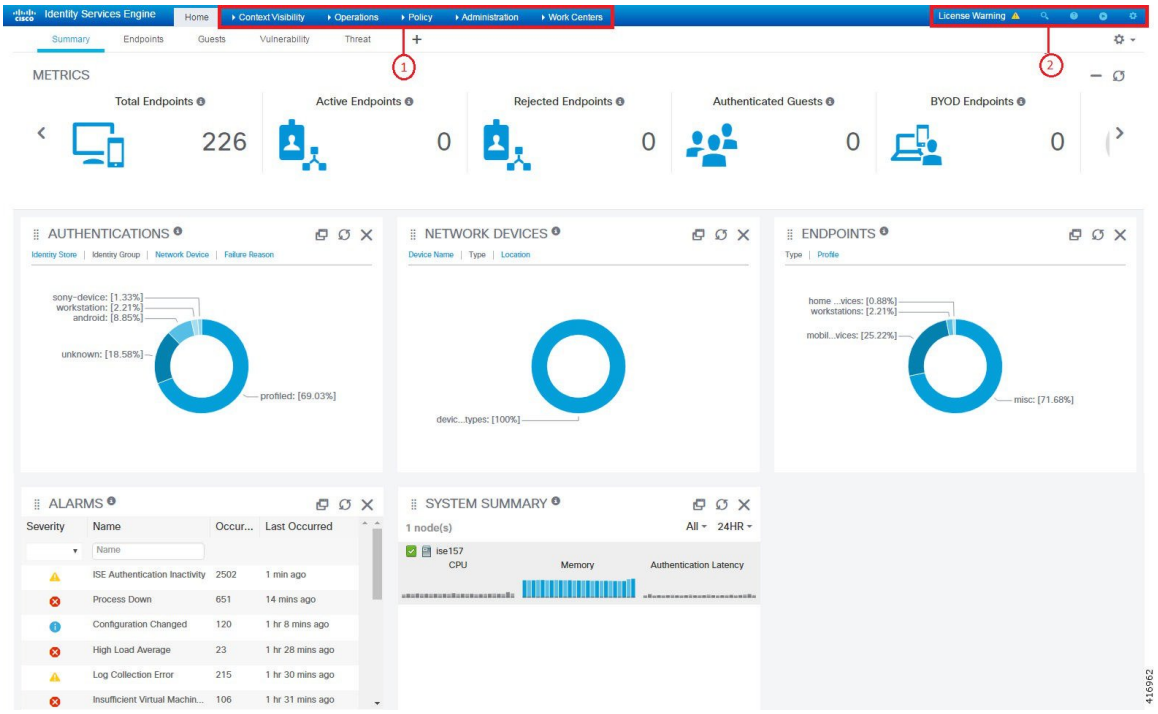
Cisco ISE 2.7 Admin Guide: Basic Setup

Basic Setup

Administrators Portal

The Admin portal provides access to ISE configuration and reporting. The following figure shows the main elements of the menu bar of portal.



1	Menu Drop-downs	• Context Visibility: These menus display information about endpoints, users, and NADs. The information can be segmented by features, applications, BYOD, and other categories, depending on your license. The Context menus use a central database, gathers information from database tables, caches, and buffers, which makes updates to context dashlets and list content very fast. The Context menus consist of dashlets at the top, and a list of information at the bottom. As you filter data by modifying the column attributes in the list, the dashlets are refreshed to show the changed content. • Policy: Access tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning. • Administration: Access tools for managing Cisco ISE nodes, licenses, certificates, network devices, users, endpoints, and guest services.

2	Top Right menu	

- 

  Search for endpoints and display their distribution by profiles, failures, identity stores, location, device type, and so on.

- 

  Access online help for the currently displayed page, plus links to the ISE Community, Portal Builder and more.

- 

  Access the following options:

  - PassiveID Setup—The **PassiveID Setup** option launches the **PassiveID Setup** wizard to set up passive identity using Active Directory. You can configure the server to gather user identities and IP addresses from external authentication servers and deliver the authenticated IP addresses to the corresponding subscriber.
  - Visibility Setup—The **Visibility Setup** option is a Proof of Value (PoV) service that collects endpoint data, such as applications, hardware inventory, USB status, firewall status, and the overall compliance state of Windows endpoints, and sends it to Cisco ISE. When you launch the **ISE Visibility Setup** Wizard, it allows you to specify an IP address range to run endpoint discovery for a preferred segment of the network or a group of endpoints.

    The PoV service uses the Cisco Stealth Temporal agent to collect endpoint posture data. Cisco ISE pushes the Cisco Stealth Temporal agent to computers running Windows with an Adminstrator account type, which automatically runs a temporary executable file to collect context and then the agent removes itself. To experience the optional debug capabilities of Cisco Stealth Temporal agent, check the **Endpoint Logging** check box (**Visibility Setup > Posture**) to save the debug logs in an endpoint or multiple endpoints. You can view the logs in either of the following locations:

    - C:\WINDOWS\syswow64\config\systemprofile\ (64-bit operating system)
    - C:\WINDOWS\system32\config\systemprofile\ (32-bit operating system)

  - Wireless Setup (BETA)— The **Wireless Setup (BETA)** option provides an easy way to set up wireless flows for 802.1x, guest, and Bring Your Own Device (BYOD). This option also provides workflows to configure and customize each portal for guest and BYOD.

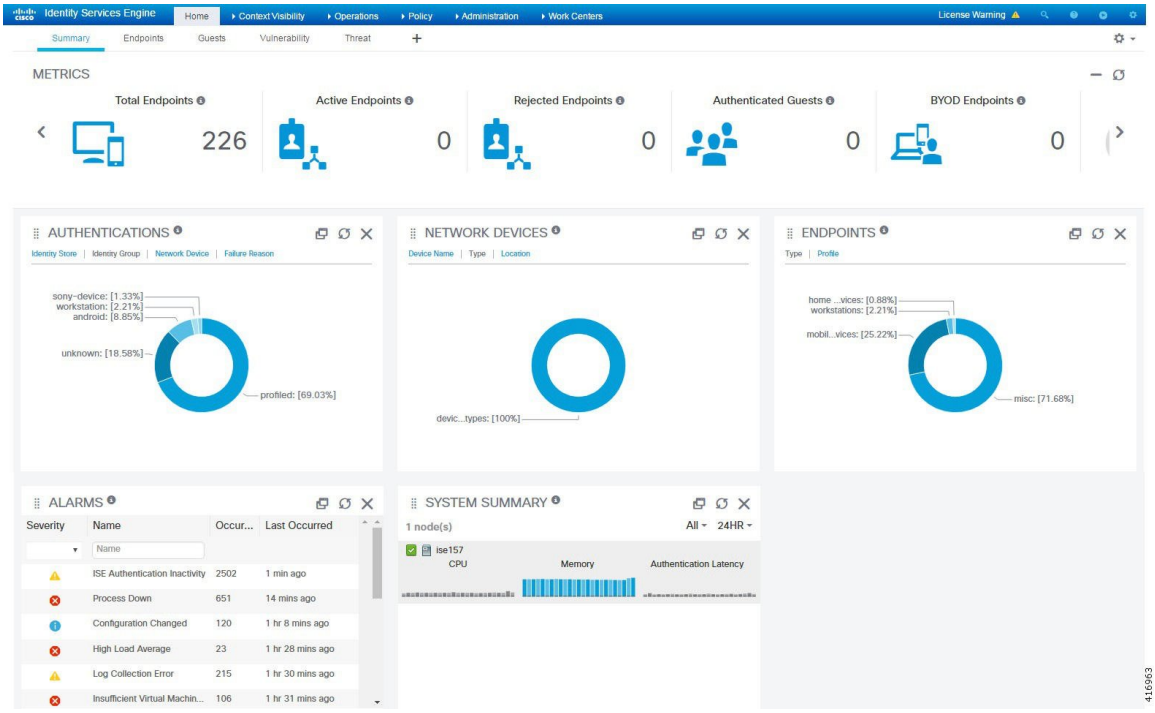
- 

  System activities, which includes bringing up the online help, and

		configuring account settings. Account Settings:

ISE Home Dashboards

The Cisco ISE Dashboard displays live consolidated and correlated statistical data that is is essential for effective monitoring and troubleshooting. Dashboard elements show activity over 24 hours, unless otherwise noted. The following figure shows some of the information available on the Cisco ISE Dashboard. You can view the Cisco ISE Dashboard data only in the Primary Administration Node (PAN).



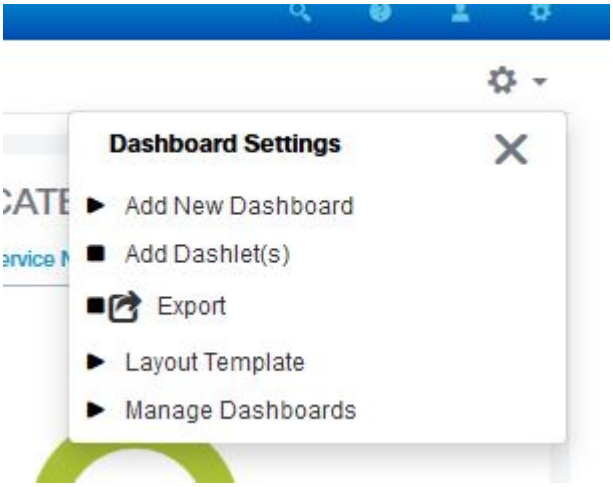
The Home page has five default dashboards that show a view of your ISE data:

- Summary—This view has a linear Metrics dashlet, pie chart dashlets, and list dashlets. The Metrics dashlet is not configurable.
- Endpoints—Status, Endpoints, Endpoint Categories, Network Devices.
- Guests—Guest user type, logon failures and location.
- Vulnerability—Information reported to ISE by vulnerability servers.
- Threat—Information reported to ISE by threat servers.

Each of these dashboards has several pre-defined dashlets. For example, the Summary dashboard has: Status, Endpoints, Endpoint Categories, and Network Devices.

Configuring Home Dashboards

You can customize a Home page dashboard by clicking the gear icon in the upper right-hand corner of the page:



- **Export** saves the currently selected home view to a PDF.
- **Layout Template** configures the number of columns displayed in this view.
- **Manage Dashboards** allows you to make the current dashboard the default (that opens when you select Home), or reset all dashboards (remove your configurations on all the Home dashboards).

Context Visibility Views

The structure of a Context Visibility page is similar to the Home page, except that Context Visibility pages:

- Retain your current context (browser window) when you filter the displayed data
- Are more customizable
- Focus on endpoint data

You can view the context visibility data only from the Primary Administration Node (PAN).

Dashlets on Context pages show information about endpoints, and endpoint connections to NADs. The information currently displayed is based on the content in the list of data below the dashlets on each page. Each page shows a view of endpoint data, based on the name of the tab. As you filter the data, both the list and dashlets update. You can filter the data by clicking on parts of one or more of the circular graphs, by filtering rows on the table, or any combination those actions. As you select filters, the effects are additive, also referred to as cascading filter, which allows you to drill down to find the particular data you are looking for. You can also click an endpoint in the list, and get a detailed view of that endpoint.

There are four main views under Context Visibility:

- Endpoints—You can select which endpoints to display based on types of devices, compliance status, authentication type, hardware inventory, and more. Refer to the The Hardware Dashboard, on page 10 section for additional information.

Note We recommend that you enable the accounting settings on the NADs to ensure that the accounting start and update information is sent to Cisco ISE.

Cisco ISE can collect accounting information, such as the latest IP address, status of the session (Connected, Disconnected, or Rejected), inactivity days of an endpoint, only if accounting is enabled. This information is displayed in the Live Logs/Live Sessions and the Context Visibility pages. When accounting is disabled on a NAD, there might be a missing, incorrect, or mismatch in the accounting information between the Live Sessions/ Live Logs and Context Visibility pages.

Note The Visibility Setup wizard allows you to add a list of IP address range for endpoints discovery. After this wizard is configured, Cisco ISE authenticates the endpoints, but the endpoints that are not included in the configured IP address range are not displayed in the Context Visibility > Endpoints tab and the Endpoints listing page (under Work Centers > Network Access > Identities > Endpoints).

- User-Based—Displays user information from user identity sources.

  Note the following points while using this view:

  1. If there is any change in the username or password attribute, it will be reflected immediately on this page when there is a change in the authentication status.
  2. If any other attribute other than the username is changed in the Active Directory, the updated attributes are displayed only after 24 hours upon re-authentication.
  3. If the username and other attributes are changed in the Active Directory, the updated changes will be displayed immediately after re-authentication.

- Network Devices—List of NADs that have endpoints connected to them. You can click the Number of Endpoints on a NAD (right-most column) to get a Context Visibility screen listing all those devices filtered by that NAD.

  Note If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report that is provided by the Monitoring service (Operations > Reports > Catalog > Network Device > Session Status Summary). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.

- Application—The Application view is used to identify the number of endpoints that have a specified application installed. The results are displayed in graphical and table formats. The graphical representation helps you make a comparative analysis. For example, you can find out the number of endpoints with the Google Chrome software along with their Version, Vendor, and Category (Anti-phishing, Browser, and so on) in a table as well as a bar chart. For more information, see The Application Dashboard section.

You can create a new view under Context Visibility to create a custom list, for additional filtering. Dashlets are not supported in custom views for this release.

Clicking a section of a circular graph in a dashlet opens a new page with filtered data from that dashlet in Context Visibility mode. From that new page, you can continue to filter the displayed data, as described in Filtering Displayed Data in a View, on page 13.

For more information about using Context Visibility to find endpoint data, see the following Cisco YouTube video, which uses ISE 2.1 https://www.youtube.com/watch?v=HvonGhrydfg.

Related Topics

The Hardware Dashboard, on page 10

Attributes in Context Visibility

The systems and services that provide attributes for Context Visibility sometimes have different values for the same attribute name. A few examples are shown below:

For Operating System

- *OperatingSystem*—Posture operating system
- *operating-system*—NMAP operating system
- *operating-system-result*—Profiler consolidated operating system

Note There might be some discrepancies in the endpoint operating system data displayed in the Context Visibility page when multiple probes are enabled for the endpoint in Cisco ISE.

For Portal Name

- *Portal.Name*—Guest portal name when device registration is turned on
- *PortalName*—Guest portal name when device registration is not turned on

Portal User

- *User-Name*—User name from RADIUS authentication
- *GuestUserName*—Guest user
- *PortalUser*—Portal user

The Application Dashboard

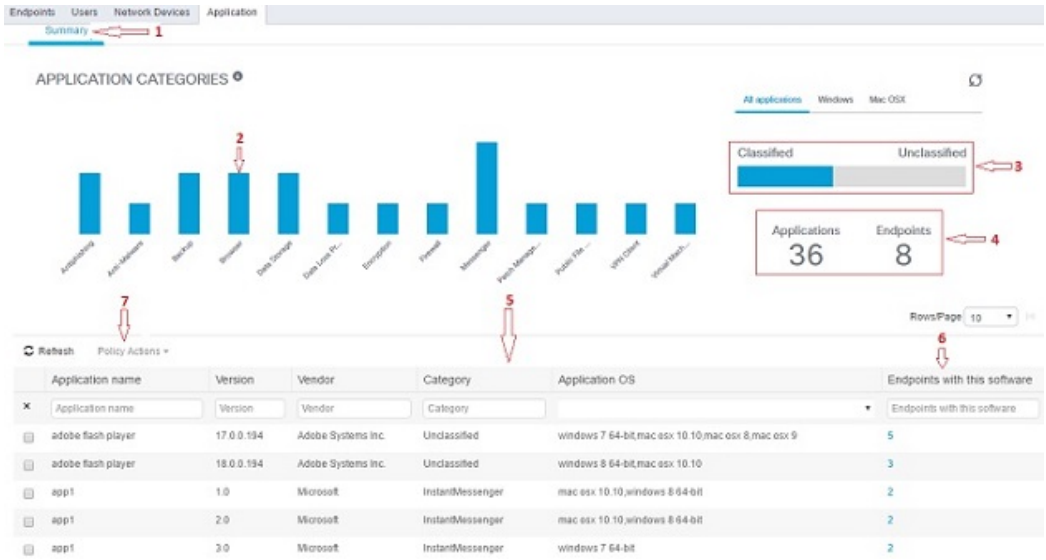
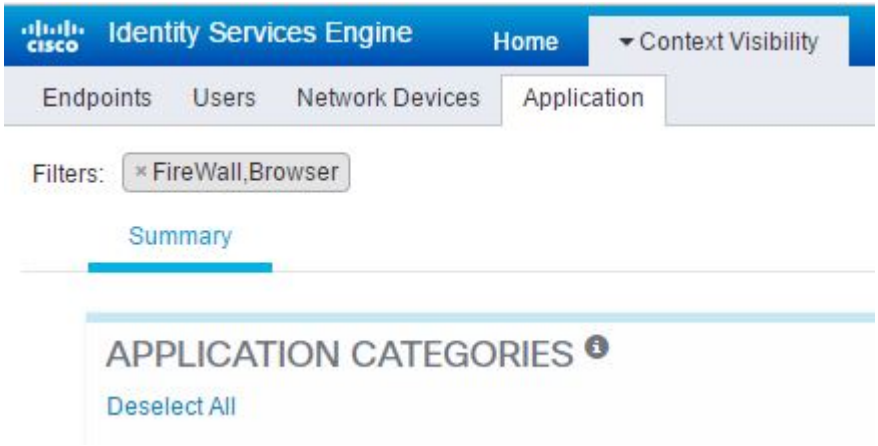


Table 1: Description of the Application Dashboard

Label	Description
1	The **Summary** tab is selected by default. It displays the **Application Categories** dashlet, which contains a bar chart. Applications are classified into 13 categories. Applications that do not fall into any of these categories are termed Unclassified. The available categories are Anti-Malware, Antiphishing, Backup, Browser, Data Loss Prevention, Data Storage, Encryption, Firewall, Messenger, Patch Management, Public File Sharing, Virtual Machine, and VPN Client.
2	Each bar corresponds to a classified category. You can hover over each bar to view the total number of applications and endpoints that correspond to the selected application category.
3	The applications and endpoints that fall under the Classified category are displayed in Blue. Unclassified applications and endpoints are displayed in Gray. You can hover over the classified or unclassified category bar to view the total number of applications and endpoints that belong to that category. You can click **Classified** and view the results in the bar chart and table (5). When you click **Unclassified**, the bar chart is disabled (grayed out) and the results are displayed in the table (5).

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>4</td><td>The applications and endpoints are displayed based on the selected filter. You can view the breadcrumb trail as you click different filters. You can click Deselect All to remove all filters.
 
</td></tr>
<tr><td>5</td><td>When you click multiple bars, the corresponding classified applications and endpoints are displayed in the table. For example, if you select the Antimalware and Patch Management categories, the following results are displayed.
<table>
<tr><th>Application Name</th><th>Version</th><th>Vendor</th><th>Category</th><th>Application OS</th><th>Endpoints With This Software</th></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>Antimalware</td><td>windows 7 64-bit,mac osx 10.10,mac osx 8,mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>Antimalware</td><td>windows 8 64-bit,mac osx 10.10</td><td>3</td></tr>
<tr><td>Software Update</td><td>2.3</td><td>Apple Inc.</td><td>Patch Management</td><td>windows 7 64-bit,mac osx 10.10,mac osx 8,mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>Click an endpoint in the Endpoints With This Software column in the table to view the endpoint details, such as Mac address, NAD IP address, NAD port ID/SSID, IPv4 address, and so on.</td></tr>
<tr><td>7</td><td>You can select an application name and choose the Create App Compliance option from the Policy Actions drop-down list to create application compliance condition and remediation.</td></tr>
</table>

The Hardware Dashboard

The endpoint hardware tab under context visibility helps you collect, analyze, and report endpoint hardware inventory information within a short time. You can gather information, such as finding endpoints with low memory capacity or finding the BIOS model/version in an endpoint. You can increase the memory capacity or upgrade the BIOS version based on these findings. You can assess the requirements before you plan the

purchase of an asset. You can ensure timely replacement of resources. You can collect this information without installing any modules or interacting with the endpoint. In summary, you can effectively manage the asset lifecycle.

The **Context Visibility** > **Endpoints** > **Hardware** page displays the **Manufacturers** and **Endpoint Utilizations** dashlets. These dashlets reflect the changes based on the selected filter. The **Manufacturers** dashlet displays hardware inventory details for endpoints with Windows and Mac OS. The **Endpoint Utilizations** dashlet displays the CPU, Memory, and Disk utilization for endpoints. You can select any of the three options to view the utilization in percentage.

- Devices With Over n% CPU Usage.
- Devices With Over n% Memory Usage.
- Devices With Over n% Disk Usage.

Note The hardware inventory data takes 120 seconds to be displayed in the ISE GUI. The hardware inventory data is collected for posture compliant and non-compliant states.

Note

- The Quick Filters in the Hardware Visibility Page need at least 3 characters to take effect. Another way to make the Quick Filter work efficiently is to click on the filters of other column attributes after entering the characters.
- Some of the column attributes are greyed out as this table is only used to filter based on attributes related to hardware.
- The Operating System filter applies only to the **Manufacturers** Chart. It is not relevant to the table below it.

