Define Network Devices in Cisco ISE

A network device, such as a switch or a router, is an authentication, authorization, and accounting (AAA) client that sends AAA service requests to Cisco ISE. Defining network devices in Cisco ISE enables interactions between Cisco ISE and network devices.

Configure network devices for RADIUS or TACACS AAA, and Simple Network Management Protocol (SNMP) for the Profiling service to collect Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) attributes for profiling endpoints, and TrustSec attributes for Cisco TrustSec devices. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

From the Cisco ISE main menu, choose **Administration** > **Network Resources** > **Network Devices**, and click **Add**. In the **New Network Device** window that is displayed, enter the following details to define a network device:

- Select the vendor profile that fits the network device. The profile includes predefined configurations for the device, such as settings for URL redirect and change of authorization.
- Configure the RADIUS protocol for RADIUS authentications. When Cisco ISE receives a RADIUS request from a network device, it looks for the corresponding device definition to retrieve the configured shared secret. If Cisco ISE finds the device definition, it obtains the configured shared secret on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the RADIUS server processes the request further based on the policy and configuration. If the shared secrets do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.
- Configure the TACACS+ protocol for TACACS+ authentications. When Cisco ISE receives a TACACS+ request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the TACACS+ server processes the request further based on the policy and configuration. If they do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.
- You can configure the Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.
- You must define Cisco TrustSec-enabled devices in Cisco ISE to process requests from TrustSec-enabled devices that can be part of the Cisco TrustSec solution. Any switch that supports the Cisco TrustSec solution is a Cisco TrustSec-enabled device.

Cisco TrustSec devices do not use IP addresses. Instead, you must define other settings so that Cisco TrustSec devices can communicate with Cisco ISE.

Cisco TrustSec-enabled devices use the TrustSec attributes to communicate with Cisco ISE. Cisco TrustSec-enabled devices, such as the Cisco Nexus 7000 Series Switches, Cisco Catalyst 6000 Series Switches, Cisco Catalyst 4000 Series Switches, and Cisco Catalyst 3000 Series Switches are authenticated using the Cisco TrustSec attributes that you define while adding Cisco TrustSec devices.

Note When you configure a network device on Cisco ISE, we recommend that you do not include a backslash (\) as part of the shared secret. This is because when you upgrade Cisco ISE, the backslash will not appear in the shared secret. However, if you reimage Cisco ISE instead of upgrading it, the backslash appears in the shared secret.

Define a Default Network Device in Cisco ISE

Cisco ISE supports the default device definition for RADIUS and TACACS authentications. You can define a default network device that Cisco ISE can use if it does not find a device definition for a particular IP address. This feature enables you to define a default RADIUS or TACACS shared secret and the level of access for newly provisioned devices.

Note We recommend that you add the default device definition only for basic RADIUS and TACACS authentications. For advanced flows, you must add a separate device definition for each network device.

Cisco ISE looks for the corresponding device definition to retrieve the shared secret that is configured in the network device definition when it receives a RADIUS or TACACS request from a network device.

Cisco ISE performs the following procedure when a RADIUS or TACACS request is received:

1. Looks for a specific IP address that matches the one in the request.
2. Looks up the ranges to see if the IP address in the request falls within the range that is specified.
3. If both step 1 and 2 fail, it uses the default device definition (if defined) to process the request.

Cisco ISE obtains the shared secret that is configured in the device definition for that device and matches it against the shared secret in the RADIUS or TACACS request to authenticate access. If no device definitions are found, Cisco ISE obtains the shared secret from the default network device definition and processes the RADIUS or TACACS request.

Network Devices

The windows described in the following sections enable you to add and manage network devices in Cisco ISE.

Note IPv4 and IPv6 are now supported for configuring network devices (TACACS and RADIUS) and external RADIUS servers. When entering an IPv4 address, you can use ranges and subnet masks. Ranges are not supported for IPv6.

Network Device Definition Settings

The following tables describe the fields in the **Network Devices** window, which you can use to configure a network access device in Cisco ISE. The navigation path for this page is **Administration** > **Network Resources** > **Network Devices**, and click **Add**.

Network Device Settings

The following table describes the fields in the **New Network Devices** window.

Table 1: Network Device Settings

Field Name	Description
Name	Enter a name for the network device. You can provide a descriptive name to the network device, which is different from the hostname of the device. The device name is a logical identifier. **Note** If needed, the name of a device can be changed after it is configured.
Description	Enter a description for the device.

