add**.
c) Enter the name of an OSCP server, an optional description, and the URL of the server in the corresponding fields.
d) Choose **Administration** > **System** > **Certificates** > **Certificate Store**.
e) For each certificate authority certificate that can sign a client certificate, specify how to do the revocation status check for that certificate authority. Choose a certificate authority certificate from the list and click Edit. On the edit page, choose OCSP or certificate revocation list (CRL) validation, or both. If you choose OCSP, choose an OCSP service to use for that certificate authority. 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) In the **Authentication Method** tab, click the **Client Certificate Based** radio button.
b) Choose the certificate authentication profile that you configured earlier from the **Certificate Authentication Profile** drop-down list.
c) Select the Active Directory instance name from the **Identity Source** drop-down list.
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.

Supported Common Access Card Standards

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card authentication devices. A Common Access Card is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee. Access via the Common Access Card 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.

Common Access Card Operation in Cisco ISE

You can configure the administration portal so that Cisco ISE authentications occur only through a client certificate. Credentials-based authentication that requires user IDs or passwords is not permitted. In client certificate-based authentication, you insert a Common Access Card card, enter a PIN, and then enter the Cisco ISE administration 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, the Cisco ISE Monitoring and Troubleshooting home page is displayed and you are given the appropriate RBAC permissions.

Secure SSH Key Exchange Using Diffie-Hellman Algorithm

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

Configure Cisco ISE to Send Secure Syslog

Before you begin

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

- Ensure that all the Cisco ISE nodes in your deployment are configured with appropriate server certificates. For your setup to be FIPS 140 compliant, the certificate keys must have a key size of 2048 bits or greater.
- Enable the FIPS mode in the administration 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 on it to function as the secure syslog receiver (TLS server).
- Check the supported RFC standards for syslogs. See Cisco Identity Services Engine Network Component Compatibility guide for your Cisco ISE release.

Step 1 Configure a 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 must be enabled.

Configure Secure Syslog Remote Logging Target

Cisco ISE system logs are collected and stored by log collectors for various purposes. To configure a secure syslog target, choose a Cisco ISE node with the Monitoring persona enabled on it as your log collector.

Step 1 Log in to the Cisco ISE administration 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 hostname or IP address of the Cisco ISE monitoring node in your deployment, in the **Host / IP Address** field.

Step 8 Enter *6514* as the port number in the **Port** field. The secure syslog receiver listens on TCP port 6514.

Step 9 Choose the syslog facility code from the **Facility Code** drop-down list. The default value is **LOCAL6**.

Step 10 Check the following check boxes to enable the corresponding configurations:

a) **Include Alarms For This Target**

b) **Comply to RFC 3164**

c) **Enable Server Identity Check**

Step 11 Check the **Buffer Messages When Server 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 the logs when the secure syslog receiver comes up.

a) Enter the buffer size in the **Buffer Size (MB)** field.

b) For Cisco ISE to periodically check the secure syslog receiver, enter the reconnect timeout value in the **Reconnect Time (Sec)** field. The timeout value is configured in seconds.

Step 12 Choose the CA certificate that Cisco ISE must present to the secure syslog server from the **Select CA Certificate** drop-down list.

Step 13 Ensure that the **Ignore Server Certificate validation** check box is not checked when configuring a Secure Syslog.

Step 14 Click **Submit**.

Remote Logging Target Settings

The following table describes the fields in the **Remote Logging Targets** window that you can use to create external locations (syslog servers) to store logging messages. The navigation path for this window is **Administration** > **System** > **Logging** > **Remote Logging Targets**. click **Add**.

Table 1: Remote Logging Target Settings

Field Name	Usage Guidelines
Name	Enter a name for the new syslog target.
Target Type	Select the target type from the drop-down list. The default value is **UDP Syslog**.
Description	Enter a brief description of the new target.
IP Address	Enter the IP address or hostname of the destination machine that will store the logs.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code that must be used for logging, from the drop-down list. Valid options are Local0 through Local7.
Maximum Length	Enter the maximum length of the remote log target messages. Valid values are from 200 through 1024 bytes.
Include Alarms For this Target	When you check this check box, alarm messages are sent to the remote server as well.
Comply to RFC 3164	When you check this check box, the delimiters (, ; { } \ \) in the syslog messages sent to the remote servers are not escaped even if a backslash (\) is used.
Buffer Message When Server Down	This check box is displayed when you choose **TCP Syslog** or **Secure Syslog** from the **Target Type** drop-down list. Check this check box to allow Cisco ISE to buffer the syslog messages when a TCP syslog target or secure syslog target is unavailable. Cisco ISE retries sending messages to the target when the connection to the target resumes. After the connection resumes, messages are sent sequentially, starting with the oldest, and proceeding to the newest. Buffered messages are always sent before new messages. If the buffer is full, old messages are discarded.
Buffer Size (MB)	Set the buffer size for each target. By default, it is set to 100 MB. Changing the buffer size clears the buffer, and all the existing buffered messages for the specific target are lost.
Reconnect Timeout (Sec)	Enter the time (in seconds) to configure how long the TCP and secure syslogs are stored for before being discarded when the server is down.
Select CA Certificate	This drop-down list is displayed when you choose **Secure Syslog** from the **Target Type** drop-down list. Choose a client certificate from the drop-down list.
Ignore Server Certificate Validation	This check box is displayed when you choose **Secure Syslog** from the **Target Type** drop-down list. Check this check box for Cisco ISE to ignore server certificate authentication and accept any syslog server. By default, this option is set to Off unless the system is in FIPS mode when this is disabled.