The hardware attributes of an endpoint and their connected external devices are displayed in a table format. The following hardware attributes are displayed:

- MAC Address
- BIOS Manufacturer
- BIOS Serial Number
- BIOS Model
- Attached Devices
- CPU Name
- CPU Speed (GHz)
- CPU Usage (%)
- Number of Cores
- Number of Processors
- Memory Size (GB)

- Memory Usage (%)
- Total Internal Disk(s) Size (GB)
- Total Internal Disk(s) Free Size (GB)
- Total Internal Disk(s) Usage (%)
- Number of Internal Disks
- NAD Port ID
- Status
- Network Device Name
- Location
- UDID
- IPv4 Address
- Username
- Hostname
- OS Types
- Anomalous Behavior
- Endpoint Profile
- Description
- Endpoint Type
- Identity Group
- Registration Date
- Identity Store
- Authorization Profile

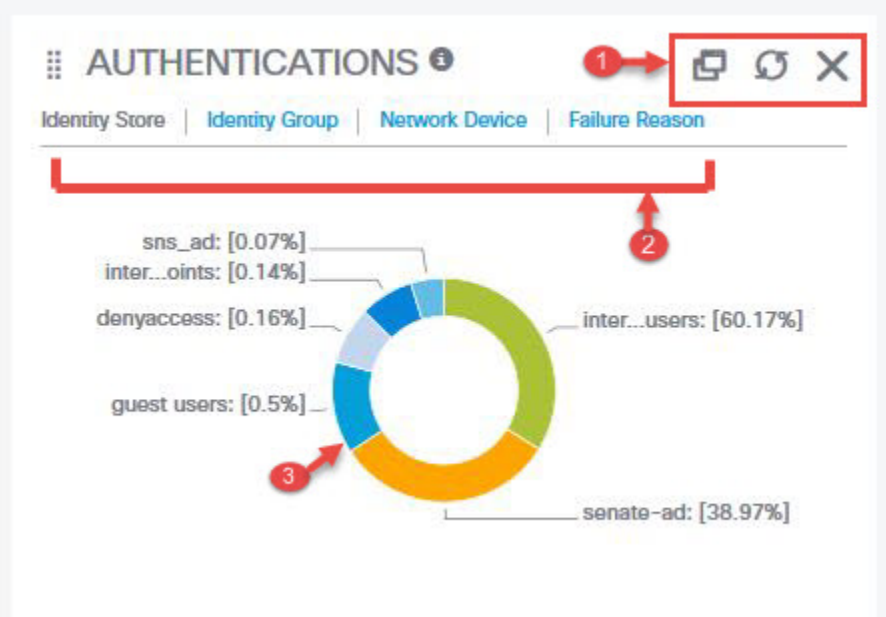
You can click the number in the **Attached Devices** column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint.

Note Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. These hardware attributes may not appear in the Hardware Context Visibility page.

The hardware inventory data collection interval can be controlled in the **Administration** > **System** > **Settings** > **Posture** > **General Settings** page. The default interval is 5 minutes.

Dashlets

The following picture shows an example dashlet:



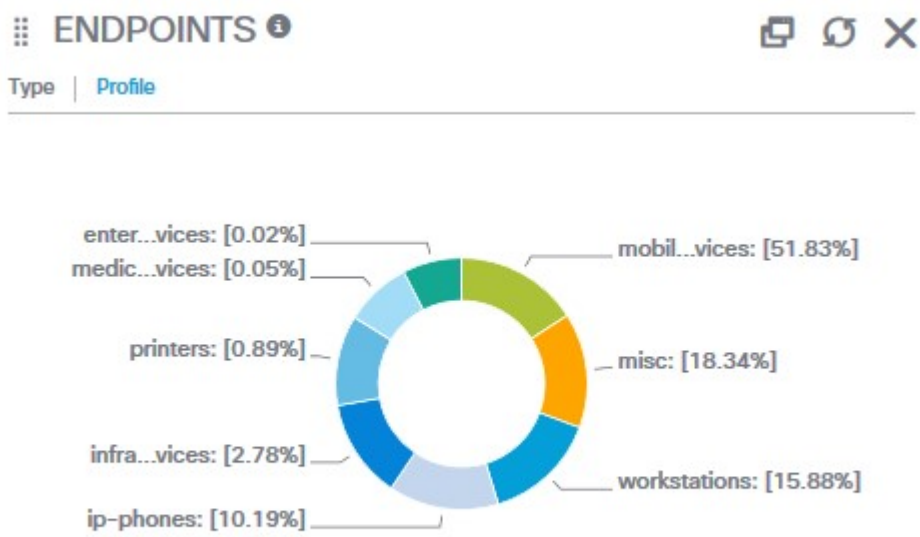
1. The stacked window symbol “detaches”, opens this dashlet in a new browser window. The circle refreshes. The X deletes this dashlet, but is only available on the Home page. You delete dashlets in Context Visibility using the gear symbol in the top-right corner of the screen.
2. Some dashlets have different categories of data. Click the link to see a pie chart with that set of data.
3. The Pie chart shows the data that you have selected. Clicking one of the pie segments opens a new tab in Context Visibility with the filtered data, based on that pie segment.

Clicking a section of the pie chart in a Home dashboard opens in new browser window that displays data filtered by the section of the pie chart that you clicked on.

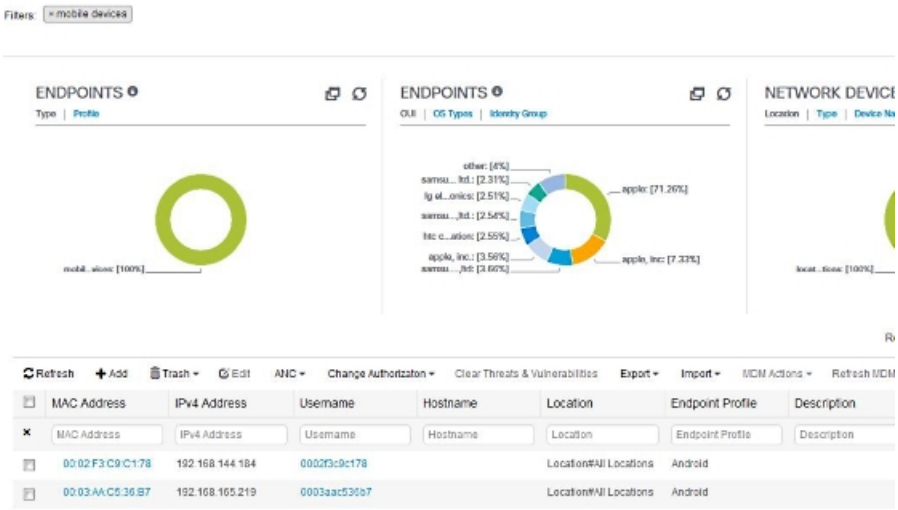
Clicking a section of the pie chart in a Context view filters the displayed data, but does not change the context; the filtered data displays in the same browser window.

Filtering Displayed Data in a View

Clicking any of the dashlets on a Context Visibility page filters the data that is displayed by the item you clicked, for example, a section of a pie chart.

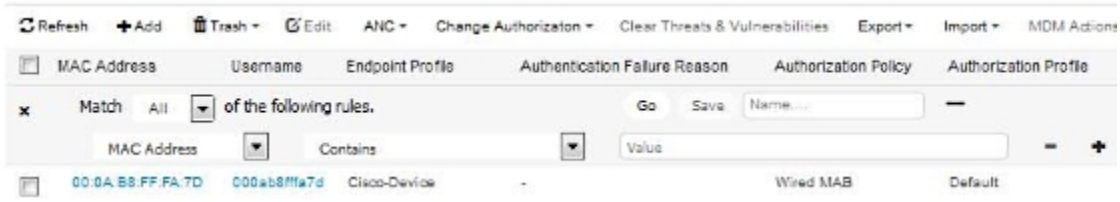


If you click **mobil…vices** in the Endpoints dashlet, the page redisplays with two Endpoints dashlets, a Network Devices dashlet, and a list of data. The dashlets and list show data for mobile devices, as shown in the following example:



You can continue to filter data by clicking more sections of the pie charts, or by using the controls on the list of data.

1. The gear icon filters the displayed columns. The drop-down lets you chose which columns to display in this dashboard's list.
2. The Quick filter is displayed by default. Entering characters into the box (label number 3) filters the list based on the result. The Custom Filter provides a more granular filter, as shown below.



You can save your custom filters.

Create Custom Filters

You can create and save custom filters and modify the filter criteria in preset filters. Custom filters are not saved in the Cisco ISE database. You can only access them using the same computer and browser used to create them.

Procedure

Step 1 Click the **Show** drop-down list and choose **Advanced Filter**.

Step 2 Specify the search attributes, such as fields, operators, and values from the Filter menus.

Step 3 Click + to add additional conditions.

Step 4 Click **Go** to display the entries that match the specified attributes.

Step 5 Click the **Save** icon to save the filter.

Step 6 Enter a name and click **Save**. The filter now appears in the Show drop-down list.

Filter Data by Conditions Using the Advanced Filter

The Advanced Filter allows you to filter information based on specified conditions, such as, First Name = Mike and User Group = Employee. You can specify more than one condition.

Procedure

Step 1 Click the **Show** drop-down list and choose **Advanced Filter**.

Step 2 Specify search the search attributes, such as fields, operators, and values from the Filter menus.

Step 3 Click **+** to add additional conditions.

Step 4 Click **Go** to display the entries that match the specified attributes.

Filter Data by Field Attributes Using the Quick Filter

The Quick Filter allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

Procedure

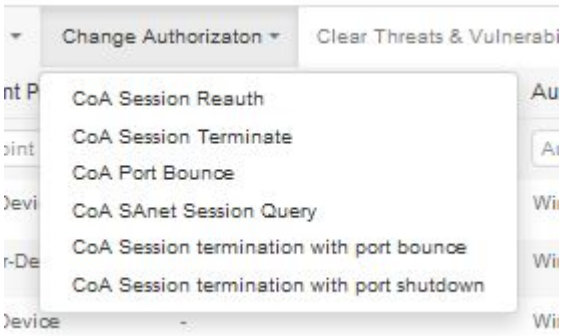
Step 1 Click the **Show** drop-down list and choose **Quick Filter**.

Step 2 Enter search criteria in one or more of the attribute fields, and the entries that match the specified attributes display automatically.

Endpoint Actions in a View's List

The toolbar at the top of the list allows you to take actions on endpoints in the list that you selected. Not all actions are enabled for every list, some actions depend on a feature being enabled for use. The following list shows two endoint actions that must be enabled in ISE before you can use them.

- If Adaptive Network Control (ANC) is enabled, you can select endpoints in the list, and assign or revoke network access. You can also issue a change of authorization (CoA):



ANC (Endpoint Protection Services) is enabled in ISE under Administration > System > Settings > Endpoint Protection Service > Adaptive Network Control. For more information, see the Enable Adaptive Network Control in Cisco ISE section in *Cisco ISE Admin Guide: Maintain and Monitor* .

- If MDM is installed, you can perform MDM actions on selected endpoints.

Cisco ISE Dashboard

The Cisco ISE dashboard or home page (**Home** > **Summary**) is the landing page that appears after you log in to the Cisco ISE administration console. The dashboard is a centralized management console consisting of metric meters along the top of the window, with dashlets below. The default dashboards are **Summary**, **Endpoints**, **Guests**, **Vulnerability**, and **Threat**. See the ISE Home Dashboards, on page 5 section for additional information.

Note You should view the dashboard data only in the Primary PAN.

The dashboard's real-time data provides an at-a-glance status of the devices and users accessing your network as well as an overview of the system's health.

Click the gear icon in the second level menu bar for a drop-down list of dashboard settings. The following table displays information about the options that are available under **Dashboard Settings**:

Option	Description
Add New Dashboard	You can have a maximum of 20 dashboards, including the five default dashboards.
Rename Dashboard	To rename a dashboard (available only for custom dashboards): **1.** Click **Rename Dashboard**. **2.** Specify a new name. **3.** Click **Apply**.
Add Dashlet	To add a dashlet to the home page dashboard: **1.** Click **Add Dashlet(s)**. **2.** In the **Add Dashlets** window, click **Add** adjacent to the dashlets that you want to add. **3.** Click **Save**. **Note** You can add a maximum of nine dashlets per dashboard.

Option	Description
Export	You can export the dashlet data as a PDF or a CSV file. To do this: 1. Select the corresponding dashboard, for example, Summary, from the Cisco ISE home page. 2. Choose **Dashboard Settings** > **Export**. 3. In the **Export** dialog box, select one of the following file formats: • The PDF format to view a snapshot of the selected dashlets. • The CSV format to download the selected dashboard data as a ZIP file. 4. In the **Dashlets** section, select the required dashlets. 5. Click **Export**. The ZIP file contains individual dashlet CSV files for the selected dashboard. Data related to each tab in a dashlet appear as separate sections in the corresponding dashlet CSV file. When you export a custom dashboard, the ZIP file is exported with the same name. For example, if you export a custom dashboard named MyDashboard, then the exported file name is MyDashboard.zip.
Layout Template	You can change the layout of the template in which the dashlets are displayed. To change the layout: 1. Choose **Dashboard Settings** > **Layout Template**. 2. Select the required layout from the options available.
Manage Dashboards	The following options are available under **Manage Dashboards**: • Mark as Default Dashboard: Use this option to set a dashboard as your default dashboard (home page). • Reset all Dashboards: Use this option to reset all the dashboards to their original settings.

You can delete a dashboard that you have created by clicking the close (**x**) icon adjacent to the corresponding custom dashboard.

Note You cannot rename or delete a default dashboard.

All the dashlets have a toolbar at the top-right corner, with the following options:

- Detach: To view a dashlet in a separate window.
- Refresh: To refresh a dashlet.
- Remove: To remove a dashlet from the dashboard.

You can drag and drop the dashlet using the gripper icon that is present at the top-left corner of the dashlet.

Quick Filter in Alarms Dashlet: You can filter alarms based on their severity, such as Critical, Warning, and Info. The Alarms dashlet is found on the home page, and contains the Filter drop-down list with the Quick Filter option.

Cisco ISE Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text. For Windows, MAC OSX, and Android devices, the native supplicant provisioning wizard can be used in any of the following supported languages.

In Cisco ISE, internalization and localization support focuses on support for non-English text in UTF-8 encoding to the end-user facing portals and on selective fields in the Admin portal.

Supported Languages

Cisco ISE, provides localization and internalization support for the following languages and browser locales:

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
Czech	cs-cz
Dutch	nl-nl
English	en
French	fr-fr
German	de-de
Hungarian	hu-hu
Italian	it-it
Japanese	ja-jp

Language	Browser Locale
Korean	ko-kr
Polish	pl-pl
Portuguese (Brazil)	pt-br
Russian	ru-ru
Spanish	es-es

End-User Web Portal Localization

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. If the client browser requests a locale that is not mapped to a template in Cisco ISE, the portals display content using the English template.

Using the Admin portal, you can modify the fields used for the Guest, Sponsor, and My Devices portals for each language individually, and you can add additional languages. Currently, you cannot customize these fields for the Client Provisioning portal.

You can further customize the Guest portal by uploading HTML pages to Cisco ISE. When you upload customized pages, you are responsible for the appropriate localization support for your deployment. Cisco ISE provides a localization support example with sample HTML pages, which you can use as a guide. Cisco ISE provides the ability to upload, store, and render custom internationalized HTML pages.

Note NAC and MAC agent installers and WebAgent pages are not localized.

Support for UTF-8 Character Data Entry

Cisco ISE fields that are exposed to the end user (through the Cisco client agent, or supplicants, or through the Sponsor, Guest, My Devices, and Client Provisioning portals) support UTF-8 character sets for all languages. UTF-8 is a multibyte-character encoding for the unicode character set, which includes many different language character sets, such as Hebrew, Sanskrit, and Arabic.

Character values are stored in UTF-8 in the administration configuration database, and the UTF-8 characters display correctly in reports and user interface components.

UTF-8 Credential Authentication

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, EAP, RADIUS proxy, RADIUS token, and web authentication from the Guest and Administrative portal login authentications. UTF-8 support for user name and password applies to authentication against the local identity store as well as external identity stores.

UTF-8 authentication depends on the client supplicant that is used for network login. Some Windows native supplicants do not support UTF-8 credentials.

Note RSA does not support UTF-8 users, hence UTF-8 authentication with RSA is not supported. Likewise, RSA servers, which are compatible with Cisco ISE, do not support UTF-8.

UTF-8 Policies and Posture Assessment

Policy rules in Cisco ISE that are conditioned on attribute values may include UTF-8 text. Rule evaluation supports UTF-8 attribute values. In addition, you can configure conditions with UTF-8 values through the Administrative portal.

Posture requirements can be modified as File, Application, and Service conditions based on a UTF-8 character set.

UTF-8 Support for Messages Sent to Supplicant

RSA prompts and messages are forwarded to the supplicant using a RADIUS attribute REPLY-MESSAGE, or within EAP data. If the text contains UTF-8 data, it is displayed by the supplicant, based on the client's local operating system language support. Some Windows-native supplicants do not support UTF-8 credentials.

Cisco ISE prompts and messages may not be in sync with the locale of the client operating system on which the supplicant is running. You must align the end-user supplicant locale with the languages that are supported by Cisco ISE.

Reports and Alerts UTF-8 Support

Monitoring and troubleshooting reports and alerts support UTF-8 values for relevant attributes, for Cisco ISE supported languages, in the following ways:

- Viewing live authentications
- Viewing detailed pages of report records
- Exporting and saving reports
- Viewing the Cisco ISE dashboard
- Viewing alert information
- Viewing tcpdump data

UTF-8 Character Support in the Portals

Many more character sets are supported in Cisco ISE fields (UTF-8) than are currently supported for localizations in portals and end-user messages. For example, Cisco ISE does not support right-to-left languages, such as Hebrew or Arabic, even though the character sets themselves are supported.

The following table lists the fields in the Admin and end-user portals that support UTF-8 characters for data entry and viewing, with the following limitations:

- Cisco ISE does not support guest usernames and passwords with UTF-8 characters.
- Cisco ISE does not support UTF-8 characters in certificates.

Table 2: Admin Portal UTF-8 Character Fields

Admin Portal Element	UTF-8 Fields
Network access user configuration	• User name The usernames can be composed of any combination of upper and lower case letters, numbers, space, and special characters (except `, %, ^, ;, :, [, {, |, },], \, ‘, “, =, <, >, ?, ! and control characters). Usernames with only spaces is also not allowed. • First name • Last name • e-mail
User list	• All filter fields • Values shown on the User List page • Values shown on the left navigation quick view
User password policy	The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. Password field accepts any characters including UTF-8 characters, but it doesn't accept control characters. Some languages do not have uppercase or lower case alphabets. If your user password policy requires the user to enter a password with uppercase or lowercase characters, and if the user’s language does not support these characters, the user cannot set a password. For the user password field to support UTF-8 characters, in the user password policy page (**Administration** > **Identity Management** > **Settings** > **User Password Policy**), you must uncheck the following options: • Lowercase alphabetic characters • Uppercase alphabetic characters
Administrator list	• All filter fields • Values shown on the Administrator List page • Values shown on the left navigation quick view
Admin login page	• User name

Admin Portal Element	UTF-8 Fields
RSA	• Messages • Prompts
RADIUS token	• Authentication tab > Prompt
Posture Requirement	• Name • Remediation action > Message shown to Agent User • Requirement list display
Posture conditions	• File condition > File path • Application condition > Process name • Service condition > Service name • Conditions list display
Guest and My Devices settings	• Sponsor > Language Template: all supported languages, all fields • Guest > Language Template: all supported languages, all fields • My Devices >Language Template: all supported languages, all fields
System settings	• SMTP Server > Default e-mail address
Operations > Alarms > Rule	• Criteria > User • Notification > e-mail Notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the av expression within policy conditions • Authorization / posture / client provisioning > other conditions > value for the av expression within policy conditions

Admin Portal Element	UTF-8 Fields
Attribute value in policy library conditions	• Authentication > simple condition / compound condition > value for the av expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition / compound condition > value for the av expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition / Dictionary compound condition > value for the av expression • Guest > simple condition / compound condition > value for the av expression

UTF-8 Support Outside the User Interface

This section contains the areas outside the Cisco ISE user interface that provide UTF-8 support.

Debug Log and CLI-Related UTF-8 Support

Attribute values and posture condition details appear in some debug logs; therefore, all debug logs accept UTF-8 values. You can download debug logs containing raw UTF-8 data that can be viewed with a UTF-8 supported viewer.

ACS Migration UTF-8 Support

Cisco ISE, allows for the migration of ACS UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by Cisco ISE UTF-8 languages, which might render some of the UTF-8 data that is provided during migration as unreadable using Administrative portal or report methods. You must convert unreadable UTF-8 values (that are migrated from ACS) into ASCII text. For more information about migrating from ACS to ISE, see the Cisco Secure ACS to Cisco ISE Migration Tool for your version of ISE.

Support for Importing and Exporting UTF-8 Values

The Admin and Sponsor portals support plain text and .csv files with UTF-8 values to be used when importing user account details. Exported files are provided as csv files.

UTF-8 Support on REST

UTF-8 values are supported on external REST communication. This applies to configurable items that have UTF-8 support in the Cisco ISE user interface, with the exception of admin authentication. Admin authentication on REST requires ASCII text credentials for login.

UTF-8 Support for Identity Stores Authorization Data

Cisco ISE allows Active Directory and LDAP to use UTF- 8 data in authorization policies for policy processing.

MAC Address Normalization

ISE supports normalization of MAC address entered by you in any of the following formats:

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

For the following ISE windows, you can provide full or partial MAC address:

- Policy > Policy Sets
- Policy > Policy Elements > Conditions > Authorization
- Authentications > Filters (Endpoint and Identity columns)
- Global Search
- Operations > Reports > Reports Filters
- Operations > Diagnostic Tools > General Tools > Endpoint Debug

For the following ISE windows, you should provide full MAC address (six octets separated by ':' or '-' or '.'):

- Operations > Endpoint Protection Services Adaptive Network Control
- Operations > Troubleshooting > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting
- Operations > Troubleshooting > Diagnostic Tools > General Tools > Posture Troubleshooting
- Administration > Identities > Endpoints
- Administration > System > Deployment
- Administration > Logging > Collection Filter

REST APIs also support normalization of full MAC address.

Valid octet can contain only 0-9, a-f or A-F.

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.

Administrator Access Console

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

Procedure

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

Step 2 Enter the username and 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.