Field Name	Description
IP Address or **IP Range**	Choose one of the following from the drop-down list and enter the required values in the fields displayed: • **IP Address**: Enter a single IP address (IPv4 or IPv6 address) and a subnet mask. • **IP Range**: Enter the required IPv4 address range. To exclude IP addresses during authentication, enter an IP address or IP address range in the **Exclude** text box. The following are the guidelines for defining the IP addresses and subnet masks, or IP address ranges: • You can define a specific IP address, or an IP range with a subnet mask. If device A has an IP address range defined, you can configure another device, B, with an individual address from the range that is defined in device A. • You can define IP address ranges in all the octets. You can use a hyphen (-) or an asterisk (*) as wildcard to specify a range of IP addresses. For example, *.*.*.*, 1-10.1-10.1-10.1-10, or 10-11.*.5.10-15. • You can exclude a subset of IP address range from the configured range in a scenario where that subset has already been added, for example, 10.197.65.*/10.197.65.1, or 10.197.65.* exclude 10.197.65.1. • You cannot define two devices with the same specific IP addresses. • You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.
Device Profile	Choose the vendor of the network device from the drop-down list. Use the tooltip next to the drop-down list to see the flows and services that the selected vendor's network devices support. The tooltip also displays the RADIUS Change of Authorization (CoA) port and type of URL redirect that is used by the device. These attributes are defined in the device type's network device profile.
Model Name	Choose the device model from the drop-down list. Use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Software Version	Choose the version of the software running on the network device from the drop-down list. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Network Device Group	In the **Network Device Group** area, choose the required values from the **Location**, **IPSEC**, and **Device Type** drop-down lists. If you do not specifically assign a device to a group, it becomes a part of the default device groups (root network device groups), which is **All Locations** by location and **All Device Types** by device type.

Note While using a filter to choose and delete a Network Access Device (NAD) from your Cisco ISE deployment, clear your browser cache to ensure that only chosen NADs are deleted.

RADIUS Authentication Settings

The following table describes the fields in the **RADIUS Authentication Settings** area.

Table 2: Fields in the RADIUS Authentication Settings Area

Field Name	Usage Guidelines
RADIUS UDP Settings	
Protocol	Displays **RADIUS** as the selected protocol.
Shared Secret	Enter the shared secret for the network device. The shared secret is the key that is configured on the network device using the **radius-host** command with the **pac** option. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration > Network Resources > Network Devices > Device Security Settings**). For a RADIUS server, the best practice is to have 22 characters. For new installations and upgraded deployments, the shared secret length is four characters by default. You can change this value in the **Device Security Settings** window.
Use Second Shared Secret	Specify a second shared secret to be used by the network device and Cisco ISE. **Note** Although Cisco TrustSec devices can take advantage of the dual shared secrets (keys), Cisco TrustSec CoA packets sent by Cisco ISE will always use the first shared secret (key). To enable the use of the second shared secret, choose the Cisco ISE node from which the Cisco TrustSec CoA packets must be sent to the Cisco TrustSec device. Configure the Cisco ISE node to be used for this task in the **Send From** drop-down list in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices** > **Add** > **Advanced TrustSec Settings** window. You can select a primary administration node (PAN) or a policy service node (PSN). If the chosen PSN node is down, the PAN sends the Cisco TrustSec CoA packets to the Cisco TrustSec device. **Note** The Second Shared Secret feature for RADIUS Access Request works only for packets containing the **Message-Authenticator** field.

Field Name	Usage Guidelines
CoA Port	Specify the port to be used for RADIUS CoA. The default CoA port for the device is defined in the network device profile that is configured for a network device (**Administration** > **Network Resources** > **Network Device Profiles** > **Network Resources** > **Network Device Profiles**). Click **Set To Default** to use the default CoA port. **Note** If you modify the CoA port specified in the **Network Devices** window (**Administration** > **Network Resources** > **Network Devices**) under **RADIUS Authentication Settings**, make sure that you specify the same CoA port for the corresponding profile in the **Network Device Profile** window (**Administration** > **Network Resources** > **Network Device Profiles**).
RADIUS DTLS Settings	
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for Secure Sockets Layer (SSL) tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and used to compute the Message Digest 5 (MD5) integrity checks.
CoA Port	Specify the port to be used for RADIUS DTLS CoA.
Issuer CA of ISE Certificates for CoA	Choose the Certificate Authority to be used for RADIUS DTLS CoA from the drop-down list.
DNS Name	Enter the DNS name of the network device. If the **Enable RADIUS/DTLS Client Identity Verification** option is enabled in the **RADIUS Settings** window (**Adminstration** > **System** > **Settings** > **Protocols** > **RADIUS**, Cisco ISE compares this DNS name with the DNS name that is specified in the client certificate to verify the identity of the network device.
General Settings	
Enable KeyWrap	Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported by the network device. The network device must be compatible with AES KeyWrap RFC (RFC 3394). This option is used to increase the RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter the encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.

Field Name	Usage Guidelines
Key Input Format	Click one of the following radio buttons: • **ASCII**: The value that is entered in the **Key Encryption Key** field must be 16 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 20 characters (bytes) in length. • **Hexadecimal**: The value that is entered in the **Key Encryption Key** field must be 32 characters (bytes) in length, and the value that is entered in the **Message Authenticator Code Key** field must be 40 characters (bytes) in length. You can specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key, and shorter values are not permitted.

TACACS Authentication Settings

Table 3: Fields in the TACACS Authentication Settings Area

Field Name	Usage Guidelines
Shared Secret	A string of text that is assigned to a network device when TACACS+ protocol is enabled. The user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. You can click either **Yes** or **No**.
Remaining Retired Period	(Available only if you click **Yes** in the **Retire** dialog box) Displays the default value that is specified in **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period.** You can change the default value, as necessary. The old shared secret remains active for the specified number of days.
End	(Available only if you click **Yes** in the **Retire** dialog box) Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS communications with the network device. Click one of the following radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support** **Note** If you disable **Single Connect Mode**, Cisco ISE uses a new TCP connection for every TACACS request.