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

Enable logging categories for Cisco ISE to send auditable events to the secure syslog target.

Step 1 Choose **Administration** > **System** > **Logging** > **Logging Categories**.

Step 2 Click the radio button next to the **Administrative and Operational Audit** logging category, then click **Edit**.

Step 3 Choose **WARN** from the **Log Severity Level** drop-down list.

Step 4 In the **Targets** area, move the secure syslog remote logging target that you created earlier to the **Selected** area.

Step 5 Click **Save**.

Step 6 Repeat this task to enable the following logging categories. Both these logging categories have **INFO** as the default log severity level and you cannot edit it.

- **AAA Audit**.
- **Posture and Client Provisioning Audit**.

Configure Logging Categories

The following table describes the fields that you can use to configure a logging category. Set a log severity level and choose the logging targets for the logs of a logging category. The navigation path for this window is **Administration** > **System** > **Logging** > **Logging Categories**.

Click the radio button next to the logging category that you want to view, and click **Edit**. The following table describes the fields that are displayed in the edit window of the logging categories.

Table 2: Logging Category Settings

Field Name	Usage Guidelines
Name	Displays the name of the logging category.
Log Severity Level	For some logging categories, this value is set by default, and you cannot edit it. For some logging categories, you can choose one of the following severity levels from a drop-down list: • **FATAL**: Emergency level. This level means that you cannot use Cisco ISE and you must immediately take the necessary action. • **ERROR**: This level indicates a critical error condition. • **WARN**: This level indicates a normal but significant condition. This is the default level set for many logging categories. • **INFO**: This level indicates an informational message. • **DEBUG**: This level indicates a diagnostic bug message.
Local Logging	Check this check box to enable logging events for a category on the local node.

Field Name	Usage Guidelines
Targets	This area allows you to choose the targets for a logging category by transferring the targets between the **Available** and the **Selected** areas using the left and right arrow icons. The **Available** area contains the existing logging targets, both local (predefined) and external (user-defined). The **Selected** area, which is initially empty, then displays the targets that have been chosen for the category.

Disable TCP Syslog and UDP Syslog Collectors

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

Step 1 Choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 2 Click the radio button next to a TCP or UDP syslog collector.

Step 3 Click **Edit**.

Step 4 Choose **Disabled** from the **Status** drop-down list.

Step 5 Click **Save**.

Step 6 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** window (click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**). You cannot delete the default syslog collectors and cannot update the following fields for the default syslog collectors:

- **Name**
- **Target Type**
- **IP/Host address**
- **Port**

During a fresh Cisco ISE installation, a certificate that is named **Default Self-signed Server Certificate** is added to the Trusted Certificates store. This certificate is marked for **Trust for Client authentication and**

Syslog usage, 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 a Cisco ISE upgrade, if there are any existing secure syslog targets pointing to MnT nodes on port 6514, the names and configurations of the target are retained. After the upgrade, you cannot delete these syslog targets and you cannot edit the following fields:

- **Name**
- **Target Type**
- **IP/Host address**
- **Port**

If no such targets exist at the time of upgrade, default secure syslog targets are created similar to the fresh installation scenario, without any certificate mapping. You can assign the 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, Cisco ISE displays the following message:

```
Please configure the certificate for log_target_name
```

Note You cannot create a new logging target using the hostname or IP address and port of an already existing target. Each logging target must have a unique hostname or IP address and port.

Offline Maintenance

If the maintenance time period is less than an hour, take the Cisco ISE node offline and perform the maintenance task. When you bring the node back online, the PAN node 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, deregister the node at the time of maintenance and reregister 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.

Note

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

Changing the Host Name in Cisco ISE

In Cisco ISE, you can change the host name only through the CLI. For information on this, see the *Cisco Identity Services Engine CLI Reference Guide* for your version.

Considerations to keep in mind before changing the host name:

- All Cisco ISE services will undergo an automatic restart at the standalone node level if the host name is changed.
- If CA-signed certificates were used on this node, you must import them again with the correct host name.
- If this node will be joining a new Active Directory domain, you must leave your current Active Directory domain before changing the host name. If this node is already joined to an existing Active Directory domain, then it is strongly recommended that you rejoin all currently joined join-points to avoid possible mismatch between the current and previous host names and joined machine account name.
- If Internal-CA signed certificates are being used, you must regenerate the ISE root CA certificate.
- Changing the host name will cause any certificate using the old host name to become invalid. Therefore, a new self-signed certificate using the new host name will be generated now for use with HTTPs or EAP.

Note All the above considerations are applicable for any change in the domain name as well.