Administrator Login Browser Support

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

- Mozilla Firefox 72 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 80 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
- SMS Message Transmission
- Social Login

The Cisco ISE proxy configuration supports basic authentication for proxy servers. NT LAN Manager (NTLM) authentication is not supported.

Procedure

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. In Cisco ISE 2.6 and later, ERS users can be either internal users or belong to an external AD. The AD group to which the external users belong must be mapped to either ERS Admin or ERS Operator groups:

- 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.

Procedure

Step 1 Choose **Administration** > **System** > **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 **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 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 30

Enable External AD Access for ERS APIs

The following steps will allow you to enable External AD access for ERS APIs:

Procedure

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

Step 2 Add the AD groups that the external user belongs to as an external identity source.

See the section "Active Directory as an External Identity Source" in Chapter "Asset Visibility" in *Cisco ISE Administrator Guide*.

Step 3 Add user groups from the ADs.

See the section "Add Users" in Chapter "Asset Visibility" in *Cisco ISE Administrator Guide*.

Step 4 Choose **Administration** > **Admin Access** > **Authentication** > **Authentication Method**.

Step 5 Choose **AD: <Join Point Name>** from the **Identity Source** drop-down.

Step 6 Choose either **Password Based** or **Client Certificate Based** authentication.

Step 7 Choose**Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**.

Step 8 Add external group(s) to ERS Admin group or ERS Operator group as a member user. Go to **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups** > **ERS AdminERS Operators**.

Step 9 Click **Add**.

Step 10 Select the user.

Step 11 Click **Save**.

The ISE administrator must assign special privileges to a user to perform operations using the External RESTful Services APIs. In Cisco ISE 2.6 and later, ERS users can be either internal users or belong to an external AD. The AD group to which the external users belong must be mapped to either ERS Admin or ERS Operator groups:

- 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.

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 timezones. 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.

Procedure

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**. Choose the **HMAC** from the 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) 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

To update the SMTP server details, go to **Administration > System > Settings > Proxy > SMTP server**.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.

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>.

The following table 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

The following fields configure the SMTP server.

- **SMTP Server Settings**
  - **SMTP Server**: Enter the hostname of the outbound SMTP server.
  - **SMTP Port**: Enter the SMTP port number. This port must be open to connect to the SMTP server.
  - **Connection Timeout**: Enter the maximum time Cisco ISE waits for a connection to the SMTP server before starting a new connection.
- **Encryption Settings**: Check Use TLS/SSL encryption to communicate with a secure SMTP server. If you use SSL, add the root certificate of the SMTP server to Cisco ISE Trusted Certificates.
- **Authentication Settings**: Authorization can either be username and password or SSL. SSL is the default. Check Use Password Authentication to use username and password instead.

Interactive Help

The Interactive Help enables users to work effectively with Cisco ISE by providing tips and step-by-step guidance to complete tasks with ease.

This feature is enabled by default. To enable or disable this feature, choose **Administration** > **System** > **Settings** > **Interactive Help**, and check or uncheck the **Enable Interactive Help** check box.

Enable Secure Unlock Client mechanism

Secure Unlock Client mechanism provides root shell access on Cisco ISE Command Line Interface (CLI) for a certain period of time. As soon as the session is closed or exited, the root access is also revoked.

The Secure Unlock Client feature has been implemented using the Consent Token tool. Consent Token is a uniform multi factor authentication scheme to securely grant privileged access for Cisco products in a trusted manner, and only after mutual consent from both customer and Cisco.

To enable root shell on Cisco ISE CLI, perform the following steps:

Procedure

Step 1 In the Cisco ISE CLI, enter **permit rootaccess**:

```
ise/admin# permit rootaccess
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
```

Step 2 Generate the Consent Token Challenge by choosing option **1**:

```
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
********************************************************************************
[redacted]
********************************************************************************
Starting background timer of 15mins
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
```

Step 3 Send the Consent Token Challenge to the Cisco Technical Assistance Center (TAC):

Cisco TAC will generates Consent Token Response using the Consent Token Challenge you provided.

Step 4 Choose option **2** and then enter the Consent Token Response provided by the Cisco TAC:

```
Enter CLI Option:
2
Please input the response when you are ready .........................
[redacted]
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
```

> **Note** The privileged access is enabled if response signature verification is successful.

What to do next

To exit from the shell mode, run the **exit** command:

```
sh-4.2# exit
exit
Root shell exited
```

You can view the history of root access sessions by choosing option **3**:

```
1.  Generate Challenge Token Request
2.  Enter Challenge Response for Root Access
3.  Show History
4.  Exit
Enter CLI Option:
3
************************************
                SN No : 1
************************************
Challenge
3/WcyAAAAQEBAQAAAABAgAEAAAAAAAMACMt89hCTWWBAQwo9lyianfhO4C5u1+v8OAQUABAAADhAGAANU0UHAAZJU0VfQ1QTAANU0UUACgJIDU2NGQ5NjgwLTEyZmEtOWI0ZS0wZjY1LTdlZDllMGQ1M2UzNQo=
  generated at 2019-06-12 15:40:01.000
************************************
                SN No : 2
************************************
```

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 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:

- 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.

When you enable the FIPS mode:

- All non-FIPS compliant cipher suites are disabled for EAP-TLS, PEAP, and EAP-FAST

- All non-FIPS compliant cipher suites are disabled in SSH
- Certificates and private keys must use only FIPS compliant hash and encryption algorithms
- RSA private keys must be of 2048 bits or greater
- ECDSA private keys must be of 224 bits or greater
- ECDSA server certificate will work with only TLS 1.2
- DHE ciphers work with DH parameters of 2048 bits or greater for all ISE TLS clients
- 3DES ciphers are not allowed for ISE as a server
- SHA1 is not allowed for generating certificates
- SHA1 is not allowed in client certificates
- The anonymous PAC provisioning option in EAP-FAST is disabled
- Local SSH server will operate in FIPS mode
- The following protocols are not supported for RADIUS:
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

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:

Procedure

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, on page 56
- Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 75
- See the Network Device Definition Settings section in *Cisco ISE Admin Guide: Secure Wired Access*

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:

- 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
- 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.

Procedure

Step 1 Configure an Active Directory identity source in Cisco ISE and join all Cisco ISE nodes to Active Directory.

Step 2 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 3 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 4 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 5 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 6 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 7 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 8 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.

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.

- Ensure that the default network access authentication policy does not allow any version of the SSL protocol.
- 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).

Procedure

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.

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.

Procedure

Step 1 Log in to 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**.

Remote Logging Target Settings

The following table describes the fields on the Remote Logging Targets page, which you can use to create external locations (syslog servers) to store logging messages. The navigation path for this page is: **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Table 3: Remote Logging Target Settings

Fields	Usage Guidelines
Name	Enter the name of the new target.
Target Type	Select the target type. By default it is set to UDP Syslog.
Description	Enter a brief description of the new target.
IP Address	Enter the IP address or hostname of the destination machine where you want to store the logs. ISE supports IPv4 and IPv6 formats for logging.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.
Maximum Length	Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 bytes.
Buffer Message When Server Down	Check this check-box if you want Cisco ISE to buffer the syslog messages when TCP syslog targets and secure syslog targets are unavailable. ISE retries sending the messages to the target when the connection resumes. After the connection resumes, messages are sent by the order from oldest to newest and 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 existing buffered messages for the specific target are lost.
Reconnect Timeout (Sec)	Give in seconds how long will the TCP and secure syslogs be kept before being discarded, when the server is down.
Select CA Certificate	Select a client certificate.
Ignore Server Certificate Validation	Check this check-box if you want ISE to ignore server certificate authentication and accept any syslog server.

Related Topics

- Cisco ISE Logging Mechanism
- Cisco ISE System Logs
- Remote Syslog Message Format
- Cisco ISE Message Catalogs
- Collection Filters
- Event Suppression Bypass Filter
- Configure Remote Syslog Collection Locations
- Configure Collection Filters

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.

Procedure

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 **Administrative and Operational Audit** logging category, then click **Edit**.

Step 4 Choose WARN from the **Log Severity Level** drop-down list.

Step 5 In the **Targets** field, 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:

- **AAA Audit**.

  Note that INFO is the default log severity level for this category and cannot be edited.

- **Posture and Client Provisioning Audit**.

Logging Category Settings

The following table describes the fields on the Logging Categories page, which you can use to configure the log severity level and choose logging targets for the logs of selected categories to be stored. The navigation path for this page is **Administration > System > Logging > Logging Categories**.

Table 4: Logging Category Settings

Fields	Usage Guidelines
Name	Displays the name of the logging category.

Fields	Usage Guidelines
Log Severity Level	Allows you to choose the severity level for the diagnostic logging categories from the following options: • **FATAL**—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately • **ERROR**—This option indicates a critical or error condition. • **WARN**—This option indicates a normal but significant condition. This is the default condition. • **INFO**—This option indicates an informational message. • **DEBUG**—This option indicates a diagnostic bug message.
Local Logging	Check this check box to enable logging event for the category on the local node.
Target	Allows you to change the targets for a category by transferring the targets between the Available and the Selected boxes using the left and right icons. The Available box contains the existing logging targets, both local (predefined) and external (user-defined). The Selected box, which is initially empty, contains the selected targets for the specific category.

Related Topics

Remote Syslog Message Format
Cisco ISE Message Codes
Configure Remote Syslog Collection Locations
Set Severity Levels for Message Codes

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.

Procedure

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.

Note

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.

Certificate Management in Cisco ISE

A certificate is an electronic document that identifies an individual, a server, a company, or other entity and associates that entity with a public key. A self-signed certificate is signed by its own creator. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). A CA-signed digital certificate is considered industry standard and more secure.

Certificates are used in a network to provide secure access. Cisco ISE uses certificates for internode communication, and for communicating with external servers such as the syslog server, feed server, and all the end-user portals (guest, sponsor, and personal devices portals). Certificates identify a Cisco ISE node to an endpoint and secures the communication between that endpoint and the Cisco ISE node.

You can use the Admin portal to manage certificates for all the nodes in your deployment.

Certificates Enable Cisco ISE to Provide Secure Access

The Cisco Identity Services Engine (ISE) relies on public key infrastructure (PKI) to provide secure communication with both endpoints and administrators, as well as between Cisco ISE nodes in a multinode deployment. PKI relies on X.509 digital certificates to transfer public keys for encryption and decryption of messages, and to verify the authenticity of other certificates representing users and devices. Cisco ISE provides the Admin Portal to manage the following two categories of X.509 certificates:

- System certificates—These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own system certificates, each of which are stored on the node along with the corresponding private key.
- Trusted certificates—These are certificate authority (CA) certificates used to establish trust for the public keys received from users and devices. The Trusted Certificates Store also contains certificates that are distributed by the Simple Certificate Enrollment Protocol (SCEP), which enables registration of mobile devices into the enterprise network. Certificates in the Trusted Certificates Store are managed on the Primary Administration Node (PAN), and are automatically replicated to all other nodes in an Cisco ISE deployment.

In a distributed deployment, you must import the certificate only in to the certificate trust list (CTL) of the PAN. The certificate gets replicated to the secondary nodes.

In general, to ensure certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verification functions, use lower case hostnames for all Cisco ISE nodes deployed in a network.

Certificate Usage

When you add or import a certificate in to Cisco ISE, you should specify the purpose for which the certificate is to be used:

- Admin: For internode communication and authenticating the Admin portal
- EAP: For TLS-based EAP authentication
- RADIUS DTLS: For RADIUS DTLS server authentication
- Portal: For communicating with all Cisco ISE end-user portals
- xGrid: For communicating with the pxGrid controller

You can associate different certificates from each node for communicating with the Admin portal (Admin), the pxGrid controller (xGrid), and for TLS-based EAP authentication (EAP). However, you can associate only one certificate from each node for each of these purposes.

With multiple Policy Service nodes (PSNs) in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that has to be used for portal communication. When you add or import certificates that are designated for portal use, you must define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. You must associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that has to be used when communicating with each of these portals. You can designate one certificate from each node for each of the portals.

Note EAP-TLS client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers:

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

Certificate Matching in Cisco ISE

When you set up Cisco ISE nodes in a deployment, those two nodes communicate with each other. The system checks the FQDN of each ISE node to ensure they match (for example ise1.cisco.com and ise2.cisco.com or if you use wild card certificates then *.cisco.com). In addition, when an external machine presents a certificate

to an ISE server, the external certificate that is presented for authentication is checked (or matched) against the certificate in the ISE server. If the two certificates match, the authentication succeeds.

For , matching is performed between the nodes (if there are two) and between the and pxGrid.

Cisco ISE checks for a matching subject name as follows:

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

Note X.509 certificates imported to Cisco ISE must be in privacy-enhanced mail (PEM) or distinguished encoding rule (DER) format. Files containing a certificate chain, which is a system certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions.

Validity of X.509 Certificates

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

- Colored expiration status icons appear in the System Certificates page.
- Expiration messages appear in the Cisco ISE System Diagnostic report.
- Expiration alarms are generated at 90 days, 60 days, and every day in the final 30 days before expiration.

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

Enable PKI in Cisco ISE

Public Key Infrastructure (PKI) is a cryptographic technique that enables secure communication and verifies the identity of a user using digital signatures.

Procedure

Step 1 Establish system certificates on each deployment node for TLS-enabled authentication protocols such as EAP-TLS, for authenticating the Admin portal, for browser and REST clients to access the Cisco ISE web portals, and for the pxGrid controller.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for EAP authentication, Admin portal, portals, and pxGrid controller. In a typical enterprise environment, this certificate is replaced with server certificates that are signed by a trusted CA.

Step 2 Populate the Trusted Certificates Store with the CA certificates that are necessary to establish trust with the user as well as device certificates that will be presented to Cisco ISE.

To validate the authenticity of a user or device certificate with a certificate chain that consists of a root CA certificate and one or more intermediate CA certificates:

- Enable trust option for the root CA.

  From the Cisco ISE GUI, choose **Administration** > **System** >**Certificate** > **Certificate Management** > **Trusted certificates**. In this window, select the root CA certificate, click **Edit**. In the **Usage** tab, check the check boxes in the section **Trusted For**.

- If you do not want to enable the trust option for the root CA, import the entire CA certificate chain into the Trusted Certificates Store.

For inter-node communication, you must populate the Trusted Certificates Store with the trust certificate(s) needed to validate the Admin system certificate belonging to each node in the Cisco ISE deployment. If you want to use the default self-signed certificate for internode communication, then you must export this certificate from the System Certificates page of each Cisco ISE node and import it into the Trusted Certificates Store. If you replace the self-signed certificates with CA-signed certificates, it is only necessary to populate the Trusted Certificates Store with the appropriate root CA and intermediate CA certificates. Be aware that you cannot register a node in a Cisco ISE deployment until you complete this step.

If you use self-signed certificates to secure communication between a client and PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and PSN with an externally-signed CA certificate or use wildcard certificates signed by an external CA.

Note After you obtain a backup from a standalone Cisco ISE node or the PAN, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore data. Otherwise, if you try to restore data using the older backup, communication between the nodes might fail.

Wildcard Certificates

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

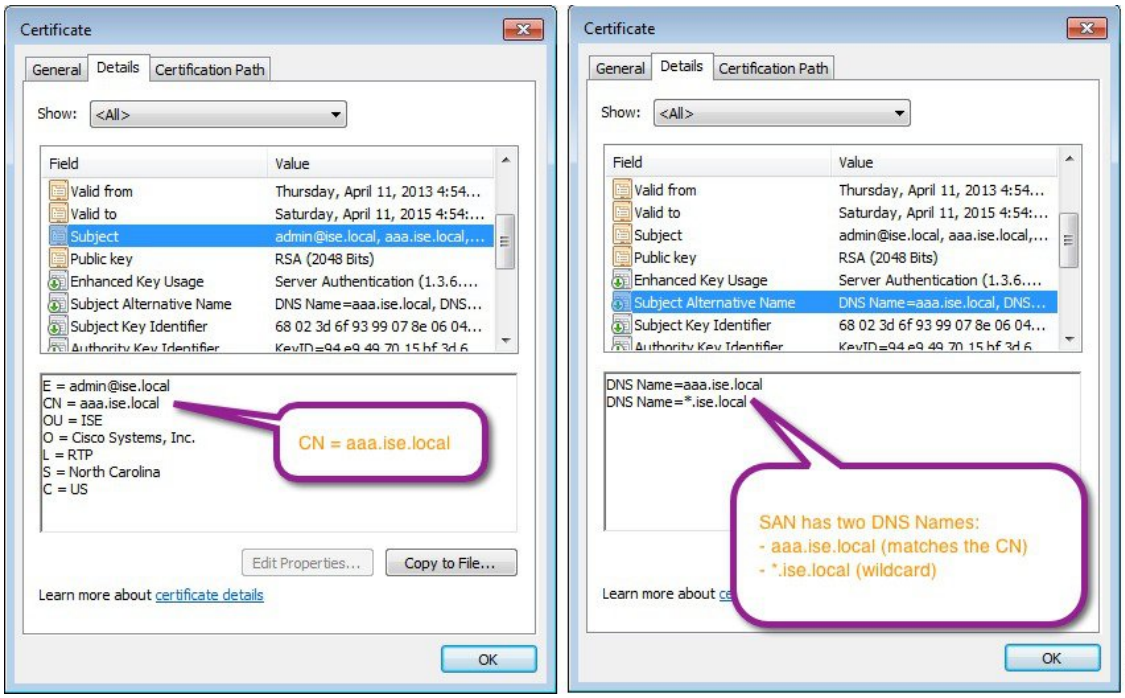
If you configure a wildcard certificate to use *.ise.local, you can use the same certificate to secure any other host whose DNS name ends with ".ise.local," such as :

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

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

The following figure shows an example of a wildcard certificate that is used to secure a web site.

Figure 1: Wildcard Certificate Example



Wildcard Certificate Support in Cisco ISE

Cisco ISE supports wildcard certificates. In earlier releases, Cisco ISE verified any certificate enabled for HTTPS to ensure the CN field matches the Fully Qualified Domain Name (FQDN) of the host exactly. If the fields did not match, the certificate could not be used for HTTPS communication.

In earlier releases, Cisco ISE used that CN value to replace the variable in the url-redirect A-V pair string. For all Centralized Web Authentication (CWA), onboarding, posture redirection, and so on, the CN value was used.

Cisco ISE uses the hostname of the ISE node as the CN.

Wildcard Certificates for HTTPS and EAP Communication

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

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

Note If you use wildcard certificates, we strongly recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it can lead to serious security issues.

Wildcard certificate uses an asterisk (*) and a period before the domain name. For example, the CN value for a certificate's Subject Name would be a generic host name such as aaa.ise.local and the SAN field would have the wildcard character such as *.ise.local. Cisco ISE supports wildcard certifications in which the wildcard character (*) is the left most character in the presented identifier. For example, *.example.com or *.ind.example.com. Cisco ISE does not support certificates in which the presented identifier contains additional characters along with the wildcard character. For example, abc*.example.com or a*b.example.com or *abc.example.com.

Fully Qualified Domain Name in URL Redirection

When Cisco ISE builds an authorization profile redirect (for central web authentication, device registration web authentication, native supplicant provisioning, mobile device management, and client provisioning and posture services), the resulting cisco-av-pair includes a string similar to the following:

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

When processing this request, Cisco ISE substitutes actual values for some keywords in this string. For example, SessionIdValue is replaced with the actual session ID of the request. For eth0 interface, Cisco ISE replaces the IP in the URL with the FQDN of the Cisco ISE node. For non-eth0 interfaces, Cisco ISE uses the IP address in the URL. You can assign a host alias(name) for interfaces eth1 through eth3, which Cisco ISE can then substitute in place of IP address during URL redirection.

To do this, you can use the **ip host** command in the configuration mode from the Cisco ISE CLI ISE /admin(config)# prompt:

ip host *IP_address host-alias FQDN-string*

where IP_address is the IP address of the network interface (eth1 or eth2 or eth3) and host-alias is the name that you assign to the network interface. FQDN-string is the fully qualified domain name of the network interface. Using this command, you can assign a host-alias or an FQDN-string or both to a network interface.

Here is an example using the **ip host** command: ip host a.b.c.d sales sales.amerxyz.com

After you assign a host alias to the non-eth0 interface, you must restart the application services on Cisco ISE using the **application start ise** command.

Use the no form of this command to remove the association of the host alias with the network interface.

no ip host *IP_address host-alias FQDN-string*

Use the **show running-config** command to view the host alias definitions.

If you provide the FQDN-string, Cisco ISE replaces the IP address in the URL with the FQDN. If you provide only the host alias, Cisco ISE combines the host alias with the configured IP domain name to form a complete FQDN, and replaces the IP address in the URL with the FQDN. If you do not map a network interface to a host alias, then Cisco ISE uses the IP address of the network interface in the URL.

When you make use of non-eth0 interfaces for client provisioning or native supplicant or guest flows, you have to make sure that the IP address or host alias for non-eth0 interfaces should be configured appropriately in the Policy Service node certificate's SAN fields.

Advantages of Using Wildcard Certificates

- Cost savings. Certificates signed by a third party Certificate Authority is expensive, especially as the number of servers increase. Wildcard certificates may be used on multiple nodes in the Cisco ISE deployment.
- Operational efficiency. Wildcard certificates allow all Policy Service Node (PSN) EAP and web services to share the same certificate. In addition to significant cost savings, certificate administration is also simplified by creating the certificate once and applying it on all the PSNs.
- Reduced authentication errors. Wildcard certificates address issues seen with Apple iOS devices where the client stores trusted certificates within the profile, and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a PSN, it does not explicitly trust the PSN certificate, even though a trusted Certificate Authority has signed the certificate. Using a wildcard certificate, the certificate will be the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without error or prompting.
- Simplified supplicant configuration. For example, Microsoft Windows supplicant with PEAP-MSCHAPv2 and server certificate trust enabled requires that you specify each of the server certificate to trust, or the user may be prompted to trust each PSN certificate when the client connects using a different PSN. With wildcard certificates, a single server certificate can be trusted rather than individual certificates from each PSN.
- Wildcard certificates result in an improved user experience with less prompting and more seamless connectivity.