SNMP Settings

The following table describes the fields in the **SNMP Settings** section.

Table 4: Fields in the SNMP Settings Area

Field Name	Usage Guidelines
SNMP Version	Choose one of the following options from the **SNMP Version** drop-down list: • **1**: SNMPv1 does not support informs. • **2c** • **3**: SNMPv3 is the most secure model because it allows packet encryption when you choose **Priv** in the **Security Level** field. **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** > **Diagnostics** > **Network Device Session Status**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Applicable only for SNMP versions 1 and 2c) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device. **Note** The caret (circumflex ^) symbol is not allowed.
SNMP Username	(Only for SNMP Version 3) Enter the SNMP username.
Security Level	(Only for SNMP Version 3) Choose one the following options from the **Security Level** drop-down list: • **Auth**: Enables MD5 or Secure Hash Algorithm (SHA) packet authentication. • **No Auth**: No authentication and no privacy security level. • **Priv**: Enables Data Encryption Standard (DES) packet encryption.
Auth Protocol	(Only for SNMP Version 3 when the security levels **Auth** or **Priv** are selected) Choose the authentication protocol that you want the network device to use from the **Auth Protocol** drop-down list. • **MD5** • **SHA**
Auth Password	(Only for SNMP Version 3 when the **Auth** or **Priv** security levels are selected) Enter the authentication key. It must be at least eight characters in length. Click **Show** to display the authentication password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.

Field Name	Usage Guidelines
Privacy Protocol	(Only for SNMP Version 3 when **Priv** security level is selected) Choose one of the following options from the **Privacy Protocol** drop-down list: • **DES** • **AES128** • **AES192** • **AES256** • **3DES**
Privacy Password	(Only for SNMP Version 3 when **Priv** security level is selected) Enter the privacy key. Click **Show** to display the privacy password that is already configured for the device. **Note** The caret (circumflex ^) symbol cannot be used.
Polling Interval	Enter the polling interval, in seconds. The default value is 3600.
Link Trap Query	Check the **Link Trap Query** check box to receive and interpret linkup and linkdown notifications that are received through the SNMP trap.
Mac Trap Query	Check the **Link Trap Query** check box to receive and interpret MAC notifications received through the SNMP trap.
Originating Policy Services Node	Choose the Cisco ISE server to be used to poll for SNMP data, from the **Originating Policy Services Node** drop-down list. The default value for this field is **Auto**. Overwrite the setting by choosing a specific value from the drop-down list.

Advanced TrustSec Settings

The following table describes the fields in the **Advanced TrustSec Settings** section.

Table 5: Fields in the Advanced TrustSec Settings Area

Field Name	Usage Guidelines
Device Authentication Settings	
Use Device ID for TrustSec Identification	Check the **Use Device ID for TrustSec Identification** check box if you want the device name to be listed as the device identifier in the **Device ID** field.
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
HTTP REST API Settings	

Field Name	Usage Guidelines
TrustSec Device Notification and Updates	
Device ID	You can use this field only if you have not checked the **Use Device ID for TrustSec Identification** check box.
Password	Enter the password that you have configured in the Cisco TrustSec device's CLI to authenticate the Cisco TrustSec device. Click **Show** to display the password.
Download Environment Data Every <...>	Specify the time interval at which the device must download its environment data from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can choose the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Download Peer Authorization Policy Every <...>	Specify the time interval at which the device must download the peer authorization policy from Cisco ISE by choosing the required values from the drop-down lists in this area. You can specify the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Reauthentication Every <...>	Specify the time interval at which the device reauthenticates itself against Cisco ISE after the initial authentication, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. For example, if you enter 1000 seconds, the device authenticates itself against Cisco ISE every 1000 seconds. The default value is one day.
Download SGACL Lists Every <...>	Specify the time interval at which the device downloads SGACL lists from Cisco ISE, by choosing the required values from the drop-down lists in this area. You can configure the time interval in seconds, minutes, hours, days, or weeks. The default value is one day.
Other TrustSec Devices to Trust This Device (TrustSec Trusted)	Check the **Other TrustSec Devices to Trust This Device** check box to allow all the peer devices to trust this Cisco TrustSec device. If this check box is not checked, the peer devices do not trust this device, and all the packets that arrive from this device are colored or tagged accordingly.
Send Configuration Changes to Device	Check the **Send Configuration Changes to Device** check box if you want Cisco ISE to send Cisco TrustSec configuration changes to the Cisco TrustSec device using CoA or CLI (SSH). Click the **CoA** or **CLI (SSH)** radio button, as required. Click the **CoA** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using CoA. Click the **CLI (SSH)** radio button if you want Cisco ISE to send the configuration changes to the Cisco TrustSec device using the CLI (using the SSH connection). For more information, see the "Push Configuration Changes to Non-CoA Supporting Devices" section in *Cisco ISE Admin Guide: Segmentation*.
Send From	From the drop-down list, choose the Cisco ISE node from which the configuration changes must be sent to the Cisco TrustSec device. You can select a PAN or a PSN. If the PSN that you choose is down, the configuration changes are sent to the Cisco TrustSec device using the PAN.