Disadvantages of Using Wildcard Certificates

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

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

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

Security devices such as ASA also support wildcard certificates.

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

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

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

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

Wildcard Certificate Compatibility

Wildcard certificates are usually created with the wildcard listed as the Common Name (CN) of the Certificate Subject. Cisco ISE supports this type of construction. However, not all endpoint supplicants support the wildcard character in the Certificate Subject.

All Microsoft native supplicants tested (including Windows Mobile) do not support wildcard character in the Certificate Subject.

You can use another supplicant, such as Cisco AnyConnect Network Access Manager (NAM) that might allow the use of wildcard character in the Subject field.

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

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

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

Certificate Hierarchy

From the Admin portal, you can view the certificate hierarchy or the certificate trust chain of all endpoint, system, and trusted certificates. The certificate hierarchy includes the certificate, all intermediate Certificate Authority (CA) certificates, and the root certificate. For example, when you choose to view a system certificate from the the Admin portal, by default, the details of the corresponding system certificate appear. The certificate hierarchy appears at the top of the certificate. Click any of the certificates in the hierarchy to view its details. The self-signed certificate does not have any hierarchy or trust chain.

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

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

System Certificates

Cisco ISE system certificates are server certificates that identify a Cisco ISE node to other nodes in the deployment and to client applications. System certificates are:

- Used for inter-node communication in a Cisco ISE deployment. Choose the Admin option in the Usage field for these certificates.
- Used by browser and REST clients who connect to Cisco ISE web portals. Choose the Portal option in the Usage field for these certificates.
- Used to form the outer TLS tunnel with PEAP and EAP-FAST. Choose the EAP option in the Usage field for mutual authentication with EAP-TLS, PEAP, and EAP-FAST.
- Used for RADIUS DTLS server authentication.

- Used to communicate with the SAML Identity Provider (IdP). Choose the SAML option in the Usage field for this certificate. If you choose the SAML option, you cannot use this certificate for any other service.
- Used to communicate with the pxGrid controller. Choose the pxGrid option in the Usage field for these certificates.

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

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

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

Note When you export a wildcard system certificate to be imported in to the other nodes (for inter-node communication), ensure that you export the certificate and private key, and specify an encryption password. During import, you will need the certificate, private key, and encryption password.

Note To find out the supported key and cipher information for your release, please find the appropriate version of the Cisco Identity Services Engine Network Component Compatibility guide.

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

1. Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 75
2. Import the Root Certificates to the Trusted Certificate Store, on page 69
3. Bind the CA-Signed Certificate to the CSR, on page 76

ISE Community Resource

How To: Implement ISE Server-Side Certificates

Certificate Renewal on Cisco Identity Services Engine Configuration Guide

View System Certificates

The System Certificate page lists all the system certificates added to Cisco ISE.

Before you begin

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

Procedure

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

The System Certificates page appears and provides the following information for the local certificates:

- Friendly Name—Name of the certificate.
- Used By—Service for which this certificate is used.
- Portal group tag—Applicable only for certificates that are designated for portal use. Specifies which certificate has to be used for the portals.
- Issued To—Common Name of the certificate subject.
- Issued By—Common Name of the certificate issuer
- Valid From—Date on which the certificate was created, also known as the Not Before certificate attribute.
- Expiration Date—Expiration date of the certificate, also known as the Not After certificate attribute. Indicates when the certificate expires. There are five categories along with an associated icon that appear here:
  - Expiring in more than 90 days (green icon)
  - Expiring in 90 days or less (blue icon)
  - Expiring in 60 days or less (yellow icon)
  - Expiring in 30 days or less (orange icon)
  - Expired (red icon)

Step 2 Select a certificate and choose **View** to display the certificate details.

Import a System Certificate

You can import a system certificate for any Cisco ISE node from the Admin portal.

Note Changing the certificate of the admin role certificate on a Primary PAN restarts services on all other nodes. The system restarts one node at a time, after the Primary Administration Node (PAN) restart has completed.

Before you begin

- Ensure that you have the system certificate and the private key file on the system that is running the client browser.

- If the system certificate that you import is signed by an external CA, import the relevant root CA and intermediate CA certificates in to the Trusted Certificates Store (**Administration > System > Certificates > Trusted Certificates**).
- Do not import a server certificate that is signed with a hash algorithm greater than SHA-256.
- If the system certificate that you import contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.
- To perform the following task, you must be a Super Admin or System Admin.

Procedure

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

Step 2 Click **Import**.
The Import Server Certificate screen opens.

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

Step 4 Click **Submit**.

System Certificate Import Settings

The following table describes the fields in the Import System Certificate page that you can use to import a server certificate. The navigation path for this page is: **Administration** > > > **System** > **Certificates** > **System Certificates** > **Import**.

Table 5: System Certificate Import Settings

Field Name	Description
Select Node	(Required) Choose the Cisco ISE node on which you want to import the system certificate.
Certificate File	(Required) Click **Browse** to select the certificate file from your local system.
Private Key File	(Required) Click **Browse** to select the private key file.
Password	(Required) Enter the password to decrypt the private key file.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
Allow Wildcard Certificates	Check this check box if you want to import a wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com. If you check this check box, Cisco ISE imports this certificate to all the other nodes in the deployment.

Field Name	Description
Validate Certificate Extensions	Check this check box if you want Cisco ISE to validate the certificate extensions. If you check this check box and the certificate that you are importing contains a basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and that the keyEncipherment bit or the keyAgreement bit, or both, are also set.
Usage	Choose the service for which this system certificate should be used: • **Admin**: Server certificate used to secure communication with the Admin portal and between ISE nodes in a deployment **Note** Changing the certificate of the admin role certificate on a Primary PAN restarts services on all other nodes. • **EAP Authentication**: Server certificate used for authentications that use the EAP protocol for SSL/TLS tunneling • **RADIUS DTLS**: Server certificate used for RADIUS DTLS authentication • **pxGrid**: Client and server certificate to secure communication between the pxGrid client and server • **SAML**: Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, etc. • **Portal**: Server certificate used to secure communication with all Cisco ISE web portals

Related Topics

System Certificates, on page 52
View System Certificates, on page 53
Import a System Certificate, on page 54

Generate a Self-Signed Certificate

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

Note If you are using a self-signed certificate and you must change the hostname of your Cisco ISE node, you must log in to the Admin portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE will continue to use the self-signed certificate with the old hostname.

Before you begin

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

Procedure

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

To generate a self-signed certificate from a secondary node, choose **Administration** > **System** > **Server Certificate**.

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

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

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

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

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

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

Self-Signed Certificate Settings

The following table describes the fields in the Generate Self Signed Certificate page. This page allows you to create system certificates for inter-node communication, EAP-TLS authentication, Cisco ISE web portals, and to communicate with the pxGrid controller. The navigation path for this page is: **Administration** > **System** > **Certificates** > **System Certificates** > **Generate Self Signed Certificate**.

Table 6: Self-Signed Certificate Settings

Field Name	Usage Guidelines
Select Node	(Required) The node for which you want to generate the system certificate.
Common Name (CN)	(Required if you do not specify a SAN) By default, the common name is the Fully Qualified Domain Name of the ISE node for which you are generating the self-signed certificate.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	An IP address, DNS name, or Uniform Resource Identifier (URI)that is associated with the certificate.
Key Type	Specify the algorithm to be used for creating the public key: RSA or ECDSA.

Field Name	Usage Guidelines
Key Length	Specify the bit size for the public key. The following options are available for RSA: • 512 • 1024 • 2048 • 4096 The following options are available for ECDSA: • 256 • 384 **Note** RSA and ECDSA public keys might have different key length for the same security level. Choose 2048 if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.
Digest to Sign With	Choose one of the following hashing algorithm: SHA-1 or SHA-256.
Certificate Policies	Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs.
Expiration TTL	Specify the number of days after which the certificate will expire.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
Allow Wildcard Certificates	Check this check box if you want to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com.

Field Name	Usage Guidelines
Usage	Choose the service for which this system certificate should be used: • **Admin**: Server certificate used to secure communication with the Admin portal and between ISE nodes in a deployment • **EAP Authentication**: Server certificate used for authentications that use the EAP protocol for SSL/TLS tunneling • **RADIUS DTLS**: Server certificate used for RADIUS DTLS authentication • **pxGrid**: Client and server certificate to secure communication between the pxGrid client and server • **SAML**: Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, etc. • **Portal**: Server certificate used to secure communication with all Cisco ISE web portals

Related Topics

System Certificates, on page 52
View System Certificates, on page 53
Generate a Self-Signed Certificate, on page 56

Edit a System Certificate

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

Before you begin

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

Procedure

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

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

Step 3 To renew a self-signed certificate, check the **Renewal Period** check box and enter the Expiration TTL (Time to Live) in days, weeks, months, or years.

Step 4 Click **Save** to save your changes.

If the **Admin** check box is checked, then the application server on the Cisco ISE node will be restarted. In addition, if the Cisco ISE node is the PAN in a deployment, then the application server on all other nodes in the deployment will also be restarted. The system restarts one node at a time, after the Primary Administration Node (PAN) restart has completed.

Note Using Chrome 65 and above to launch ISE can cause BYOD portal or Guest portal to fail to launch in the browser even though URL is redirected successfully. This is because of a new security feature introduced by Google that requires all certificates to have a Subject Alternative Name field. For releases ISE 2.4 and later, you must fill the Subject Alternative Name field.

To launch with Chrome 65 and above, follow the steps below:

1. Generate a new self-signed certificate from ISE GUI by filling the Subject Alternative Name field. Both DNS and IP Address must be filled.

2. ISE services will now restart.

3. Redirect the portal in Chrome browser.

4. From browser View Certificate>Details>Copy the certificate by selecting base-64 encoded.

5. Install the certificate in Trusted path.

6. Close the Chrome browser and try to redirect the portal.

Note When configuring wireless BYOD setup for the browser Firefox 64 and above, with operating systems Win RS4 or RS5, you may not be able to add Certificate Exception. This behaviour is expected in the case of fresh installs of Firefox 64 and above, and does not occur in the case of upgrading to Firefox 64 and above from a previous version. The following steps will allow you to add certificate exception in this case:

1. Configure for BYOD flow single/dual PEAP or TLS.

2. Configure CP Policy with Windows ALL option.

3. Connect Dot1.x/MAB SSID in end client Windows RS4/RS5.

4. Type 1.1.1.1 in FF64 browser for redirection to Guest/BYOD portal.

5. Click **Add Exception** > **Unable to add certificate**, and proceed with flow.

As a workaround, you will have to add the certificate manually for Firefox 64, by navigating **Options** > **Privacy & Settings** > **View Certificates** > **Servers** > **Add Exception**

Delete System Certificate

You can delete system certificates that you no longer use.

Even though you can delete multiple certificates from the System Certificates store at a time, you must have at least one certificate that can be used for Admin and EAP authentication. Also, you cannot delete any certificate that is in use for Admin, EAP Authentication, Portals, or pxGrid controller. However, you can delete the pxGrid certificate when the service is disabled.

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

Procedure

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

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

A warning message appears.

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

Export a System Certificate

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

Before you begin

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

Procedure

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

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

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

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

Step 4 Enter the password if you have chosen to export the private key. The password should be at least 8 characters long.

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

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

Trusted Certificates Store

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

The certificates in the Trusted Certificate Store are managed on the PAN, and are replicated to every node in the Cisco ISE deployment. Cisco ISE supports wildcard certificates.

Cisco ISE uses the trusted certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing ISE-PICthe Admin Portal using certificate-based administrator authentication.

- To enable secure communication between Cisco ISE nodes in a deployment. The Trusted Certificates Store must contain the chain of CA certificates needed to establish trust with the system certificate on each node in a deployment.
  - If a self-signed certificate is used for the system certificate, the self-signed certificate from each node must be placed in the Trusted Certificates Store of the PAN.
  - If a CA-signed certificate is used for the system certificate, the CA root certificate, as well as any intermediate certificates in the trust chain, must be placed in the Trusted Certificates Store of the PAN.
- To enable secure LDAP authentication, a certificate from the Certificate Store must be selected when defining an LDAP identity source that will be accessed over SSL.
- To distribute to personal devices preparing to register in the network using the personal devices portals. Cisco ISE implements the SCEP on Policy Service Nodes (PSN) to support personal device registration. A registering device uses the SCEP protocol to request a client certificate from a PSN. The PSN contains a registration authority (RA) that acts as an intermediary; it receives and validates the request from the registering device, and then forwards the request to an external CA or the internal Cisco ISE CA, which issues the client certificate. The CA sends the certificate back to the RA, which returns it to the device.

  Each SCEP CA used by Cisco ISE is defined by a SCEP RA Profile. When a SCEP RA Profile is created, two certificates are automatically added to the Trusted Certificates Store:
  - A CA certificate (a self-signed certificate)
  - An RA certificate (a Certificate Request Agent certificate), which is signed by the CA.

  The SCEP protocol requires that these two certificates be provided by the RA to a registering device. By placing these two certificates in the Trusted Certificates Store, they are replicated to all PSN nodes for use by the RA on those nodes.

Note When a SCEP RA Profile is removed, the associated CA chain is also removed from the Trusted Certificates Store.

Note

- X.509 certificates imported to Cisco ISE must be in Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rule (DER) format. Files containing a certificate chain, that is, a system certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions.
- When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until the ISE services are restarted

ISE Community Resource

Install a Third-Party CA Certificate in ISE 2.0

Certificates in Trusted Certificates Store

The Trusted Certificate Store is prepopulated with trusted certificates: Manufacturing certificate, Root certificate, and other trusted certificates. The Root certificate (Cisco Root CA) signs the Manufacturing (Cisco CA Manufacturing) certificate. These certificates are disabled by default. If you have Cisco IP phones as endpoints in your deployment, you should enable these two certificates so the Cisco-signed client certificates for the phones can be authenticated.

Trusted Certificate Store Page

The following table describes the fields on the Trusted Certificates Store page, which you can use to view the certificates that are added to the Administration node. The navigation path for this page is: **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Table 7: Certificate Store Page

Field Name	Usage Guidelines
Friendly Name	Displays the name of the certificate.
Status	Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Trusted for	Displays the service for which the certificate is used.
Issued To	Common Name (CN) of the certificate subject.
Issued By	Common Name (CN) of the certificate issuer.
Valid From	The "Not Before" certificate attribute.
Expiration Date	The "Not After" certificate attribute.
Expiration Status	Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column: • **Green**: Expiring in more than 90 days • **Blue**: Expiring in 90 days or less • **Yellow**: Expiring in 60 days or less • **Orange**: Expiring in 30 days or less • **Red**: Expired

Related Topics

Trusted Certificates Store, on page 61
View Trusted Store Certificates, on page 65
Change the Status of a Certificate in Trusted Certificates Store, on page 65
Add a Certificate to Trusted Certificates Store, on page 65

Trusted Certificate Naming Constraint

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

The following name constraints are supported:

- Directory name

  The Directory name constraint should be a prefix of the directory name in subject/SAN. For example,

  - Correct subject prefix:

    CA certificate name constraint: Permitted: O=Cisco

    Client certificate subject: O=Cisco,CN=Salomon

  - Incorrect subject prefix:

    CA certificate name constraint: Permitted: O=Cisco

    Client certificate subject: CN=Salomon,O=Cisco

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

The following name constraints are not supported:

- IP address
- Othername

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

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

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

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

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

View Trusted Store Certificates

The Trusted Certificates page lists all the trusted certificates that have been added to Cisco ISE. To view the trusted certificates, you must be a Super Admin or System Admin.

To view all the certificates, choose Choose **Administration** > **System** > **Certificates** > **Trusted Certificates**. The Trusted Certificates page appears, listing all the trusted certificates.

Before you begin

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

Change the Status of a Certificate in Trusted Certificates Store

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

Procedure

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

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

Step 3 Change the status.

Step 4 Click **Save**.

Add a Certificate to Trusted Certificates Store

The Certificate Store page allows you to add CA certificates to Cisco ISE.

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Ensure that the certificate store certificate resides on the file system of the computer where your browser is running. The certificate must be in PEM or DER format.
- If you plan to use the certificate for Admin or EAP authentication, ensure that the basic constraints are defined in the certificate and the CA flag is set to true.

Procedure

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

Step 2 Click **Import**.

Step 3 Configure the field values as necessary.

If you plan to use any sub-CA certificate in the certificate chain for EAP authentication or certificate-based administrator authentication, ensure that you check the **Trust for client authentication and Syslog** checkbox

while importing all the certificates in the certificate chain up until the Root CA. In Cisco ISE 2.6 patch 1 and above, you can import more than one CA certificate with the same subject name. For certificate-based administrator authentication, select the checkbox **Trust for certificate based admin authentication** when adding a trusted certificate.

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

Edit a Trusted Certificate

After you add a certificate to the Trusted Certificates Store, you can further edit it by using the edit settings.

Before you begin

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

Procedure

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

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

Step 3 Modify the editable fields as required.

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

Edit Certificate Settings

The following table describes the fields on the Certificate Store Edit Certificate page, which you can use to edit the Certificate Authority (CA) certificate attributes. The navigation path for this page is: **Administration** > **System** > **Certificates** > **Trusted Certificates** > **Certificate** > **Edit**.

Table 8: Certificate Store Edit Settings

Field Name	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate.
Status	Choose Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Description	Enter an optional description.
Usage	
Trust for authentication within ISE	Check the check box if you want this certificate to verify server certificates (from other ISE nodes or LDAP servers).

Field Name	Usage Guidelines
Trust for client authentication and Syslog	(Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to ISE using the EAP protocol • Trust a Syslog server
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.
Certificate Status Validation	ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second is to validate the certificate against a Certificate Revocation List (CRL) which is downloaded from the CA into ISE. Both of these methods can be enabled, in which case OCSP is used first, and only if a status determination cannot be made then the CRL is used.
Validate Against OCSP Service	Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box.
Reject the request if OCSP returns UNKNOWN status	Check the check box to reject the request if certificate status is not determined by OCSP. If you check this check box, an unknown status value returned by the OCSP service will cause ISE to reject the client or server certificate currently being evaluated.
Reject the request if OCSP Responder is unreachable	Check the check box for ISE to reject the request if the OCSP Responder is not reachable.
Download CRL	Check the check box for the Cisco ISE to download a CRL.
CRL Distribution URL	Enter the URL to download the CRL from a CA. This field will be automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.”
Retrieve CRL	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.

Field Name	Usage Guidelines
If download failed, wait	Configure the time interval to wait before Cisco ISE tries to download the CRL again.
Bypass CRL Verification if CRL is not Received	Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.
Ignore that CRL is not yet valid or expired	Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL. Uncheck this check box if you want Cisco ISE to check the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected.

Related Topics

Trusted Certificates Store, on page 61
Edit a Trusted Certificate, on page 66

Delete Trusted Certificates

You can delete trusted certificates that you no longer need. However, ensure that you do not delete the ISE Internal CA (Certificate Authority) certificates. The ISE Internal CA certificates can be deleted only when you replace the ISE Root Certificate Chain for the entire deployment.

Procedure

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

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

A warning message appears. If you have chosen to delete the ISE Internal CA certificates, click:

- **Delete**—To delete the ISE internal CA certificates. All endpoint certificates signed by the ISE Internal CA become invalid and the endpoints cannot get on to the network. To allow the endpoints on the network again, import the same ISE Internal CA Certificates in to the Trusted Certificates store.
- **Delete & Revoke**—Deletes and revokes the ISE internal CA certificates. All endpoint certificates signed by the ISE Internal CA become invalid and the endpoints cannot get on to the network. This operation cannot be undone. You must replace the ISE Root Certificate Chain for the entire deployment.

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

Export a Certificate from the Trusted Certificates Store

Before you begin

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

Note If you are exporting certificates from the internal CA, and plan to use that export to restore from backup, you must use the CLI command `application configure ise`. For more information, see Export Cisco ISE CA Certificates and Keys, on page 98.

Procedure

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

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

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

Import the Root Certificates to the Trusted Certificate Store

While importing the root CA and intermediate CA certificates, you can specify the service(s) for which the Trusted CA certificates are to be used.

Before you begin

You must have the root certificate and other intermediate certificates from the Certificate Authority that signed your CSRs and returned the digitally signed CA certificates.

Procedure

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

Step 2 Click **Import**.

Step 3 In the **Import a new Certificate into the Certificate Store** window that is displayed, click **Choose File** to select the root CA certificate signed and returned by your CA.

Step 4 Enter a **Friendly Name**.

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

Step 5 Check the check boxes next to the services for which you want to use this trusted certificate for.

Step 6 (Optional) In the **Description** field, enter a description for your certificate.

Step 7 Click **Submit**.

What to do next

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

Trusted Certificate Import Settings

The following table describes the fields on the Trusted Certificate Import page, which you can use to add Certificate Authority (CA) certificates to Cisco ISE. The navigation path for this page is: **Administration** > **System** > **Certificates** > **Trusted Certificates** > **Import**.

Table 9: Trusted Certificate Import Settings

Fields	Description
Certificate File	Click **Browse** to choose the certificate file from the computer that is running the browser.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name>#<issuer>#<nnnnn>, where <nnnnn> is a unique five-digit number.
Trust for authentication within ISE	Check the check box if you want this certificate to be used to verify server certificates (from other ISE nodes or LDAP servers).
Trust for client authentication and Syslog	(Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to ISE using the EAP protocol • Trust a Syslog server
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.
Validate Certificate Extensions	(Only if you check both the Trust for client authentication and Enable Validation of Certificate Extensions options) Ensure that the “keyUsage” extension is present and the “keyCertSign” bit is set, and that the basic constraints extension is present with the CA flag set to true.
Description	Enter an optional description.

Related Topics

Trusted Certificates Store, on page 61
Certificate Chain Import, on page 71
Import the Root Certificates to the Trusted Certificate Store, on page 69

Certificate Chain Import

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

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

Importing a certificate chain is a two-step process:

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

Install Trusted Certificates for Cisco ISE Inter-node Communication

When you set up the deployment, before you register a secondary node, you must populate the PAN's Certificate Trust List (CTL) with appropriate CA certificates that are used to validate the Admin certificate of the secondary node. The procedure to populate the CTL of the PAN is different for different scenarios:

- If the secondary node is using a CA-signed certificate to communicate with the Admin portal, you must import the CA-signed certificate of the secondary node, the relevant intermediate certificates(if any), and the root CA certificate (of the CA that signed the secondary node's certificate) in to the CTL of the PAN.
- If the secondary node is using a self-signed certificate to communicate with the Admin portal, you can import the self-signed certificate of the secondary node in to the CTL of the PAN.

Note

- If you change the Admin certificate on a registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node’s Admin certificate and import it in to the CTL of the PAN.
- If you use self-signed certificates to secure communication between a client and PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and PSN with an externally-signed CA certificate or use wildcard certificates signed by an external CA.

Ensure that the certificate issued by the external CA has basic constraints defined and the CA flag set to true. To install CA-signed certificates for inter-node communication, carry out the following steps. For information on these tasks, refer to Chapter "Basic Setup" in the *Cisco ISE Administrator Guide*.

Procedure

Step 1 Create a Certificate Signing Request (CSR) and submit the CSR to a Certificate Authority.

Step 2 Import the root certificates to the trusted certificate store.

Step 3 Bind the CA-signed certificate to the CSR.

Default Trusted Certificates in Cisco ISE

The Trusted Certificates store (**Administration** > **System** > **Certificates** > **Trusted Certificates**) in Cisco ISE includes some certificates that are available by default. These certificates are automatically imported into the store to meet security requirements. However, it is not mandatory for you to use all of them. Unless mentioned otherwise in the table below, you can use certificates of your choice instead of the ones that are already available.

Table 10:

Trusted Certificate Name	Serial Number	Purpose of the Certificate	Cisco ISE Releases with Certificate
Baltimore CyberTrust Root CA	02 00 00 B9	This certificate can serve as the root CA certificate in CA chains used by cisco.com in some geographies. The certificate was also used in ISE 2.4 posture/CP update XML files when they hosted at https://s3.amazonaws.com.	Releases 2.4 and above.
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	This certificate can serve as the root CA certificate for the CA chain used by cisco.com.	Releases 2.4 and above.
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	This certificate can serve as the root CA . certificate for the CA chain used by cisco.com and perfigo.com.	Releases 2.4 and above.
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	This certificate serves as the root CA certificate for VeriSign Class 3 Secure Server CA-G3. You must use this certificate when configuring profiler feed services in Cisco ISE.	Releases 2.4 and above.

Trusted Certificate Name	Serial Number	Purpose of the Certificate	Cisco ISE Releases with Certificate
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	Thist is an intermediate CA certificate that expires on February 7, 2020. You do not need to renew this certificate. You can remove the certificate by following the task below.	Releases 2.4 and above.
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	This certificate may be used by certain Cisco devices connecting to Cisco ISE. The certificate is disabled by default.	Releases 2.4 and 2.6.
Cisco Manufacturing CA SHA2	02	This certificate can be used in CA chains for administrator authentications, endpoint authentications and deployment infrastructure flows.	Releases 2.4 and above.
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	This certificate can be used by certain Cisco devices connecting to Cisco ISE. The certificate is disabled by default.	Releases 2.4 and above.
Cisco Root CA M2	01	This certificate can be used in CA chains for administrator authentications, endpoint authentications and deployment infrastructure flows.	Releases 2.4 and above.
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	You must use this certificate for flows where guest login with Facebook is used.	Releases 2.4 and above.
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	You must use this certificate for flows where guest login with Facebook is used.	Releases 2.4 and above.

Trusted Certificate Name	Serial Number	Purpose of the Certificate	Cisco ISE Releases with Certificate
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Trusted for Cisco services.	Releases 2.4 and 2.6.
QuoVadis Root CA 2	05 09	You must use this certificate in profiler, posture, and client provisioning flows.	Releases 2.4 and above.
Cisco ECC Root CA	01	This certificate is part of the Cisco Trust root store bundle used in Cisco ISE.	Release 2.6.
Cisco Licensing Root CA	01	This certificate is part of the Cisco Trust root store bundle used in Cisco ISE.	Releases 2.6 and above.
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	This certificate is part of the Cisco Trust root store bundle used in Cisco ISE.	Releases 2.6 and above.
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	This certificate is part of the Cisco Trust Root Store bundle used in Cisco ISE.	Releases 2.6 and above.
Cisco RXC-R2	01	This certificate is part of the Cisco Trust root store bundle used in Cisco ISE.	Releases 2.6 and above.
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	This certificate is part of the Cisco Trust root store bundle used in Cisco ISE.	Releases 2.6 and above.
Cisco ECC Root CA 2099	03	This certificate is part of the Cisco Trust root store bundle used in Cisco ISE.	Releases 2.6 and above.

Remove a Default Trusted Certificate from Cisco ISE

- Go to **Administration** > **System** > **Certificates** > **Trusted Certificates** to view all your trusted certificates.
- Export the certificate you wish to delete and save it, so that it can be imported again if needed.

  Click the check box against the certificate you wish to export, and click **Export** on the menu bar above. The key chain will download to your system.
- Delete the certificate. Click the check box against the certificate you wish to delete, and click **Delete** on the menu bar above. You will not be allowed to delete the certificate if it is being used by any CA chain, secure syslog, or secure LDAP.

- Make the necessary configuration changes to remove the certificate from the CA chain(s), secure syslogs, and syslogs it is part of, and then delete the certificate.
- After the certificate is deleted, check that the related services (refer to the purpose of the certificate) are working as expected.

Certificate Signing Requests

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

The list of Certificate Signing Requests (CSRs) that you have created is available in the Certificate Signing Requests page. To obtain signatures from a Certificate Authority (CA), you must export the CSRs and then send the certificates to the CA. The CA signs and returns your certificates.

You can manage the certificates centrally from the Admin portal. You can create CSRs for all nodes in the deployment and export them. Then you should submit the CSRs to a CA, obtain the CA-signed certificates from the CA, import the root and intermediary CA certificates returned by the CA in to the Trusted Certificates Store, and bind the CA-signed certificates to the CSRs.

Create a Certificate Signing Request and Submit the CSR to a Certificate Authority

You can generate a certificate signing request (CSR) to obtain a CA-signed certificate for the nodes in your deployment. You can generate the CSR for select nodes in the deployment or for all the nodes in your deployment.

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Signing Requests**

Step 2 Enter the values for generating a CSR. See Certificate-Signing Request Settings for information on each of the fields.

Step 3 Click **Generate** to generate the CSR.

The CSR is generated.

Step 4 Click **Export** to open the CSR in a Notepad.

Step 5 Copy all the text from "-----BEGIN CERTIFICATE REQUEST-----" through "-----END CERTIFICATE REQUEST-----."

Step 6 Paste the contents of the CSR in to the certificate request of a chosen CA.

Step 7 Download the signed certificate.

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

Bind the CA-Signed Certificate to the CSR

After you have the digitally signed certificate returned by the CA, you must bind it to the certificate signing request (CSR). You can perform the bind operation for all the nodes in your deployment from the Admin portal.

Before you begin

- You must have the digitally signed certificate, and the relevant root intermediate CA certificates returned by the CA.
- Import the relevant root and intermediate CA certificates in to the Trusted Certificates Store (**Administration** > **System** > **Certificates** > **Trusted Certificates**).

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Signing Requests**

Check the check box next to the node for which you are binding the CSR with the CA-signed certificate.

Step 2 Click **Bind**.

Step 3 Click **Browse** to choose the CA-signed certificate.

Step 4 Specify a Friendly Name for the certificate.

Step 5 Check the **Validate Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.

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

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

Step 6 Check the service for which this certificate will be used in the Usage area.

This information is autopopulated, if you have enabled the Usage option while generating the CSR. If you do not want to specify the usage at the time of binding the certificate, uncheck the Usage option. You can edit the certificate later and specify the usage.

Note Changing the certificate of the admin role certificate on a Primary PAN restarts services on all other nodes

Changing the certificate of the admin role certificate on a Primary PAN restarts services on all other nodes. The system restarts one node at a time, after the Primary Administration Node (PAN) restart has completed.

Step 7 Click **Submit** to bind the CA-signed certificate.

If you have chosen to use this certificate for Cisco ISE internode communication, the application server on the Cisco ISE node is restarted.

Repeat this process to bind the CSR with the CA-signed certificate on the other nodes.

What to do next

Import the Root Certificates to the Trusted Certificate Store, on page 69

Export a Certificate Signing Request

You can use this page to export certificate signing requests.

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Signing Requests**

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

Step 3 Click **OK** to save the file to the file system that is running the client browser.

Certificate-Signing Request Settings

Cisco ISE allows you to generate CSRs for all the nodes in your deployment from the Admin portal in a single request. Also, you can choose to generate the CSR for a single node or multiple both nodes in the deployment. If you choose to generate a CSR for a single node, ISE automatically substitutes the Fully Qualified Domain Name (FQDN) of the particular node in the CN= field of the certificate subject. If you choose to include an entry in the Subject Alternative Name (SAN) field of the certificate, you must enter the FQDN of the ISE node in addition to other SAN attributes. If you choose to generate CSRs for all the nodes in your deployment, check the Allow Wildcard Certificates check box and enter the wildcard FQDN notation in the SAN field (DNS name), for example, *.amer.example.com. If you plan to use the certificate for EAP Authentication, do not enter the wildcard value in the CN= field.

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

The following table describes the fields in the Certificate Signing Request (CSR) page, which you can use to generate a CSR that can be signed by a Certificate Authority (CA). The navigation path for this page is: **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Request**.

Table 11: Certificate Signing Request Settings

Field	Usage Guidelines
Certificate(s) will be used for	

Field	Usage Guidelines

	Choose the service for which you are going to use the certificate:
	Cisco ISE Identity Certificates
	• **Multi-Use**: Used for multiple services (Admin, EAP-TLS Authentication, pxGrid, and Portal). Multi-use certificates use both client and server key usages. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
	• **Admin**: Used for server authentication (to secure communication with the Admin portal and between ISE nodes in a deployment). The certificate template on the signing CA is often called a Web Server certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **EAP Authentication**: Used for server authentication. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	Note Digital signature key usage is required for EAP-TLS client certificates.
	• **RADIUS DTLS**: Used for RADIUS DTLS server authentication. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **Portal**: Used for server authentication (to secure communication with all ISE web portals). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)
	  • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
	• **pxGrid**: Used for both client and server authentication (to secure communication between the pxGrid client and server). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
	  • **Key Usage**: Digital Signature (Signing)

Field	Usage Guidelines
	• **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2) • **SAML**: Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, etc. • **Key Usage**: Digital Signature (Signing) • **Extended Key Usage**: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) **Note** We recommend that you do not use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute. If you use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute, the certificate is considered invalid and the following error message is displayed: `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE Certificate Authority Certificates** • **ISE Root CA**: (Applicable only for the internal CA service) Used for regenerating the entire internal CA certificate chain including the root CA on the Primary PAN and subordinate CAs on the PSNs. • **ISE Intermediate CA**: (Applicable only for the internal CA service when ISE acts as an intermediate CA of an external PKI) Used to generate an intermediate CA certificate on the Primary PAN and subordinate CA certificates on the PSNs. The certificate template on the signing CA is often called a Subordinate Certificate Authority. This template has the following properties: • **Basic Constraints**: Critical, Is a Certificate Authority • **Key Usage**: Certificate Signing, Digital Signature • **Extended Key Usage**: OCSP Signing (1.3.6.1.5.5.7.3.9) • **Renew ISE OCSP Responder Certificates**: (Applicable only for the internal CA service) Used to renew the ISE OCSP responder certificate for the entire deployment (and is not a certificate signing request). For security reasons, we recommend that you renew the ISE OCSP responder certificates every six months.
Allow Wildcard Certificates	Check this check box to use a wildcard character (*) in the CN and/or the DNS name in the SAN field of the certificate. If you check this check box, all the nodes in the deployment are selected automatically. You must use the asterisk (*) wildcard character in the left-most label position. If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it can lead to security issues.

Field	Usage Guidelines
Generate CSRs for these Nodes	Check the check boxes next to the nodes for which you want to generate the certificate. To generate a CSR for select nodes in the deployment, you must uncheck the Allow Wildcard Certificates option.
Common Name (CN)	By default, the common name is the FQDN of the ISE node for which you are generating the CSR. $FQDN$ denotes the FQDN of the ISE node. When you generate CSRs for multiple nodes in the deployment, the Common Name field in the CSRs is replaced with the FQDN of the respective ISE nodes.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	An IP address, DNS name, Uniform Resource Identifier (URI), or Directory Name that is associated with the certificate. • **DNS Name**: If you choose the DNS name, enter the fully qualified domain name of the ISE node. If you have enabled the Allow Wildcard Certificates option, specify the wildcard notation (an asterisk and a period before the domain name). For example, *.amer.example.com. • **IP Address**: IP address of the ISE node to be associated with the certificate. • **Uniform Resource Identifier**: A URI that you want to associate with the certificate. • **Directory Name**: A string representation of distinguished name(s) (DNs) defined per RFC 2253. Use a comma (,) to separate the DNs. For “dnQualifier” RDN, escape the comma and use backslash-comma “\,” as separator. For example, CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
Key Type	Specify the algorithm to be used for creating the public key: RSA or ECDSA.

Field	Usage Guidelines
Key Length	Specify the bit size for the public key. The following options are available for RSA: • 512 • 1024 • 2048 • 4096 The following options are available for ECDSA: • 256 • 384 **Note** RSA and ECDSA public keys might have different key length for the same security level. Choose 2048 or greater if you plan to get a public CA-signed certificate.
Digest to Sign With	Choose one of the following hashing algorithm: SHA-1 or SHA-256.
Certificate Policies	Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs.

Related Topics

Certificate Signing Requests, on page 75
Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 75
Bind the CA-Signed Certificate to the CSR, on page 76

Set Up Certificates for Portal Use

With multiple Policy Service nodes (PSNs) in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that has to be used for portal communication. When you add or import certificates that are designated for portal use, you must define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. You must associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that has to be used when communicating with each of these portals. You can designate one certificate from each node for each of the portals.

Note Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use).

Procedure

Step 1 Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 75.

You must choose a Certificate Group Tag that you have already defined or create a new one for the portal. For example, mydevicesportal.

Step 2 Import the Root Certificates to the Trusted Certificate Store, on page 69.

Step 3 Bind the CA-Signed Certificate to the CSR, on page 76.

Reassign Default Portal Certificate Group Tag to CA-Signed Certificate

By default, all Cisco ISE portals use the self-signed certificate. If you want to use a CA-signed certificate for portals, you can assign the default portal certificate group tag to a CA-signed certificate. You can use an existing CA-signed certificate or generate a CSR and obtain a new CA-signed certificate for portal use. You can reassign any portal group tag from one certificate to another.

Note When you edit an existing certificate, if the portal tag (guest) that is associated with the certificate is already in use by any of the portals, then you cannot reassign the default portal certificate group tag or any other portal group tag to this certificate. The system displays the list of portals that use the "guest" portal tag.

The following procedure describes how to reassign the default portal certificate group tag to a CA-signed certificate.

Procedure

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

Hover the mouse over the i icon next to the Default Portal Certificate Group tag to view the list of portals that use this tag. You can also view the ISE nodes in the deployment that have portal certificates which are assigned this tag.

Step 2 Check the check box next to the CA-signed certificate that you want to use for portals, and click **Edit**.

Be sure to choose a CA-signed certificate that is not in use by any of the portals.

Step 3 Under the **Usage** area, check the **Portal** check box and choose the Default Portal Certificate Group Tag.

Step 4 Click **Save**.

A warning message appears.

Step 5 Click **Yes** to reassign the default portal certificate group tag to the CA-signed certificate.

Associate the Portal Certificate Tag Before You Register a Node

If you use the "Default Portal Certificate Group" tag for all the portals in your deployment, before you register a new ISE node, ensure that you import the relevant CA-signed certificate, choose "Portal" as a service, and associate the "Default Portal Certificate Group" tag with this certificate.

When you add a new node to a deployment, the default self-signed certificate is associated with the "Default Portal Certificate Group" tag and the portals are configured to use this tag.

After you register a new node, you cannot change the Certificate Group tag association. Therefore, before you register the node to the deployment, you must do the following:

Procedure

Step 1 Create a self-signed certificate, choose "Portal" as a service, and assign a different certificate group tag (for example, tempportaltag).

Step 2 Change the portal configuration to use the newly created certificate group tag (tempportaltag).

Step 3 Edit the default self-signed certificate and remove the Portal role.

This option removes the Default Portal Certificate Group tag association with the default self-signed certificate.

Step 4 Do one of the following:

Option	Description
Generate a CSR	When you generate the CSR: **a.** Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag. **b.** Send the CSR to a CA and obtain the signed certificate. **c.** Import the root and any other intermediate certificates of the CA that signed your certificate in to the Trusted Certificates store. **d.** Bind the CA-signed certificate with the CSR.
Import the private key and the CA-signed certificate	When you import the CA-signed certificate: **a.** Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag. **b.** Import the root and any other intermediate certificates of the CA that signed your certificate in to the Trusted Certificates store.
Edit an existing CA-signed certificate.	When you edit the existing CA-signed certificate: Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.

Step 5 Register the ISE node to the deployment.

The portal configuration in the deployment is configured to the "Default Portal Certificate Group" tag and the portals are configured to use the CA-signed certificate associated with the "Default Portal Certificate Group" tag on the new node.

User and Endpoint Certificate Renewal

By default, Cisco ISE rejects a request that comes from a device whose certificate has expired. However, you can change this default behavior and configure ISE to process such requests and prompt the user to renew the certificate.

If you choose to allow the user to renew the certificate, Cisco recommends that you configure an authorization policy rule which checks if the certificate has been renewed before processing the request any further. Processing a request from a device whose certificate has expired may pose a potential security threat. Hence, you must configure appropriate authorization profiles and rules to ensure that your organization's security is not compromised.

Some devices allow you to renew the certificates before and after their expiry. But on Windows devices, you can renew the certificates only before it expires. Apple iOS, Mac OSX, and Android devices allow you to renew the certificates before or after their expiry.

Dictionary Attributes Used in Policy Conditions for Certificate Renewal

Cisco ISE certificate dictionary contains the following attributes that are used in policy conditions to allow a user to renew the certificate:

- Days to Expiry: This attribute provides the number of days for which the certificate is valid. You can use this attribute to create a condition that can be used in authorization policy. This attribute can take a value from 0 to 15. A value of 0 indicates that the certificate has already expired. A value of 1 indicates that the certificate has less than 1 day before it expires.
- Is Expired: This Boolean attribute indicates whether a certificate has expired or not. If you want to allow certificate renewal only when the certificate is near expiry and not after it has expired, use this attribute in authorization policy condition.

Authorization Policy Condition for Certificate Renewal

You can use the CertRenewalRequired simple condition (available by default) in authorization policy to ensure that a certificate (expired or about to expire) is renewed before Cisco ISE processes the request further.

CWA Redirect to Renew Certificates

If a user certificate is revoked before its expiry, Cisco ISE checks the CRL published by the CA and rejects the authentication request. In case, if a revoked certificate has expired, the CA may not publish this certificate in its CRL. In this scenario, it is possible for Cisco ISE to renew a certificate that has been revoked. To avoid this, before you renew a certificate, ensure that the request gets redirected to Central Web Authentication (CWA) for a full authentication. You must create an authorization profile to redirect the user for CWA.

Configure Cisco ISE to Allow Users to Renew Certificates

You must complete the tasks listed in this procedure to configure Cisco ISE to allow users to renew certificates.

Before you begin

Configure a limited access ACL on the WLC to redirect a CWA request.

Procedure

Step 1 Update the Allowed Protocol Configuration, on page 86

Step 2 Create an Authorization Policy Profile for CWA Redirection, on page 86

Step 3 Create an Authorization Policy Rule to Renew Certificates, on page 87

Step 4 Enable BYOD Settings in the Guest Portal, on page 88

Update the Allowed Protocol Configuration

Procedure

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols** > **Default Network Access**.

Step 2 Check the **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy** check box under the EAP-TLS protocol and EAP-TLS inner methods for PEAP and EAP-FAST protocols.

Requests that use the EAP-TLS protocol will go through the NSP flow.

For PEAP and EAP-FAST protocols, you must manually configure Cisco AnyConnect for Cisco ISE to process the request.

Step 3 Click **Submit**.

What to do next

Create an Authorization Policy Profile for CWA Redirection, on page 86

Create an Authorization Policy Profile for CWA Redirection

Before you begin

Ensure that you have configured a limited access ACL on the WLC.

Procedure

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add**.

Step 3 Enter a name for the authorization profile. For example, CertRenewal_CWA.

Step 4 Check the **Web Redirection (CWA, DRW, MDM, NSP, CPP)** check box in the Common Tasks area.

Step 5 Choose **Centralized Web Auth** from the drop-down list and the limited access ACL.

Step 6 Check the **Display Certificates Renewal Message** check box.

The URL-redirect attribute value changes and includes the number of days for which the certificate is valid.

Step 7 Click **Submit**.

Note If you have configured the following Device Registration WebAuth (DRW) policies for wireless devices in Cisco ISE 1.2:

- DRW-Redirect policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-drw-redirect
- DRW-Allow policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-Permit

After upgrading to ISE 1.3 or above version, you must update the DRW-Allow policy condition as follows:

- Condition = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) and Profile = Wireless-Permit

What to do next

Create an Authorization Policy Rule to Renew Certificates, on page 87

Create an Authorization Policy Rule to Renew Certificates

Before you begin

Ensure that you have created an authorization profile for central web authentication redirection.