Field Name	Usage Guidelines
Test Connection	You can use this option to test the connectivity between the Cisco TrustSec device and the selected Cisco ISE node (PAN or PSN).
SSH Key	To use this feature, open an SSHv2 tunnel from Cisco ISE to the network device, and use the device's CLI to retrieve the SSH key. You must copy this key and paste it in the **SSH Key** field for validation. For more information, see the "SSH Key Validation" section in *Cisco ISE Admin Guide: Segmentation*.
Device Configuration Deployment	
Include this device when deploying Security Group Tag Mapping Updates	Check the **Include this device when deploying Security Group Tag Mapping Updates** check box if you want the Cisco TrustSec device to obtain the IP-SGT mappings using the device interface credentials.
EXEC Mode Username	Enter the username that you use to log in to the Cisco TrustSec device.
EXEC Mode Password	Enter the device password. Click **Show** to view the password. **Note** We recommend that you avoid using the % character in passwords, including in the EXEC modes and Enable mode passwords to avoid security vulnerabilities.
Enable Mode Password	(Optional) Enter the enable password that is used to edit the configuration of the Cisco TrustSec device in privileged EXEC mode. Click **Show** to view the password.
Out Of Band TrustSec PAC	
Issue Date	Displays the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Expiration Date	Displays the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Issued By	Displays the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Generate PAC	Click the **Generate PAC** button to generate the out-of-band Cisco TrustSec PAC for the Cisco TrustSec device.

Default Network Device Definition Settings

The following table describes the fields in the **Default Network Device** window, with which you configure a default network device that Cisco ISE can use for RADIUS or TACACS+ authentication. Choose one of the following navigation paths:

- **Administration** > **Network Resources** > **Network Devices** > **Default Device**
- **Work Centers** > **Device Administration** > **Network Resources** > **Default Devices**

Table 6: Fields in the Default Network Device Window

Field Name	Usage Guidelines
Default Network Device Status	Choose **Enable** from the **Default Network Device Status** drop-down list to enable the default network device definition. **Note** If the default device is enabled, you must enable either the RADIUS or the TACACS+ authentication settings by checking the relevant check box in the window.
Device Profile	Displays **Cisco** as the default device vendor.
RADIUS Authentication Settings	
Enable RADIUS	Check the **Enable RADIUS** check box to enable RADIUS authentication for the device.
RADIUS UDP Settings	
Shared Secret	Enter a shared secret. The shared secret can be up to 127 characters in length. The shared secret is the key that you have configured on the network device using the **radius-host** command with the **pac** keyword. **Note** The length of the shared secret must be equal to or greater than the value configured in the **Minimum RADIUS Shared Secret Length** field in the **Device Security Settings** window (**Administration** > **Network Resources** > **Network Devices** > **Device Security Settings**). By default, this value is four characters for new installations and upgraded deployments. For the RADIUS server, the best practice is to have 22 characters.
RADIUS DTLS Settings	
DTLS Required	If you check the **DTLS Required** check box, Cisco ISE processes only the DTLS requests from this device. If this option is disabled, Cisco ISE processes both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for SSL tunnel establishment and RADIUS communication.
Shared Secret	Displays the shared secret that is used for RADIUS DTLS. This value is fixed and is used to compute the MD5 integrity checks.
Issuer CA of ISE Certificates for CoA	Choose the certificate authority to be used for RADIUS DTLS CoA from the **Issuer CA of ISE Certificates for CoA** drop-down list.
General Settings	

Field Name	Usage Guidelines
Enable KeyWrap	(Optional) Check the **Enable KeyWrap** check box only if KeyWrap algorithms are supported on the network device, which increases RADIUS security through an AES KeyWrap algorithm.
Key Encryption Key	Enter an encryption key to be used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.
Key Input Format	Choose one of the following formats by clicking the corresponding radio button, and enter values in the **Key Encryption Key** and **Message Authenticator Code Key** fields: • **ASCII**: The **Key Encryption Key** must be 16 characters (bytes) in length, and the **Message Authenticator Code Key** must be 20 characters (bytes) in length. • **Hexadecimal**: The **Key Encryption Key** must be 32 bytes in length, and the **Message Authenticator Code Key** must be 40 bytes in length. Specify the key input format that you want to use to enter the Key Encryption Key and Message Authenticator Code Key so that it matches the configuration on the network device. The value that you specify must be the correct (full) length for the key. Shorter values are not permitted.
TACACS Authentication Settings	
Shared Secret	Enter a string of text to assign to a network device when the TACACS+ protocol is enabled. Note that a user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click **Retire**, a dialog box is displayed. Click **Yes** or **No**.
Remaining Retired Period	(Optional) Available only if you click **Yes** in the **Retire** dialog box. Displays the default value that is specified in the **Work Centers** > **Device Administration** > **Settings** > **Connection Settings** > **Default Shared Secret Retirement Period** window. You can change the default values. This allows a new shared secret to be entered. The old shared secret remains active for the specified number of days.
End	(Optional) Available only if you select **Yes** in the **Remaining Retired Period** dialog box. Ends the retirement period and terminates the old shared secret.

Field Name	Usage Guidelines
Enable Single Connect Mode	Check the **Enable Single Connect Mode** check box to use a single TCP connection for all TACACS+ communication with the network device. Click one of the following the radio buttons: • **Legacy Cisco Devices** • **TACACS Draft Compliance Single Connect Support**. **Note** If you disable this field, Cisco ISE uses a new TCP connection for every TACACS+ request.

Network Device Import Settings

Table 7: Import Network Devices Settings

Field Name	Usage Guidelines
Generate a Template	Click **Generate a Template** to create a comma-separated value (CSV) template file. Update the template with network devices information in the CSV format and save it locally. Then, use the edited template to import network devices into any Cisco ISE deployment.
File	Click **Choose File** to choose the CSV file that you have recently created, or previously exported from a Cisco ISE deployment. You can import network devices into another Cisco ISE deployment with new and updated network devices information, by using the **Import** option.
Overwrite Existing Data with New Data	Check the **Overwrite Existing Data with New Data** check box to replace the existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.
Stop Import on First Error	Check the **Stop Import on First Error** check box if you want Cisco ISE to discontinue import when it encounters an error during import. Cisco ISE imports network devices until the time of an error. If this check box is not checked and an error is encountered, the error is reported and Cisco ISE continues to import the remaining devices.

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 a network device in the **Network Devices** (**Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**) window.

Before you begin

The AAA function must be enabled on the network device to be added. See the section "Command to Enable AAA Functions" in chapter the "Integrations" in the *Cisco ISE Administrator Guide* for your release.

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

Step 2 Click **Add**.

Step 3 Enter the corresponding values in the **Name**, **Description**, and **IP Address** fields.

Note IPv4 and IPv6 are both supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configuration. Ranges and subnet masks are supported for IPv4 addresses. Ranges are not supported for IPv6 addresses.

Step 4 Choose the required values from the **Device Profile**, **Model Name**, **Software Version**, and **Network Device Group** drop-down lists.

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 SNMP for the Cisco ISE profiling service to collect information from the network device.

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

Step 9 Click **Submit**.

Import Network Devices into Cisco ISE

To enable Cisco ISE to communicate with network devices, you must add device definitions of the network devices in Cisco ISE. Import device definitions of network devices into Cisco ISE through the **Network Devices** window (From the main menu, choose **Administration** > **Network Resources** > **Network Devices**).

Import a list of device definitions into a Cisco ISE node using a comma-separated value (CSV) file. A CSV template file is available when you click **Import** in the **Network Devices** window. Download this file, enter the required device definitions, and then upload the edited file through the **Import** window.

You cannot execute multiple imports of the same resource type at the same time. For example, you cannot concurrently import network devices from two different import files.

When you import a CSV file of device definitions, you can either create new records or update existing records by clicking the **Overwrite Existing Data with New Data** option.

Import templates may vary in each Cisco ISE. Do not import CSV files of network devices that have exported from a different Cisco ISE release. Enter the details of the network devices in the CSV template file for your release, and import this file into Cisco ISE.

Note You can import the network devices with IP ranges in all the octets.

Note IPv4 and IPv6 are supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configuration. When entering an IPv4 address, you can use ranges and subnet masks. Ranges are not supported for IPv6.

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

Step 2 Click **Import**.

Step 3 In the **Import Network Devices** window that is displayed, click **Generate A Template** to download a CSV file that you can edit and then import it into Cisco ISE with the required details.

Step 4 Click **Choose File** to choose the CSV file from the system that is running the client browser.

Step 5 (Optional) Check the for **Overwrite Existing Data with New Data** and **Stop Import on First Error**check boxes, as required.

Step 6 Click **Import**.

After the file import is complete, Cisco ISE displays a summary message. This message includes the import status (successful or unsuccessful), number of errors encountered, if any, and the total processing time taken for the file import process.

Export Network Devices from Cisco ISE

Export the device definitions of the network devices that are available in a Cisco ISE node in the form of a CSV file. You can then import this CSV file into another Cisco ISE node so that the device definitions are available to the required Cisco ISE nodes.

Note You can export the network devices with IP ranges in all the octets.

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

Step 2 Click **Export**.

Step 3 Export the device definitions for the network devices added to the Cisco ISE node by performing one of the following actions.

- Check the check boxes next to the devices that you want to export, choose **Export Selected** from the **Export** drop-down list.
- Choose **Export All** from the **Export** drop-down list to export all the network devices that are added to the Cisco ISE node.

Step 4 In both cases, a CSV file of device definitions downloads to your system.

Troubleshoot Network Device Configuration Issues

Step 1 Choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Evaluate Configuration Validator**.

Step 2 Enter the IP address of the network device that you want to evaluate in the **Network Device IP** field.

Step 3 Check the check boxes and click the radio buttons next to the configuration options you want to compare against the recommended template.

Step 4 Click **Run**.

Step 5 In the **Progress Details...** area, click **Click Here to Enter Credentials**.