Enable Policy Sets on **Administration** > **System** > **Settings** > **Policy Settings**.

Procedure

Step 1 Choose **Work Centers** > **Device Administration** > **Policy Sets**.

Step 2 Click **Create Above**.

Step 3 Enter a name for the new rule.

Step 4 Choose the following simple condition and result:

If CertRenewalRequired EQUALS True, then choose the authorization profile that you created earlier (CertRenewal_CWA) for the permission.

Step 5 Click **Save**.

What to do next

When you access the corporate network with a device whose certificate has expired, click **Renew** to reconfigure your device.

Enable BYOD Settings in the Guest Portal

For a user to be able to renew a personal device certificate, you must enable the BYOD settings in the chosen guest portal.

Procedure

Step 1 Choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals**.

a) Select the chosen CWA portal and click **Edit**.

Step 2 From BYOD Settings, check the **Allow employees to use personal devices on the network** check box.

Step 3 Click **Save**.

Certificate Renewal Fails for Apple iOS Devices

When you use ISE to renew the endpoint certificates on Apple iOS devices, you might see a "Profiled Failed to Install" error message. This error message appears if the expiring or expired network profiles were signed by a different Admin HTTPS certificate than the one that is used in processing the renewal, either on the same Policy Service Node (PSN) or on another PSN.

As a workaround, use a multi-domain SSL certificate, which is commonly referred to as Unified Communications Certificate (UCC), or a wildcard certificate for Admin HTTPS on all PSNs in the deployment.

Check the Status of the Certificates (OCSP or CRL).

Cisco ISE checks the Certificate Revocation Lists (CRL) periodically. Using this page, you can configure Cisco ISE to check ongoing sessions against CRLs that are downloaded automatically. You can specify the time of the day when the OCSP or CRL checks should begin each day and the time interval in hours that Cisco ISE waits before checking the OCSP server or CRLs again.

The following table describes the fields in the Certificate Periodic Check Settings page, which you can use to specify the time interval for checking the status of certificates (OCSP or CRL). The navigation path for this page is: **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Periodic Check Settings**.

Table 12: Certificate Periodic Check Settings

Field Name	Usage Guidelines
Certificate Check Settings	
Check ongoing sessions against automatically retrieved CRL	Check this check box if you want Cisco ISE to check ongoing sessions against CRLs that are automatically downloaded.
CRL/OCSP Periodic Certificate Checks	

Field Name	Usage Guidelines
First check at	Specify the time of the day when the CRL or OCSP check should begin each day. Enter a value between 00:00 and 23:59 hours.
Check every	Specify the time interval in hours that Cisco ISE waits before checking the CRL or OCSP server again.

Related Topics

OCSP Services, on page 118
Add OCSP Client Profiles, on page 120

Cisco ISE CA Service

Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). The Cisco ISE Internal Certificate Authority (ISE CA) issues and manages digital certificates for endpoints from a centralized console to allow employees to use their personal devices on the company's network. A CA-signed digital certificate is considered industry standard and more secure. The Primary PAN is the Root CA. The Policy Service Nodes (PSNs) are subordinate CAs to the Primary PAN (SCEP RA). The ISE CA offers the following functionalities:

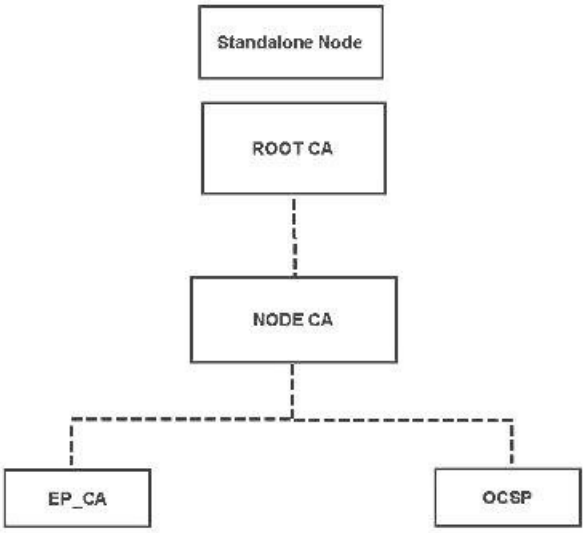
- Certificate Issuance: Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to your network.
- Key Management: Generates and securely stores keys and certificates on both PAN and PSN nodes.
- Certificate Storage: Stores certificates issued to users and devices.
- Online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

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

ISE CA Certificates Provisioned on Administration and Policy Service Nodes

After installation, a Cisco ISE node is provisioned with a Root CA certificate, and a Node CA certificate to manage certificates for endpoints.

Figure 2: ISE CA Certificates Provisioned on a Standalone Node

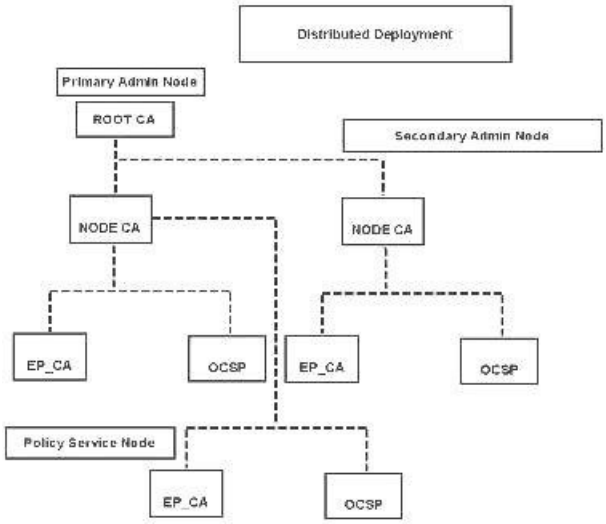


When you set up a deployment, the node that you designate as the Primary Administration Node (PAN) becomes the Root CA. The PAN has a Root CA certificate and a Node CA certificate that is signed by the Root CA.

When you register a Secondary Administration Node to the PAN, a Node CA certificate is generated and is signed by the Root CA on the Primary Administration Node.

Any Policy Service Node (PSN) that you register with the PAN is provisioned an Endpoint CA and an OCSP certificate signed by the Node CA of the PAN. The Policy Service Nodes (PSNs) are subordinate CAs to the PAN. When you use the ISE CA, the Endpoint CA on the PSN issues the certificates to the endpoints that access your network.

Figure 3: ISE CA Certificates Provisioned on Administration and Policy Service Nodes in a Deployment



ISE CA Chain Regeneration

When you regenerate the Cisco ISE CA chain, all the certificates including the Root CA, Node CA, and Endpoint CA certificates are regenerated. You must regenerate the ISE CA chain when you change the domain name or hostname of your PAN or PSN. When you upgrade from earlier releases to Release 2.0 or later, we recommend that you regenerate the ISE CA chain to move from the two root hierarchy to a single root hierarchy.

When you regenerate a system certificate, whether root CA or an intermediate CA certificate, ISE Messaging Service restarts to load the new certificate chain. Audit logs will be lost until the ISE Messaging Service is available again.

Note Whenever the Cisco ISE internal CA is replaced in a deployment, then the ISE messaging service must also be refreshed that time to retrieve the complete certificate chain.

Elliptical Curve Cryptography Certificates Support

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

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

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

Because of the smaller key size, encryption is quicker.

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

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

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

Cisco ISE CA service supports ECC certificates for devices connecting through the BYOD flow. You can also generate ECC certificates from the Certificate Provisioning Portal.

Note The following table lists the operating systems and versions that support ECC along with the supported curve types. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

Operating System	Supported Versions	Supported Curve Types
Windows	8 and later	P-256, P-384, and P-521
Android	4.4 and later **Note** Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Android 6.0, which does not support the P-192 curve type).

Windows 7 and Apple iOS do not natively support ECC for authentication over EAP-TLS. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the BYOD flow with Enrollment over Secure Transport (EST) protocol is not working properly, check the following:

- Certificate Services Endpoint Sub CA certificate chain is complete. To check whether the certificate chain is complete:
  1. Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.
  2. Check the check box next to the certificate that you want to check and click **View**.
- Ensure that the CA and EST services are up and running. If the services are not running, go to **Administration > System > Certificates > Certificate Authority > Internal CA Settings** to enable the CA service.
- If you have upgraded to Cisco ISE 2.x from an ISE version prior to 2.0, replace the ISE Root CA certificate chain after the upgrade. To do this:
  1. Choose **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.
  2. Click **Generate Certificate Signing Requests (CSR)**.
  3. Choose ISE Root CA from one or more Certificates **will be used for** drop-down list.
  4. Click **Replace ISE Root CA Certificate Chain**.

Note This release of Cisco ISE does not support EST clients to authenticate directly against the EST Server residing within Cisco ISE.

While on-boarding an Android or a Windows endpoint, ISE triggers an EST flow if the request is for an ECC-based certificate.

Cisco ISE Certificate Authority Certificates

The Certificate Authority (CA) Certificates page lists all the certificates related to the internal Cisco ISE CA. In previous releases, these CA certificates were present in the Trusted Certificates store and are now moved to the CA Certificates page. These certificates are listed node wise in this page. You can expand a node to view all the ISE CA certificates of that particular node. The Primary and Secondary Administration nodes have the root CA, node CA, subordinate CA, and OCSP responder certificates. The other nodes in the deployment have the endpoint subordinate CA and OCSP certificates.

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

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

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

Edit a Cisco ISE CA Certificate

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

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates.**.

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

Step 3 Modify the editable fields as required. See Edit Certificate Settings for a description of the fields.

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

Export a Cisco ISE CA Certificate

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

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**.

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

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

Import a Cisco ISE CA Certificate

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

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Export the ISE root CA, node CA, and endpoint sub CA certificates from the deployment where the endpoint certificate is signed and store it on the file system of the computer where your browser is running.

Procedure

Step 1 Log in to the Admin Portal of the deployment where the endpoint is getting authenticated.

Step 2 Choose**Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 3 Click **Import**.

Step 4 Configure the field values as necessary. See Trusted Certificate Import Settings for more information.

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

Certificate Templates

Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template.

Cisco ISE comes with the following default certificate templates for the ISE CA. You can create additional certificate templates, if needed. The default certificate templates are:

- CA_SERVICE_Certificate_Template—For other network services that use Cisco ISE as the Certificate Authority. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users. You can modify only the validity period in this certificate template.
- EAP_Authentication_Certificate_Template—For EAP authentication.
- pxGrid_Certificate_Template—For the pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

Certificate Template Name Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. This extension represents the certificate template that was used to create that endpoint certificate. The extension ID is 1.3.6.1.4.1.9.21.2.5. You can use the CERTIFICATE: Template Name attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.

Use Certificate Template Name in Authorization Policy Conditions

You can use the certificate template name extension in authorization policy rules.

Procedure

Step 1 Choose **Policy** > **Policy Sets**, and expand the Default policy set to view the authorization policy rules.

Step 2 Add a new rule or edit an existing rule. This example describes editing the Compliant_Device_Access rule:

a) Edit the Compliant_Device_Access rule.
b) Choose **Add Attribute/Value**.
c) From Dictionaries, choose the **CERTIFICATE: Template Name** attribute and **Equals** operator.
d) Enter the value of the certificate template name. For example, EAP_Authentication_Certificate_Template.

Step 3 Click **Save**.

Deploy Cisco ISE CA Certificates for pxGrid Controller

Cisco ISE CA provides a certificate template for the pxGrid controller to generate a certificate from the Certificate Provisioning Portal.

Before you begin

Generate a certificate signing request (CSR) for the pxGrid client and copy the contents of the CSR in to the clipboard.

Procedure

Step 1 Create a network access user account (Administration > Identity Management > Identities > Users > Add).

Make note of the user group to which the user is assigned.

Step 2 Edit the Certificate Provisioning Portal Settings (Administration > Device Portal Management > Certificate Provisioning).

a) Select the certificate provisioning portal and click **Edit**.
b) Click the **Portal Settings** drop-down list. From the Configure authorized groups Available list, select the user group to which the network access user belongs to and move it to Chosen list.
c) Click the **Certificate Provisioning Portal Settings** drop-down list. Choose the pxGrid_Certificate_Template. See the Portal Settings for Certificate Provisioning Portal section in *Cisco ISE Admin Guide: Guest and BYOD* for more information.
d) Save the portal settings.

Step 3 Launch the Certificate Provisioning Portal. Click the Portal Test URL link.

a) Log in to the Certificate Provisioning Portal using the user account created in step 1.
b) Accept the AUP and click **Continue**.
c) From the **I want to** drop-down list, choose **Generate a single certificate (with certificate signing request)**.
d) In the Certificate Signing Request Details field, paste the contents of the CSR from the clipboard.
e) From the **Certificate Download Format** drop-down list, choose **PKCS8 format**.

Note If you choose the PKCS12 format, you must convert the single certificate file in to separate certificate and key files. The certificate and key files must be in binary DER encoded or PEM format before you can import them in to Cisco ISE.

f) From the **Choose Certificate Template** drop-down list, choose **pxGrid_Certificate_Template**.
g) Enter a certificate password.
h) Click **Generate**.

The certificate is generated.

i) Export the certificate.

The certificate along with the certificate chain is exported.

Step 4 Import the Cisco ISE CA chain in to the Trusted Certificates store in the pxGrid client.

Simple Certificate Enrollment Protocol Profiles

To help enable certificate provisioning functions for the variety of mobile devices that users can register on the network, Cisco ISE enables you to configure one or more Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA) profiles (called as Cisco ISE External CA Settings) to point Cisco ISE to multiple CA locations. The benefit of allowing for multiple profiles is to help ensure high availability and perform load balancing across the CA locations that you specify. If a request to a particular SCEP CA goes unanswered three consecutive times, Cisco ISE declares that particular server unavailable and automatically moves to the CA with the next lowest known load and response times, then it begins periodic polling until the server comes back online.

For details on how to set up your Microsoft SCEP server to interoperate with Cisco ISE, see

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

Issued Certificates

The Admin portal lists all the certificates issued by the internal ISE CA to endpoints (Administration > System > Certificates > Endpoint Certificates). The Issued Certificates page provides you an at-a-glance view of the certificate status. You can mouse over the Status column to find out the reason for revocation if a certificate has been revoked. You can mouse over the Certificate Template column to view additional details such as Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), and Validity of the certificate. You can click on the endpoint certificate to view the certificate.

All certificates issued by the ISE CA (certificates automatically provisioned through the BYOD flow and certificates obtained from the Certificate Provisioning portal) are listed in the Endpoint Certificates page. You can manage these certificates from this page.

For example, if you want to view the certificates issued to user7, enter user7 in the text box that appears below the Friendly Name field. All the certificates issued by Cisco ISE to this user appear. Remove the search term from the text box to cancel the filter. You can also use the Advanced Filter option to view records based on various search criteria.

This Endpoint Certificates page also provides you the option to revoke an endpoint certificate, if necessary.

The Certificate Management Overview page displays the total number of endpoint certificates issued by each PSN node in your deployment. You can also view the total number of revoked certificates per node and the total number of certificates that have failed. You can filter the data on this page based on any of the attributes.

Issued and Revoked Certificates

The following table describes the fields on the Overview of Issued and Revoked Certificates page. The PSN nodes in your deployment issue certificates to endpoints. This page provides you information about the endpoint certificates issued by each of the PSN nodes in your deployment. The navigation path for this page is: **Administration** > **System** > **Certificates** > **Overview**.

Table 13: Issued and Revoked Certificates

Fields	Usage Guidelines
Node Name	Name of the Policy Service node (PSN) that issued the certificate.
Certificates Issued	Number of endpoint certificates issued by the PSN node.
Certificates Revoked	Number of revoked endpoint certificates (certificates that were issued by the PSN node).
Certificates Requests	Number of certificate-based authentication requests processed by the PSN node.
Certificates Failed	Number of failed authentication requests processed by the PSN node.

Related Topics

Issued Certificates, on page 96
User and Endpoint Certificate Renewal, on page 85
Configure Cisco ISE to Use Certificates for Authenticating Personal Devices, on page 101
Configure Cisco ISE to Allow Users to Renew Certificates, on page 85
Revoke an Endpoint Certificate, on page 118

Backup and Restore of Cisco ISE CA Certificates and Keys

You must back up the Cisco ISE CA certificates and keys securely to be able to restore them back on a Secondary Administration Node in case of a PAN failure and you want to promote the Secondary Administration Node to function as the root CA or intermediate CA of an external PKI. The Cisco ISE configuration backup does not include the CA certificates and keys. Instead, you should use the Command Line Interface (CLI) to export the CA certificates and keys to a repository and to import them. The **application configure ise** command now includes export and import options to backup and restore CA certificates and keys.

The following certificates from the Trusted Certificates Store are restored on the Secondary Administration Node:

- Cisco ISE Root CA certificate

- Cisco ISE Sub CA certificate
- Cisco ISE Endpoint RA certificate
- Cisco ISE OCSP Responder certificate

You must back up and restore Cisco ISE CA certificates and keys when you:

- Have a Secondary Administration Node in the deployment
- Replace the entire Cisco ISE CA root chain
- Configure Cisco ISE root CA to act as a subordinate CA of an external PKI
- Upgrade from Release 1.2 to a later release
- Restore data from a configuration backup. In this case, you must first regenerate the Cisco ISE CA root chain and then back up and restore the ISE CA certificates and keys.

Note Whenever the Cisco ISE internal CA is replaced in a deployment, then the ISE messaging service must also be refreshed that time to retrieve the complete certificate chain.

Export Cisco ISE CA Certificates and Keys

You must export the CA certificates and keys from the PAN to import them on the Secondary Administration Node. This option enables the Secondary Administration Node to issue and manage certificates for endpoints when the PAN is down and you promote the Secondary Administration Node to be the PAN.

Before you begin

Ensure that you have created a repository to store the CA certificates and keys.

Procedure

Step 1 Enter **application configure ise** command from the Cisco ISE CLI.

Step 2 Enter 7 to export the certificates and keys.

Step 3 Enter the repository name.

Step 4 Enter an encryption key.

A success message appears with the list of certificates that were exported, along with the subject, issuer, and serial number.