Step 6 In the **Credentials Window** dialog box, enter the connection parameters and credentials that are required to establish a connection with the network devices.

Step 7 Click **Submit**.

Step 8 (Optional) To cancel the workflow, click **Click Here to Cancel the Running Workflow** in the **Progress Details...** window.

Step 9 (Optional) Check the check boxes next to the interfaces that you want to analyze, and click **Submit**.

Step 10 (Optional) Click **Show Results Summary** for details of the configuration evaluation.

The Execute Network Device Command Diagnostic Tool

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device.

The results that are displayed are the same as what you would see on a console. The tool enables you to identify problems, if any, in a device configuration.

Use this tool to validate the configuration of any network device, or if you are want to know how a network device is configured.

To access the Execute Network Device Command diagnostic tool, choose one of the following navigation paths:

1. Choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Execute Network Device Command**.Choose **Work Centers** > **Profiler** > **Troubleshoot** > **Execute Network Device Command**.
2. In the **Execute Network Device Command** window that is displayed, enter the IP address of the network device and the **show** command that you want to run in the corresponding fields.
3. Click **Run**.

Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) by using network device profiles. A NAD profile defines the capabilities of a third-party device with a simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols that the network device supports, such as RADIUS, TACACS+, and Cisco TrustSec. You can import into Cisco ISE any vendor-specific RADIUS dictionaries that exist for the network device.
- The attributes and values that the device uses for various authentication flows such as Wired MAB and 802.1X. These attributes and values allow Cisco ISE to detect the right authentication flow for your device according to the attributes that the network device uses.
- The Change of Authorization (CoA) capabilities of the network device. While the RADIUS protocol RFC 5176 defines a CoA request, the attributes used in a CoA request vary depending on the network device. Most non-Cisco devices with RFC 5176 support the *Push* and *Disconnect* functions. For devices that do not support the RADIUS CoA type, Cisco ISE also supports SNMP CoA.
- The attributes and protocols that the network device uses for MAB flows. Network devices from different vendors perform MAB authentication differently.
- The VLAN and ACL permissions that are used by the device. When you save the profile, Cisco ISE automatically generates authorization profiles for each configured permission.
- URL redirection technique information. URL redirection is necessary for advanced flows such as Bring Your Own Device (BYOD), guest access, and posture services. Two types of URL redirections are found on a network device—static and dynamic. For static URL redirection, you can copy and paste the Cisco ISE portal URL into the configuration. For dynamic URL redirection, Cisco ISE uses a RADIUS attribute to tell the network device where to redirect to.

  If the network device does not support both dynamic and static URL redirects, Cisco ISE provides an Auth VLAN configuration by which URL redirect is simulated. The Auth VLAN configuration is based on DHCP and DNS services running in Cisco ISE.

After you have defined your network devices in Cisco ISE, configure these device profiles or use the preconfigured device profiles that are offered by Cisco ISE to define the capabilities that Cisco ISE uses to enable basic authentication flows, and advanced flows such as Profiler, Guest, BYOD, MAB, and Posture.

URL Redirect Mechanism and Auth VLAN

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, Cisco ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP or DNS service on Cisco ISE.

The following is an example of an Auth VLAN flow:

1. A guest endpoint connects to the NAD.
2. The network device sends the RADIUS or MAB request to Cisco ISE.
3. Cisco ISE runs the configured authentication and authorization policy and stores the user accounting information.
4. Cisco ISE sends the RADIUS access accept message that contains the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request, and obtains a client IP address and the Cisco ISE DNS sink hole IP address from the Cisco ISE DHCP service.
7. The guest endpoint opens a browser that sends a DNS query and receives the Cisco ISE IP address.
8. The endpoint HTTP and HTTPS requests are directed to Cisco ISE.

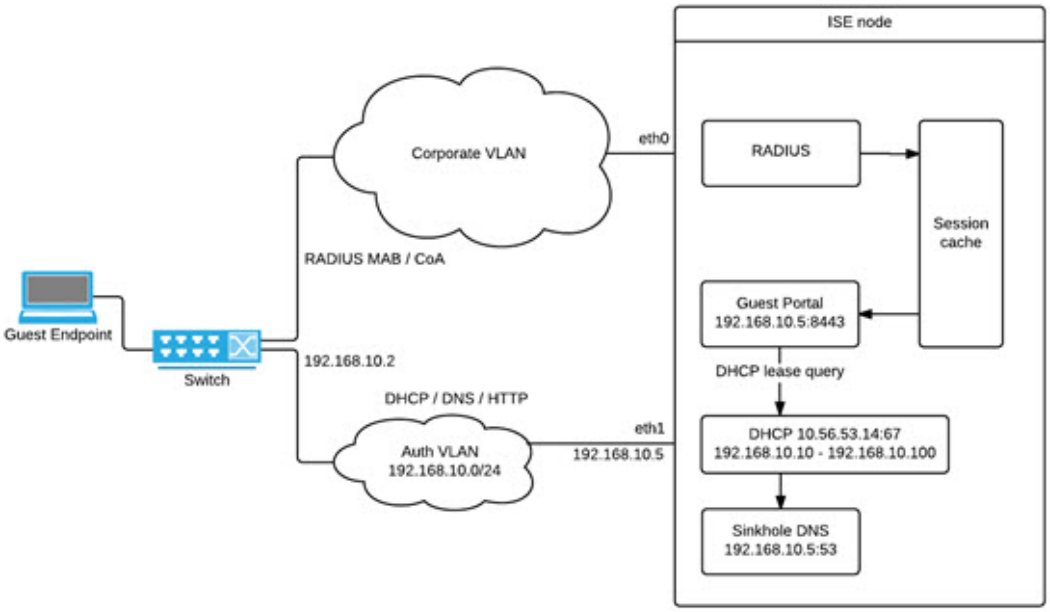
9. Cisco ISE responds with an **HTTP 301 Moved** message with a guest portal URL. The endpoint browser redirects to the guest portal window.
10. The guest endpoint user logs in for authentication.
11. Cisco ISE validates endpoint compliance and then responds to the NAD. Cisco ISE sends the CoA, authorizes the endpoint, and bypasses the sink hole.
12. The guest user receives the appropriate access based on the CoA, and the endpoint receives an IP address from an enterprise DHCP. The guest user can now use the network.