Example:

```
 The following 4 CA key pairs were exported to repository 'sftp' at
'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa
```

```
        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Import Cisco ISE CA Certificates and Keys

After you register the Secondary Administration Node, you must export the CA certificates and keys from the PAN and import them in to the Secondary Administration Node.

Procedure

Step 1 Enter **application configure ise** command from the Cisco ISE CLI.

Step 2 Enter 8 to import the CA certificates and keys.

Step 3 Enter the repository name.

Step 4 Enter the name of the file that you want to import. The file name should be in the format **ise_ca_key_pairs_of_<vm hostname>**.

Step 5 Enter the encryption key to decrypt the file.

A success message appears.

Example:

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

Generate Root CA and Subordinate CAs on the Primary PAN and PSN

When you set up the deployment, Cisco ISE generates a root CA on the Primary PAN and subordinate CA certificates on the Policy Service Nodes (PSNs) for the Cisco ISE CA service. However, when you change the domain name or the hostname of the Primary PAN or PSN, you must regenerate root CA on the Primary PAN and sub CAs on the PSNs respectively.

If you want to change the hostname on a PSN, instead of regenerating the root CA and subordinate CAs on the Primary PAN and PSNs respectively, you can deregister the PSN before changing the hostname, and register it back. A new subordinate certificate gets provisioned automatically on the PSN.

Procedure

Step 1 **Administration** > **System** > **Certificates** > **Certificate Signing Requests**

Step 2 Click **Generate Certificate Signing Requests (CSR)**.

Step 3 Choose ISE Root CA from the **Certificate(s) will be used for** drop-down list.

Step 4 Click **Replace ISE Root CA Certificate chain**.

The root CA and subordinate CA certificates get generated for all the nodes in your deployment.

What to do next

If you have a Secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and restore it on the Secondary PAN. This ensures that the Secondary PAN can function as the root CA in case of a Primary PAN failure and you promote the Secondary PAN to be the Primary PAN.

Configure Cisco ISE Root CA as Subordinate CA of an External PKI

If you want the root CA on the Primary PAN to act as a subordinate CA of an external PKI, generate an ISE intermediate CA certificate signing request, send it to the external CA, obtain the root and CA-signed certificates, import the root CA certificate in to the Trusted Certificates Store, and bind the CA-signed certificate to the CSR. In this case, the external CA is the root CA, the Primary PAN is a subordinate CA of the external CA, and the PSNs are subordinate CAs of the Primary PAN.

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Signing Requests**.

Step 2 Click **Generate Certificate Signing Requests (CSR)**.

Step 3 Choose ISE Intermediate CA from the **Certificate(s) will be used for** drop-down list.

Step 4 Click **Generate**.

Step 5 Export the CSR, send it to the external CA, and obtain the CA-signed certificate.

Step 6 Import the root CA certificate from the external CA in to the Trusted Certificates store.

Step 7 Bind the CA-signed certificate with the CSR.

What to do next

If you have a Secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and restore it on the Secondary PAN. This ensures that the Secondary PAN can function as subordinate CA of the external PKI in case of a Primary PAN failure and you promote the Secondary PAN to be the Primary PAN.

Configure Cisco ISE to Use Certificates for Authenticating Personal Devices

You can configure Cisco ISE to issue and manage certificates for endpoints (personal devices) that connect to your network. You can use the internal Cisco ISE Certificate Authority (CA) service to sign the certificate signing request (CSR) from endpoints or forward the CSR to an external CA.

Before you begin

- Obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and store them in a secure location for disaster recovery purposes.
- If you have a Secondary PAN in the deployment, back up the Cisco ISE CA certificates and keys from the Primary PAN and restore them on the Secondary PAN.

Procedure

Step 1 Add Users to the Employee User Group, on page 102

You can add users to the internal identity store or to an external identity store such as Active Directory.

Step 2 Create a Certificate Authentication Profile for TLS-Based Authentication, on page 102

Step 3 Create an Identity Source Sequence for TLS-Based Authentication, on page 103

Step 4 Creating a client provisioning policy.

a) Configure Certificate Authority Settings, on page 103
b) Create a CA Template, on page 104
c) Create a Native Supplicant Profile to be Used in Client Provisioning Policy, on page 106
d) Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems, on page 107
e) Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices, on page 108

Step 5 Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 108

Step 6 Configure authorization policy rules for TLS-based authentications.

a) Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows, on page 109
b) Create Authorization Policy Rules, on page 110

When you use ECDHE-RSA based certificates, while connecting to the wireless SSID from your personal device, you will be prompted to enter the password a second time.

Add Users to the Employee User Group

The following procedure describes how to add users to the Employee user group in the Cisco ISE identity store. If you are using an external identity store, make sure that you have an Employee user group to which you can add users.

Procedure

Step 1 Choose **Administration** > **Identity Management** > **Identities** > **Users**.

Step 2 Click **Add**.

Step 3 Enter the user details.

Step 4 In the **Passwords** section, choose the **Login Password** and TACACS+ **Enable Password** to set the access level to a network device.

Step 5 Select Employee from the User Group drop-down list.

All users who belong to the Employee user group share the same set of privileges.

Step 6 Click **Submit**.

What to do next

Create a Certificate Authentication Profile for TLS-Based Authentication, on page 102

Create a Certificate Authentication Profile for TLS-Based Authentication

To use certificates for authenticating endpoints that connect to your network, you must define a certificate authentication profile in Cisco ISE or edit the default Preloaded_Certificate_Profile. The certificate authentication profile includes the certificate field that should be used as the principal username. For example, if the username is in the Common Name field, then you can define a certificate authentication profile with the Principal Username being the Subject - Common Name, which can be verified against the identity store.

Procedure

Step 1 Choose **Administration** > **Identity Management** > **External Identity Sources** > **Certificate Authentication Profile**.

Step 2 Enter a name for your certificate authentication profile. For example, CAP.

Step 3 Choose Subject - Common Name as the **Principal Username X509 Attribute**.

Step 4 Click **Save**.

What to do next

Create an Identity Source Sequence for TLS-Based Authentication, on page 103

Create an Identity Source Sequence for TLS-Based Authentication

After you create a certificate authentication profile, you must add it to the identity source sequence so that Cisco ISE can obtain the attribute from the certificate and match it against the identity sources that you have defined in the identity source sequence.

Before you begin

Ensure that you have completed the following tasks:

- Add users to the Employee user group.
- Create a certificate authentication profile for certificate-based authentication.

Procedure

Step 1 Choose **Administration** > **Identity Management** > **Identity Source Sequences**.

Step 2 Click **Add**.

Step 3 Enter a name for the identity source sequence. For example, Dot1X.

Step 4 Check the **Select Certificate Authentication Profile** check box and select the certificate authentication profile that you created earlier, namely CAP.

Step 5 Move the identity source that contains your user information to the **Selected** list box in the Authentication Search List area.

You can add additional identity sources and Cisco ISE searches these data stores sequentially until a match is found.

Step 6 Click the **Treat as if the user was not found and proceed to the next store in the sequence** radio button.

Step 7 Click **Submit**.

What to do next

Configure Certificate Authority Settings, on page 103

Configure Certificate Authority Settings

You must configure the external CA settings if you are going to use an external CA for signing the CSRs. The external CA settings was known as the SCEP RA profile in previous releases of Cisco ISE. If you are using the Cisco ISE CA, then you do not have to explicitly configure the CA settings. You can review the Internal CA settings at Administration > System > Certificates > Internal CA Settings.

Once users' devices receive their validated certificate, they reside on the device as described in the following table.

Table 14: Device Certificate Location

Device	Certificate Storage Location	Access Method
iPhone/iPad	Standard certificate store	Settings > General > Profile

Device	Certificate Storage Location	Access Method
Android	Encrypted certificate store	Invisible to end users. **Note** Certificates can be removed using Settings > Location & Security > Clear Storage.
Windows	Standard certificate store	Launch mmc.exe from the **/cmd** prompt or view in the certificate snap-in.
Mac	Standard certificate store	Application > Utilities > Keychain Access

Before you begin

If you are going to use an external Certificate Authority (CA) for signing the certificate signing request (CSR), then you must have the URL of the external CA.

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **External CA Settings**.

Step 2 Click **Add**.

Step 3 Enter a name for the external CA setting. For example, EXTERNAL_SCEP.

Step 4 Enter the external CA server URL in the URL text box.

Click **Test Connection** to check if the external CA is reachable. Click the + button to enter additional CA server URLs.

Step 5 Click **Submit**.

What to do next

Create a CA Template, on page 104

Create a CA Template

The certificate template defines the SCEP RA profile that must be used (for the internal or external CA), Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), validity period of the certificate, and the Extended Key Usage. This example assumes that you are going to use the internal Cisco ISE CA. For an external CA template, the validity period is determined by the external CA and you cannot specify it.

You can create a new CA template or edit the default certificate template, EAP_Authentication_Certificate_Template.

By default, the following CA templates are available in Cisco ISE:

- CA_SERVICE_Certificate_Template—For other network services that use the ISE CA. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users.

- EAP_Authentication_Certificate_Template—For EAP authentication.
- pxGrid_Certificate_Template—For pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

Note Certificate templates that use the ECC key type can be used only with the internal Cisco ISE CA.

Before you begin

Ensure that you have configured the CA settings.

Procedure

Step 1 Choose **Administration** > **System** > **CA Service** > **Internal CA Certificate Template**.

Step 2 Enter a name for the internal CA template. For example, Internal_CA_Template.

Step 3 (Optional) Enter values for the Organizational Unit, Organization, City, State, and Country fields.

We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template.

The username of the internal user generating the certificate is used as the Common Name of the certificate. Cisco ISE Internal CA does not support "+" or "*" characters in the Common Name field. Ensure that your username does not include "+" or "*" special characters.

Step 4 Specify the Subject Alternative Name (SAN) and the validity period of the certificate.

Step 5 Specify a Key Type. Choose RSA or ECC.

The following table lists the operating systems and versions that support ECC along with the curve types that are supported. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

Operating System	Supported Versions	Supported Curve Types
Windows	8 and later	P-256, P-384, and P-521
Android	4.4 and later **Note** Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Android 6.0, which does not support the P-192 curve type).

Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the devices in your network run an operating system that is not supported (Windows 7, MAC OS X, or Apple iOS, we recommend that you choose RSA as the Key Type.

Step 6 (Applicable if you choose the RSA Key Type) Specify a key size. You must choose 1024 or a higher key size.

Step 7 (Applicable only if you choose the ECC Key Type) Specify the Curve Type. The default is P-384.

Step 8 Choose ISE Internal CA as the SCEP RA Profile.

Step 9 Enter the validity period in days. The default is 730 days. Valid range is between 1 and 730.

Step 10 Specify the Extended Key Usage. Check the **Client Authentication** check box if you want the certificate to be used for client authentication. Check the **Server Authentication** check box if you want the certificate to be used for server authentication.

Step 11 Click **Submit**.

The internal CA certificate template is created and will be used by the client provisioning policy.

What to do next

Create a Native Supplicant Profile to be Used in Client Provisioning Policy, on page 106

Internal CA Settings

The following table describes the fields in the internal CA settings page. You can view the internal CA settings and disable the internal CA service from this page. The navigation path for this page is: **Administration** > **System** > **Certificates** > **Internal CA Settings**.

Table 15: Internal CA Settings

Field Name	Usage Guidelines
Disable Certificate Authority	Click this button to disable the internal CA service.
Host Name	Host name of the Cisco ISE node that is running the CA service.
Personas	Cisco ISE node personas that are enabled on the node running the CA service. For example, Administration, Policy Service, etc.
Role(s)	The role(s) assumed by the Cisco ISE node running the CA service. For example, Standalone or Primary or Secondary.
CA, EST & OCSP Responder Status	Enabled or disabled
OCSP Responder URL	URL for Cisco ISE node to access the OCSP server.
SCEP URL	URL for the Cisco ISE node to access the SCEP server.

Related Topics

Cisco ISE CA Service, on page 89
Configure Cisco ISE to Use Certificates for Authenticating Personal Devices, on page 101

Create a Native Supplicant Profile to be Used in Client Provisioning Policy

You can create native supplicant profiles to enable users to bring personal devices to your Corporate network. Cisco ISE uses different policy rules for different operating systems. Each client provisioning policy rule contains a native supplicant profile, which specifies which provisioning wizard is to be used for which operating system.

Before you begin

- Configure the CA certificate template in Cisco ISE.
- Open up TCP port 8905 and UDP port 8905 to enable client agents and supplicant provisioning wizard installation. For more information about port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

Procedure

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Native Supplicant Profile**.

Step 3 Enter a name for the native supplicant profile. For example, EAP_TLS_INTERNAL.

Step 4 Choose ALL from the **Operating System** drop-down list.

Note The MAC OS version 10.10 user should manually connect to the provisioned SSID for dual-SSID PEAP flow.

Step 5 Check the **Wired** or **Wireless** check box.

Step 6 Choose TLS from the **Allowed Protocol** drop-down list.

Step 7 Choose the CA certificate template that you created earlier.

Step 8 Click **Submit**.

What to do next

Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems, on page 107

Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems

For Windows and MAC OS X operating systems, you must download the remote resources from the Cisco site.

Before you begin

Ensure that you are able to access the appropriate remote location to download client provisioning resources to Cisco ISE, by verifying that the proxy settings for your network are correctly configured.

Procedure

Step 1 Choose **Policy** > **Policy Elements** > **Resources** > **Client Provisioning** > **Resources**.

Step 2 Choose **Add** > **Agent resources from Cisco site**.

Step 3 Check the check boxes next to the **Windows** and **MAC OS X** packages. Be sure to include the latest versions.

Step 4 Click **Save**.

What to do next

Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices, on page 108

Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices

Client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

To enable employees to bring iOS, Android, MACOSX devices, you must create policy rules for each of these devices on the Client Provisioning Policy page.

Before you begin

You must have configured the required native supplicant profiles and downloaded the required agents from the Client Provisioning Policy pages.

Procedure

Step 1 Choose **Policy** > **Client Provisioning**.

Step 2 Create client provisioning policy rules for Apple iOS, Android, and MACOSX devices.

Step 3 Click **Save**.

What to do next

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 108

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication

This task shows how to update the Dot1X authentication policy rule for TLS-based authentications.

Before you begin

Ensure that you have the certificate authentication profile created for TLS-based authentication.

Procedure

Step 1 Choose **Policy** > **Policy Sets**.

Step 2 Click the arrow icon › from the **View** column to open the Set view screen and view, manage, and update the authentication policy.

The default rule-based authentication policy includes a rule for Dot1X authentication.

Step 3 To edit the conditions for the Dot1X authentication policy rule, hover over the cell in the **Conditions** column and click  . The Conditions Studio opens.

Step 4 From the **Actions** column in the Dot1X policy rule, click the cog icon and then from the drop-down menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Policy Sets table.

Step 5 Enter a name for the rule. For example, eap-tls.

Step 6 From the **Conditions** column, click the (+) symbol.

Step 7 Create the required conditions in the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Network Access:UserName Equals User1).

You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 8 Click **Use**.

Step 9 Leave the default rule as is.

Step 10 Click **Save**.

What to do next

Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows, on page 109

Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows

You must define authorization profiles to determine the access that must be granted to the user after the certificate-based authentication is successful.

Before you begin

Ensure that you have configured the required access control lists (ACLs) on the wireless LAN controller (WLC). Refer to the *TrustSec How-To Guide: Using Certificates for Differentiated Access* for information on how to create the ACLs on the WLC.

This example assumes that you have created the following ACLs on the WLC.

- NSP-ACL - For native supplicant provisioning
- BLACKHOLE - For restricting access to blacklisted devices
- NSP-ACL-Google - For provisioning Android devices

Procedure

Step 1 Choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add** to create a new authorization profile.

Step 3 Enter a name for the authorization profile.

Step 4 From the **Access Type** drop-down list, choose ACCESS_ACCEPT.

Step 5 Click **Add** to add the authorization profiles for central web authentication, central web authentication for Google Play, native supplicant provisioning, and native supplicant provisioning for Google.

Step 6 Click **Save**.

What to do next

Create Authorization Policy Rules, on page 110

Create Authorization Policy Rules

Cisco ISE evaluates the authorization policy rules and grants the user access to the network resources based on the authorization profile specified in the policy rule.

Before you begin

Ensure that you have created the required authorization profiles.

Procedure

Step 1 Choose **Policy** > **Policy Sets**, and expand the policy set to view the authorization policy rules.

Step 2 Insert additional policy rules above the default rule.

Step 3 Click **Save**.

CA Service Policy Reference

This section provides reference information for the authorization and client provisioning policy rules that you must create before you can enable the Cisco ISE CA service.

Client Provisioning Policy Rules for Certificate Services

This section lists the client provisioning policy rules that you must create while using the Cisco ISE certificate services. The following table provides the details.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
iOS	Any	Apple iOS All	Condition(s)	EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
Android	Any	Android	Condition(s)	EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.
MACOSX	Any	MACOSX	Condition(s)	Under the Native Supplicant Configuration, specify the following: 1. Config Wizard: Select the MACOSX supplicant wizard that you downloaded from the Cisco site. 2. Wizard Profile: Choose the EAP_TLS_INTERNAL native supplicant profile that you created earlier. If you are using an external CA, select the native supplicant profile that you have created for the external CA.

Authorization Profiles for Certificate Services

This section lists the authorization profiles that you must create for enabling certificate-based authentication in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC).

- CWA - This profile is for devices that go through the central web authentication flow. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL in the ACL text box.

- CWA_GooglePlay - This profile is for Android devices that go through the central web authentication flow. This profile enables Android devices to access Google Play Store and download the Cisco Network Setup Assistant. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL-Google in the ACL text box.
- NSP - This profile is for non-Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL in the ACL text box.
- NSP-Google - This profile is for Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL-Google in the ACL text box.

Review the default Blackhole_Wireless_Access authorization profile. The Advanced Attributes Settings should be:

- Cisco:cisco-av-pair = url-redirect=https://*ip*:*port*/blacklistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

Authorization Policy Rules for Certificate Services

This section lists the authorization policy rules that you must create while enabling the Cisco ISE CA service.

- Corporate Assets-This rule is for corporate devices that connect to the corporate wireless SSID using 802.1X and MSCHAPV2 protocol.
- Android_SingleSSID-This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to single SSID setup.
- Android_DualSSID-This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to dual SSID setup.
- CWA-This rule is for devices that go through the central web authentication flow.
- NSP-This rule is for devices that go through the native supplicant provisioning flow using a certificate for EAP-TLS authentication.
- EAP-TLS-This rule is for devices that have completed the supplicant provisioning flow and are provisioned with a certificate. They will be given access to the network.

The following table lists the attributes and values that you must choose while configuring authorization policy rules for the Cisco ISE CA service. This example assumes that you have the corresponding authorization profiles configured in Cisco ISE as well.

Rule Name	Conditions	Permissions (authorization profiles to be applied)
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google

Rule Name	Conditions	Permissions (authorization profiles to be applied)
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is http://<*IP Address or FQDN of ISE CA server*>:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

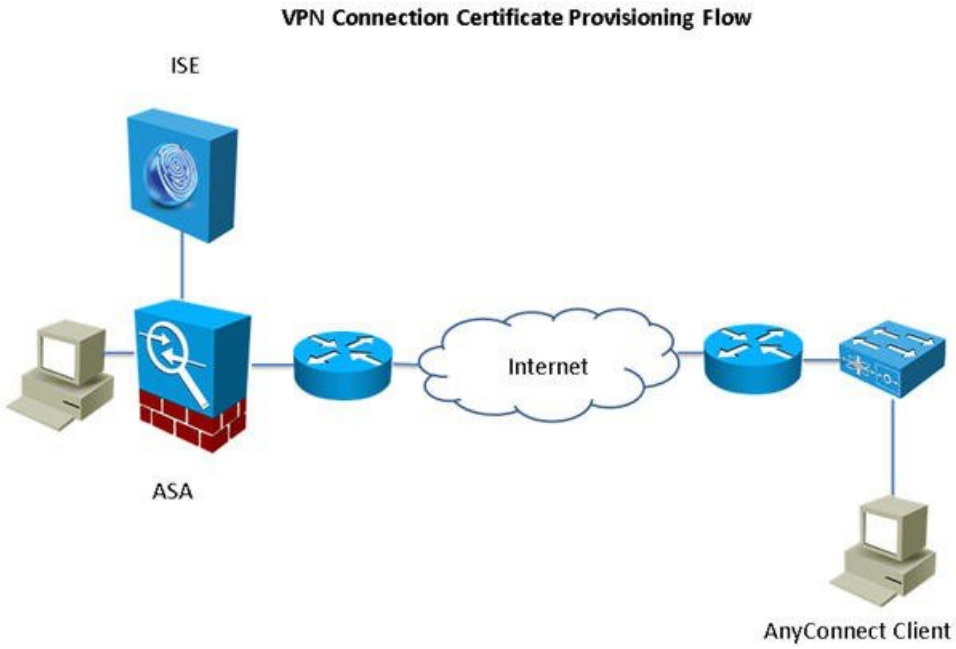
You can configure certificate renewal before expiration in the AnyConnect Client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

Supported versions include:

- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

VPN Connection Certificate Provisioning Flow

Figure 4: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.
2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA.
3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate.
4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE).
   a. If authentication fails, the connection is terminated immediately.
   b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to “true” and apply ACLs and web ACLs.
5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established.
6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP.
7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment.
8. ASA relays the response from ISE CA back to the client.
9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session.

10. The user can again authenticate using the certificate and a normal VPN connection is established.

Configure Cisco ISE CA to Issue Certificates to ASA VPN Users

You must perform the following configurations on Cisco ISE and ASA to provision certificates to ASA VPN users.

Before you begin

- Ensure that the VPN user account is present in Cisco ISE internal or external identity source.
- Ensure that the ASA and the Cisco ISE Policy Service Nodes are synchronized using the same NTP server.

Procedure

Step 1 Define the ASA as a network access device in Cisco ISE. See Add a Network Device in Cisco ISE, on page 115 for information on how to add ASA as a network device.

Step 2 Configure Group Policy in ASA, on page 116.

Step 3 Configure AnyConnect Connection Profile for SCEP Enrollment, on page 116.

Step 4 Configure a VPN Client Profile in ASDM, on page 117.

Step 5 Import Cisco ISE CA Certificates into ASA.

Add a Network Device in Cisco ISE

You can add a network device in Cisco ISE or use the default network device.

You can also add the network device in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** page.

Before you begin

Make sure that the AAA function is enabled on the network devices. To know more, see the section “Command to Enable AAA Functions” in book “Integrations” in the *ISE Admin Guide* .

Procedure

Step 1 Choose **Administration** > **Network Resources** > **Network Devices**.

Step 2 Click **Add**.

Step 3 Enter the **Name** of the network device.

Step 4 Enter the **IP address**.

Step 5 (Optional) Check the **RADIUS Authentication Settings** check box to configure the RADIUS protocol for authentication.

Step 6 (Optional) Check the **TACACS Authentication Settings** check box to configure the TACACS protocol for authentication.

Step 7 (Optional) Check the **SNMP Settings** check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.

Step 8 (Optional) Check the **Advanced Trustsec Settings** check box to configure a Trustsec-enabled device.

Step 9 Click **Submit**.

Configure Group Policy in ASA

Configure a group policy in ASA to define the ISE CA URL for AnyConnect to forward the SCEP enrollment request.

Procedure

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, click **Group Policies**.

Step 3 Click **Add** to create a group policy.

Step 4 Enter a name for the group policy. For example, ISE_CA_SCEP.

Step 5 In the SCEP forwarding URL field, uncheck the **Inherit** check box and enter the ISE SCEP URL with port number.

If you are using the FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN of the ISE node.

Example:

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

Step 6 Click **OK** to save the group policy.

Configure AnyConnect Connection Profile for SCEP Enrollment

Configure an AnyConnect connection profile in ASA to specify the ISE CA server, authentication method, and ISE CA SCEP URL.

Procedure

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, click **AnyConnect Connection Profiles**.

Step 3 Click **Add** to create a connection profile.

Step 4 Enter a name for the connection profile. For example, Cert-Group.

Step 5 (Optional) Enter a description for the connection profile in the Aliases field. For example, SCEP-Call-ASA.

Step 6 In the Authentication area, specify the following:

- Method—Click the **Both** radio button
- AAA Server Group—Click **Manage** and choose your ISE server

Step 7 In the Client Address Assignment area, select the DHCP server and client address pools to use.

Step 8 In the Default Group Policy area, click **Manage** and select the Group Policy that you have created with the ISE SCEP URL and port number.

Example:

For example, ISE_CA_SCEP.

Step 9 Choose **Advanced** > **General** and check the **Enable Simple Certificate Enrollment Protocol** check box for this connection profile.

Step 10 Click **OK**.
Your AnyConnect connection profile is created.

What to do next

Configure a VPN Client Profile in ASDM