You can separate the Auth VLAN from the corporate network to prevent unauthorized network access by a guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the Cisco ISE machine, or connect one of the Cisco ISE network interfaces to the Auth VLAN.

Multiple VLANs may be connected to one network interface card by configuring a VLAN IP helper from the NAD configuration. For more information about configuring an IP helper, see the administration guide for the network device for instructions. For guest access flows that include VLANs with IP helpers, define a guest portal, and select that portal in an authorization profile that is bound to MAB authorization. For more information about guest portals, see the Cisco ISE Guest Services section in *Cisco ISE Admin Guide: Guest and BYOD* .

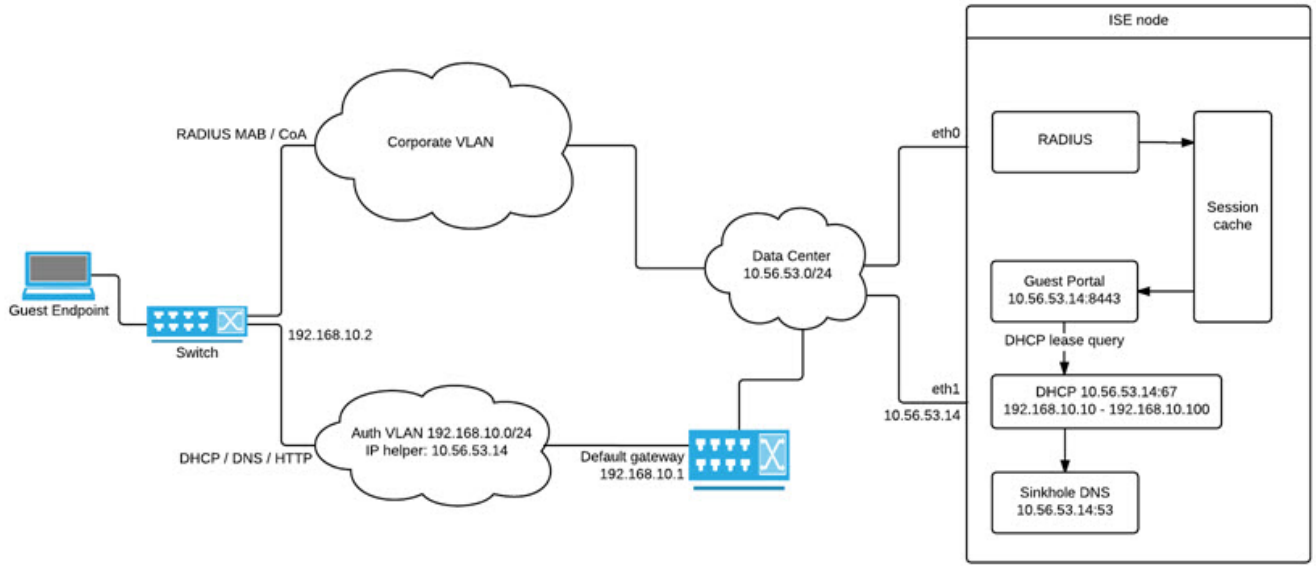
The following diagram displays a basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to a Cisco ISE node).

Figure 1: Auth VLAN Connected to Cisco ISE Node



The following diagram displays a network with Auth VLAN and an IP helper.

Figure 2: Auth VLAN Configured with IP Helper



CoA Types

Cisco ISE supports both RADIUS and SNMP CoA types. RADIUS or SNMP CoA type support is required for the NAD to work in complex flows, while it is not mandatory for basic flows.

Define the RADIUS and SNMP settings that the network device supports when you configure the NAD in Cisco ISE. Indicate the CoA type to be used for a specific flow when configuring the NAD profile. For more information about defining protocols for your NADs, see Network Device Definition Settings, on page 3. Check with your third-party supplier to verify which CoA type your NAD supports before creating the device profile and NAD profile in Cisco ISE.