Configure a VPN client profile in AnyConnect for SCEP enrollment.

Procedure

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, click **AnyConnect Client Profile**.

Step 3 Select the client profile that you want to use and click **Edit**.

Step 4 Click **Certificate Enrollment** from the Profile navigation pane on the left.

Step 5 Check the **Certificate Enrollment** check box.

Step 6 Enter the values in the following fields:

- Certificate Expiration Threshold—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported when SCEP is enabled). The default is zero (no warning displayed). The range of values is zero to 180 days.
- Automatic SCEP Host—Enter the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name Cert_Group.
- CA URL—Identifies the SCEP CA server. Enter the FQDN or IP Address of the ISE server. For example, http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

Step 7 Enter values for the Certificate Contents that define how the client requests the contents of the certificate.

Step 8 Click **OK**.
The AnyConnect client profile is created. Refer to the Cisco AnyConnect Secure Mobility Client for your version of AnyConnect for additional information.

Import Cisco ISE CA Certificates into ASA

Import the Cisco ISE internal CA certificates into the ASA.

Before you begin

Export the Cisco ISE internal CA certificates. Go to **Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**. Check the check boxes next to **Certificate Services Node CA** and **Certificate Services Root CA** certificates and export them, one certificate at a time.

Procedure

Step 1 Log in to Cisco ASA ASDM.

Step 2 From the Remote Access VPN navigation pane on the left, choose **Certificate Management** > **CA Certificates**.

Step 3 Click **Add** and select the Cisco ISE internal CA certificates to import them in to ASA.

Revoke an Endpoint Certificate

If you need to revoke a certificate issued to an employee's personal device, you can revoke it from the Endpoint Certificates page. For example, if an employee's device has been stolen or lost, you can log in to the Cisco ISE Admin portal and revoke the certificate issued to that device from the Endpoint Certificates page. You can filter the data on this page based on the Friendly Name, Device Unique Id, or Serial Number.

If a PSN (sub CA) is compromised, you can revoke all certificates issued by that PSN by filtering on the Issued By field from the Endpoint Certificates page.

When you revoke a certificate issued to an employee, if there is an active session (authenticated using that certificate), the session is terminated immediately. Revoking a certificate ensures that unauthorized users do not have any access to resources as soon as the certificate is revoked.

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.

Step 2 Check the check box next to the endpoint certificate that you want to revoke and click **Revoke**.

You can search for the certificate based on the Friendly Name and Device Type.

Step 3 Enter the reason for revoking the certificate.

Step 4 Click **Yes**.

OCSP Services

The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the Certificate Revocation List (CRL) and addresses issues that result in handling CRLs.

Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications. The OCSP configuration is configured in a reusable configuration object that can be referenced from any certificate authority (CA) certificate that is configured in Cisco ISE.

You can configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP. If a communication problem is detected with both the primary and secondary OCSP servers, or if an unknown status is returned for a given certificate, Cisco ISE switches to checking the CRL.

Cisco ISE CA Service Online Certificate Status Protocol Responder

The Cisco ISE CA OCSP responder is a server that communicates with OCSP clients. The OCSP clients for the Cisco ISE CA include the internal Cisco ISE OCSP client and OCSP clients on the Adaptive Security Appliance (ASA). The OCSP clients should communicate with the OCSP responder using the OCSP request/response structure defined in RFC 2560, 5019.

The Cisco ISE CA issues a certificate to the OCSP responder. The OCSP responder listens on port 2560 for any incoming requests. This port is configured to allow only OCSP traffic.

The OCSP responder accepts a request that follows the structure defined in RFC 2560, 5019. Nonce extension is supported in the OCSP request. The OCSP responder obtains the status of the certificate and creates an OCSP response and signs it. The OCSP response is not cached on the OCSP responder, although you can cache the OCSP response on the client for a maximum period of 24 hours. The OCSP client should validate the signature in the OCSP response.

The self-signed CA certificate (or the intermediate CA certificate if ISE acts as an intermediate CA of an external CA) on the PAN issues the OCSP responder certificate. This CA certificate on the PAN issues the OCSP certificates on the PAN and PSNs. This self-signed CA certificate is also the root certificate for the entire deployment. All the OCSP certificates across the deployment are placed in the Trusted Certificates Store for ISE to validate any response signed using these certificates.

OCSP Certificate Status Values

OCSP services return the following values for a given certificate request:

- Good—Indicates a positive response to the status inquiry. It means that the certificate is not revoked, and the state is good only until the next time interval (time to live) value.
- Revoked—The certificate was revoked.
- Unknown—The certificate status is unknown. OCSP service returns this value if the certificate was not issued by the CA of this OCSP responder.
- Error—No response was received for the OCSP request.

OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, and they are called primary and secondary OCSP servers. Each OCSP server configuration contains the following parameters:

- URL—The OCSP server URL.
- Nonce—A random number that is sent in the request. This option ensures that old communications cannot be reused in replay attacks.
- Validate response—Cisco ISE validates the response signature that is received from the OCSP server.

In case of timeout (which is 5 seconds), when Cisco ISE communicates with the primary OCSP server, it switches to the secondary OCSP server.

Cisco ISE uses the secondary OCSP server for a configurable amount of time before attempting to use the primary server again.

OCSP Failures

The three general OCSP failure scenarios are as follows:

- Failed OCSP cache or OCSP client side (Cisco ISE) failures.
- Failed OCSP responder scenarios, for example:

  The first primary OCSP responder not responding, and the secondary OCSP responder responding to the Cisco ISE OCSP request.

  Errors or responses not received from Cisco ISE OCSP requests.

  An OCSP responder may not provide a response to the Cisco ISE OCSP request or it may return an OCSP Response Status as not successful. OCSP Response Status values can be as follows:

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

    There are many date-time checks, signature validity checks and so on, in the OCSP request. For more details, refer to *RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* which describes all the possible states, including the error states.

- Failed OCSP reports

Add OCSP Client Profiles

You can use the OCSP Client Profile page to add new OCSP client profiles to Cisco ISE.

Before you begin

If the Certificate Authority (CA) is running the OCSP service on a nonstandard port (other than 80 or 443), you must configure ACLs on the switch to allow for communication between Cisco ISE and the CA on that port. For example:

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP port number*>

Procedure

Step 1 Choose **Administration** > **System** > **Certificates** > **Certificate Management** > **OCSP Client Profile**.

Step 2 Enter the values to add an OCSP Client Profile.

Step 3 Click **Submit**.

OCSP Client Profile Settings

The following table describes the fields on the OCSP Client Profile page, which you can use to configure OCSP client profiles. The navigation path for this page is **Administration** > **Certificates** > **Certificate Management** > **OCSP Client Profile**.

Table 16: OCSP Client Profile Settings

Field Name	Usage Guidelines
Name	Name of the OCSP Client Profile.
Description	Enter an optional description.
Configure OCSP Responder	
Enable Secondary Server	Check this check box to enable a secondary OCSP server for high availability.
Always Access Primary Server First	Use this option to check the primary server before trying to move to the secondary server. Even if the primary was checked earlier and found to be unresponsive, Cisco ISE will try to send a request to the primary server before moving to the secondary server.
Fallback to Primary Server After Interval *n* Minutes	Use this option when you want Cisco ISE to move to the secondary server and then fall back to the primary server again. In this case, all other requests are skipped, and the secondary server is used for the amount of time that is configured in the text box. The allowed time range is 1 to 999 minutes.
Primary and Secondary Servers	
URL	Enter the URL of the primary and/or secondary OCSP server.
Enable Nonce Extension Support	You can configure a nonce to be sent as part of the OCSP request. The Nonce includes a pseudo-random number in the OCSP request. It is verified that the number that is received in the response is the same as the number that is included in the request. This option ensures that old communications cannot be reused in replay attacks.

Field Name	Usage Guidelines
Validate Response Signature	The OCSP responder signs the response with one of the following certificates: • The CA certificate • A certificate different from the CA certificate In order for Cisco ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different certificates. This is true as long as OCSP sends the certificate that signed the response for Cisco ISE to validate it. If OCSP signs the response with a different certificate that is not configured in Cisco ISE, the response verification will fail.
Use OCSP URLs specified in Authority Information Access (AIA)	Click the radio button to use the OCSP URLs specified in the Authority Information Access extension.
Response Cache	
Cache Entry Time To Live *n* Minutes	Enter the time in minutes after which the cache entry expires. Each response from the OCSP server holds a nextUpdate value. This value shows when the status of the certificate will be updated next on the server. When the OCSP response is cached, the two values (one from the configuration and another from response) are compared, and the response is cached for the period of time that is the lowest value of these two. If the nextUpdate value is 0, the response is not cached at all. Cisco ISE will cache OCSP responses for the configured time. The cache is not replicated or persistent, so when Cisco ISE restarts, the cache is cleared. The OCSP cache is used in order to maintain the OCSP responses and for the following reasons: • To reduce network traffic and load from the OCSP servers on an already-known certificate • To increase the performance of Cisco ISE by caching already-known certificate statuses By default, the cache is set to 2 minutes for the internal CA OCSP client profile. If an endpoint authenticates a second time within 2 minutes of the first authentication, the OCSP cache is used and the OCSP responder is not queried. If the endpoint certificate has been revoked within the cache period, the previous OCSP status of Good will be used and the authentication succeeds. Setting the cache to 0 minutes prevents any responses from being cached. This option improves security, but decreases authentication performance.

Field Name	Usage Guidelines
Clear Cache	Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service. In a deployment, **Clear Cache** interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment.

Related Topics

OCSP Services, on page 118
Cisco ISE CA Service Online Certificate Status Protocol Responder, on page 119
OCSP Certificate Status Values, on page 119
OCSP High Availability, on page 119
OCSP Failures, on page 120
OCSP Statistics Counters, on page 123
Add OCSP Client Profiles, on page 120

OCSP Statistics Counters

Cisco ISE uses OCSP counters to log and monitor the data and health of the OCSP servers. Logging occurs every five minutes. Cisco ISE sends a syslog message to the Monitoring node and it is preserved in the local store. The local store contains data from the previous five minutes. After Cisco ISE sends the syslog message, the counters are recalculated for the next interval. This means, after five minutes, a new five-minute window interval starts again.

The following table lists the OCSP syslog messages and their descriptions.

Table 17: OCSP Syslog Messages

Message	Description
OCSPPrimaryNotResponsiveCount	The number of nonresponsive primary requests
OCSPSecondaryNotResponsiveCount	The number of nonresponsive secondary requests
OCSPPrimaryCertsGoodCount	The number of ‘good’ certificates that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsGoodCount	The number of ‘good’ statuses that are returned for a given CA using the primary OCSP server
OCSPPrimaryCertsRevokedCount	The number of ‘revoked’ statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsRevokedCount	The number of ‘revoked’ statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsUnknownCount	The number of ‘Unknown’ statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsUnknownCount	The number of ‘Unknown’ statuses that are returned for a given CA using the secondary OCSP server

Message	Description
OCSPPrimaryCertsFoundCount	The number of certificates that were found in cache from a primary origin
OCSPSecondaryCertsFoundCount	The number of certificates that were found in cache from a secondary origin
ClearCacheInvokedCount	How many times clear cache was triggered since the interval
OCSPCertsCleanedUpCount	How many cached entries were cleaned since the t interval
NumOfCertsFoundInCache	Number of the fulfilled requests from the cache
OCSPCacheCertsCount	Number of certificates that were found in the OCSP cache

Configure Admin Access Policies

An Admin Access (RBAC) policy is represented in an if-then format, where if is the RBAC Admin Group value and then is the RBAC Permissions value.

The RBAC policies page (**Administration > System > Admin Access > Authorization >RBAC Policy**) contains a list of default policies. You cannot edit or delete these default policies. However, you can edit the data access permissions for the Read-Only Admin policy. The RBAC policies page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

When you assign limited menu access, make sure that the data access permissions allow the administrator to access the data that is required to use the specified menus. For example, if you give menu access to the MyDevices portal, but don't allow data access to Endpoint Identity Groups, then that administrator cannot modify the portal.

Note Admin users can move endpoint MAC addresses from the Endpoint Identity Groups they have read-only access to, to the Endpoint Identity Groups they have full access to. The other way around is not possible.

Before you begin

- Ensure that you have created all admin groups for which you want to define the RBAC policies.
- Ensure that these admin groups are mapped to the individual admin users.
- Ensure that you have configured the RBAC permissions, such as menu access and data access permissions.

Procedure

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authorization** > **RBAC Policy**.

The RBAC Policies page contains a set of ready-to-use predefined policies for default admin groups. You cannot edit or delete these default policies. However, you can edit the data access permissions for the default Read-Only Admin policy.

Step 2 Click **Actions** next to any of the default RBAC policy rule.

Here, you can insert new RBAC policies, duplicate an existing RBAC policy, and delete an existing RBAC policy.

Step 3 Click **Insert new policy**.

Step 4 Enter values for the Rule Name, RBAC Group(s), and Permissions fields.

You cannot select multiple menu access and data access permissions when creating an RBAC policy.

Step 5 Click **Save**.

Administrator Access Settings

Cisco ISE allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define under the Administrator Account Settings in Cisco ISE applies to all administrator accounts.

Cisco ISE does not support administrator passwords with UTF-8 characters.

Configure the Maximum Number of Concurrent Administrative Sessions and Login Banners

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners are disabled.

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Access** > **Session**.

Step 2 Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.

Step 3 If you want Cisco ISE to display a message before an administrator logs in, check the **Pre-login banner** check box and enter your message in the text box.

Step 4 If you want Cisco ISE to display a message after an administrator logs in, check the **Post-login banner** check box and enter your message in the text box.

Step 5 Click **Save**.

Related Topics

Allow Administrative Access to Cisco ISE from Select IP Addresses, on page 126

Allow Administrative Access to Cisco ISE from Select IP Addresses

Cisco ISE allows you to configure a list of IP addresses from which administrators can access the Cisco ISE management interfaces.

The administrator access control settings are only applicable for Cisco ISE nodes that assume the Administration, Policy Service, or Monitoring personas. These restrictions are replicated from the primary to the secondary nodes.

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Access** > **IP Access**.

Step 2 Select **Allow only listed IP addresses to connect**.

Note Connection on Port 161 (SNMP) is used for Administrative access. However, when IP Access restrictions are configured, the snmpwalk fails if the node from which it was performed is not configured for Administrative access.

Step 3 From the Configure IP List for Access Restriction area, click **Add**.

Step 4 Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.

Note This IP address can range from IPv4 and IPv6. You can now configure multiple IPv6 adresses for an ISE node.

Step 5 Enter the subnet mask in the Netmask in CIDR format field.

Step 6 Click **OK**. Repeat the process to add more IP address ranges to this list.

Step 7 Click **Save** to save the changes.

Step 8 Click **Reset** to refresh the **IP Access** page.

Allow Access to the MnT Section in Cisco ISE

Cisco ISE allows you to configure a list of nodes from which administrators can access the MnT section in Cisco ISE.

Before you begin

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

Procedure

Step 1 From the Cisco ISE home page, choose **Administration** > **System** > **Admin Access** > **Settings** > **Access**.

Step 2 Click the **MnT Access** tab.

Step 3 To allow nodes or entities either within the deployment or outside the deployment to send syslogs to MnT, click the **Allow any IP address to connect to MnT** radio button. To allow only nodes or entities within the deployment to send syslogs to MnT, click the **Allow only the nodes in the deployment to connect to MnT** radio button.

Note For ISE 2.6 P2 and later, Use ISE Messaging Service for UDP Syslogs delivery to MnT is turned on by default which doesn't allow syslogs coming from any other entities outside of deployment.

Configure a Password Policy for Administrator Accounts

Cisco ISE also allows you to create a password policy for administrator accounts to enhance security. You can define whether you want a password based or client certificate based administrator authentication. The password policy that you define here is applied to all administrator accounts in Cisco ISE.

Note

- Email notifications for internal Admin users are sent to root@host. You cannot configure the email address, and many SMTP servers reject this email.

  You can follow open defect CSCui5583, which is an enhancement to allow you to change the email address.

- Cisco ISE does not support administrator passwords with UTF-8 characters.

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Make sure that the auto-failover configuration, if enabled in your deployment, is turned off. When you change the authentication method, you will be restarting the application server processes. There might be a delay while these services restart. Due to this delay in restart of services, auto-failover of secondary Administration node might get initiated.

Procedure

Step 1 Choose **Administration** > **System** > **Admin Access** > **Authentication**.

Step 2 Select either of these authentication methods:

- Password Based—If you want to use the standard user ID and password credentials for an administrator login, choose the **Password Based** option and specify either the "Internal" or "External" authentication type.

Note If you have configured an external identity source such as LDAP and want to use that as your authentication source to grant access to the admin user, you must select that particular identity source from the Identity Source list box.

- Client Certificate Based—If you want to specify a certificate-based policy, choose the **Client Certificate Based** option, and select an existing Certificate Authentication Profile.

Step 3 Click the **Password Policy** tab and enter the values.

Step 4 Click **Save** to save the administrator password policy.

Note If you are using an external identity store to authenticate administrators at login, remember that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator's username and password.

Related Topics

Administrator Password Policy Settings, on page 130
Configure Account Disable Policy for Administrator Accounts, on page 128
Configure Lock or Suspend Settings for Administrator Accounts, on page 128

Configure Account Disable Policy for Administrator Accounts

Cisco ISE allows you to disable the administrator account if the administrator account is not authenticated for the configured consecutive number of days.

Procedure

Step 1 Choose **Administration > System > Admin Access > Authentication > Account Disable Policy**.

Step 2 Check the **Disable account after *n* days of inactivity** check box and enter the number of days.

This option allows you to disable the administrator account if the administrator account was inactive for the consecutive number of days. However, you can exclude individual administrator account from this account disable policy using the **Inactive Account Never Disabled** option available at **Administration > System > Admin Access > Administrators > Admin Users**.

Step 3 Click **Save** to configure the global account disable policy for administrators.

Configure Lock or Suspend Settings for Administrator Accounts

Cisco ISE allows you to lock or suspend administrator accounts (including password-based Internal Admin accounts and certificate-based Admin accounts) that have more than a specified number of failed login attempts.

Procedure

Step 1 Choose **Administration > System > Admin Access > Authentication > Lock/Suspend Settings**.

Step 2 Check the Suspend or Lock Account With Incorrect Login Attempts check box and enter the number of failed attempts after which action should be taken. The valid range is between 3 and 20.

- Suspend Account For n Minutes—Select this option to suspend an account that exceeds a specified number of incorrect login attempts. The valid range is between 15 and 1440.
- Lock Account—Select this option to lock an account that exceeds a specified number of incorrect login attempts.

You can enter a custom e-mail remediation message, such as asking the end user to contact helpdesk to unlock the account.

Note The Lock/Suspend settings were available in the Password Policy tab in the earlier releases of Cisco ISE.

Configure Session Timeout for Administrators

Cisco ISE allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE Admin portal.

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Session** > **Session Timeout**.

Step 2 Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

Step 3 Click **Save**.

Terminate an Active Administrative Session

Cisco ISE displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

Before you begin

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

Procedure

Step 1 Choose **Administration** > **System** > **Admin Access** > **Settings** > **Session** > **Session Info**.

Step 2 Check the check box next to the session ID that you want to terminate and click **Invalidate**.

Change Administrator Name

Cisco ISE allows you to change your username from the GUI.

Before you begin

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

Procedure

Step 1 Log in to the Admin portal.
Step 2 Click your username that appears as a link at the upper right corner of the Cisco ISE UI.
Step 3 Enter the new username in the Admin User page that appears.
Step 4 Edit any other details about your account that you want to change.
Step 5 Click **Save**.

Admin Access Settings

These pages enable you to configure access settings for administrators.

Administrator Password Policy Settings

The following table describes the fields on the Administrator Password Policy page, which you can use to define a criteria that administrator passwords should meet. The navigation path for this page is:**Administration** > **System** > **Admin Access** > **Authentication** > **Password Policy**.

Table 18: Administrator Password Policy Settings

Fields	Usage Guidelines
Minimum Length	Specifies the minimum length of the password (in characters). The default is six characters.

Fields	Usage Guidelines
Password must not contain	Admin name or its characters in reverse order—Check this check box to restrict the use of the administrator username or its characters in reverse order.
	"cisco" or its characters in reverse order—Check this check box to restrict the use of the word “cisco” or its characters in reverse order.
	This word or its characters in reverse order—Check this check box to restrict the use of any word that you define or its characters in reverse order.
	Repeated characters four or more times consecutively—Check this check box to restrict the use of repeated characters four or more times consecutively.
	Dictionary words, their characters in reverse order or their letters replaced with other characters—Check this check box to restrict the use of dictionary words, their characters in reverse order or their letters replaced with other characters. Substitution of "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e" is not permitted. For example, Pa$$w0rd • Default Dictionary—Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words. By default, this option is selected. • Custom Dictionary—Choose this option to use your customized dictionary. Click **Choose File** to select the custom dictionary file. The text file must be of newline-delimited words, .dic extension, and size less than 20 MB.
Required Characters	Specifies that the administrator password must contain at least one character of the type that you choose from the following choices: • Lowercase alphabetic characters • Uppercase alphabetic characters • Numeric characters • Non-alphanumeric characters

Fields	Usage Guidelines
Password History	Specifies the number of previous passwords from which the new password must be different to prevent the repeated use of the same password. Also, specifies the number of characters that must be different from the previous password. Enter the number of days before which you cannot reuse a password.
Password Lifetime	Specifies the following options to force users to change passwords after a specified time period: • Time (in days) before the administrator account is disabled if the password is not changed. (The allowable range is 0 to 2,147,483,647 days.) • Reminder (in days) before the administrator account is disabled.
Display Network Device Sensitive Data	
Require Admin Password	Check this check box if you want the admin user to enter the login password to view network device sensitive data such as shared secrets and passwords.
Password cached for	The password that is entered by the admin user is cached for this time period. The admin user will not be prompted to enter the password again during this period to view network device sensitive data. The valid range is from 1 to 60 minutes.

Related Topics

Cisco ISE Administrators
Create a New Administrator

Session Timeout and Session Information Settings

The following table describes the fields on the Session page, which you can use to define session timeout and terminate an active administrative session. The navigation path for this page is:**Administration** > **System** > **Admin Access** > **Settings** > **Session**.

Table 19: Session Timeout and Session Info Settings

Fields	Usage Guidelines
Session Timeout	
Session Idle Timeout	Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

Fields	Usage Guidelines
Session Info	
Invalidate	Check the check box next to the session ID that you want to terminate and click **Invalidate.**

Related Topics

Administrator Access Settings, on page 125
Configure Session Timeout for Administrators, on page 129
Terminate an Active Administrative Session, on page 129