Network Device Profiles

Cisco ISE supports some third-party NADs by using network device profiles. These profiles define the capabilities that Cisco ISE uses to enable basic flows, and advanced flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from several vendors. Cisco ISE 2.1 and later releases have been tested with the network devices listed in the following table.

Table 8: Vendor Devices Tested with Cisco ISE 2.1 and Later Releases

Device Type	Vendor	CoA Type	URL Redirect Type	Supported or Validated Use Cases				
				802.1X and MAB Flows	Profiler without CoA	Profiler with CoA	Posture	Guest and BYOD Flows

Wireless	Aruba 7000, InstantAP	RADIUS	Static URL	Yes	Yes	Yes	Yes	Yes
	Motorola RFS 4000	RADIUS	Dynamic URL	Yes	Yes	Yes	Yes	Yes
	HP 830	RADIUS	Static URL	Yes	Yes	Yes	Yes	Yes
	Ruckus ZD 1200	RADIUS	—	Yes	Yes	Yes	Yes	Yes
Wired	HP A5500	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	HP 3800 and 2920 (ProCurve)	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	Alcatel 6850	SNMP	Dynamic URL	Yes	Yes	Yes	Yes	Yes
	Brocade ICX 6610	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
	Juniper EX3300-24p	RADIUS	Auth VLAN provided by ISE	Yes	Yes	Yes	Yes	Yes
For other third-party NADs, you must identify the device properties and capabilities, and create custom NAD profiles in Cisco ISE.				Yes	Yes	Requires CoA support	Requires CoA support. If a wired device does not support URL redirect, Cisco ISE uses Auth VLAN. Wireless devices have not been tested with Auth VLAN.	

You must create custom NAD profiles for other third-party network devices that do not have a predefined profile. For advanced workflows such as Guest, BYOD, and Posture, the network device must support the RADIUS protocol RFC 5176, which pertains to CoA support for these flows. See the device's administration guide for information on the attributes that are required to create network device profiles in Cisco ISE.

ISE Community Resource

For information about third-party NAD profiles, see ISE Third-Party NAD Profiles and Configs.

Configure a Third-Party Network Device in Cisco ISE

Cisco ISE supports third-party NADs by using network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Before you begin

See Network Device Profiles, on page 20.

Step 1 Add the third-party network device to Cisco ISE (See Import Network Devices into Cisco ISE, on page 15. If you are configuring Guest, BYOD, or Posture workflows, ensure that CoA is defined and the NAD's URL redirect mechanism is configured to point to the relevant Cisco ISE portal. To configure the URL redirect, copy the Cisco ISE portal URL from the portal's landing page. For more information about configuring CoA types and URL redirects for the NAD in Cisco ISE, see Network Device Definition Settings, on page 3. In addition, see the third-party device's administration guide for instructions.

Step 2 Ensure that an appropriate NAD profile for your device is available in Cisco ISE. To view the existing profiles, choose **Administration** > **Network Resources** > **Network Device Profiles**. If an appropriate profile does not exist in Cisco ISE, create a custom profile. See Create a Network Device Profile, on page 22 for information on how to create custom profiles.

Step 3 Assign a NAD profile to the NAD that you want to configure. Choose **Administration** > **Network Resources** > **Network Devices**. Open the device to which you want to assign a profile, and from the **Device Profile** drop-down list, choose the profile that you want to assign.

Step 4 When you configure your policy rules, set the authorization profile to the NAD profile in step 1, or **Any** if you are just using VLAN or ACL, or if you have different devices from different vendors in your network. To set the NAD profile for the authorization profile, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. Open the relevant authorization profile and from the **Network Device Profile** drop-down list, choose the relevant NAD profile. When using Auth VLAN for Guest flows, you should also define a guest portal and select that portal in an Authorization profile that is bound to MAB authorization—similar to regular Guest flows. For more information about guest portals, see the "Cisco ISE Guest Services" section in *Cisco ISE Admin Guide: Guest and BYOD* .

Create a Network Device Profile

Before you begin

- Most NADs have a vendor-specific RADIUS dictionary that provides several vendor-specific attributes, apart from the standard IETF RADIUS attributes. If the network device has a vendor-specific RADIUS dictionary, import it into Cisco ISE. See the third-party device's administration guide for instructions on which RADIUS dictionary is required. In Cisco ISE, choose **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Radius** > **RADIUS Vendors**. To import RADIUS dictionaries, see the "Create RADIUS-Vendor Dictionaries" section in *Secure Access* .
- For complex flows such as Guest and Posture, the network device must support the CoA types that are defined in RFC 5176
- For information about the fields and possible values for creating a network device profile, see the "Network Device Profiles Settings" section in *Secure Access* .

Step 1 Choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Click **Add**.

Step 3 In the **New Network Device Profile** window that is displayed, enter the corresponding values in the **Name** and **Description** fields for the network device.

Step 4 From the **Vendor** drop-down list, choose the vendor of the network device.

Step 5 In the **Icon** area, click **Change Icon...** to upload an icon for the network device from your system.

Alternatively, in the **Icon** area, click **Set To Default** to use the default icon provided by Cisco ISE.

Step 6 In the **Supported Protocols** area, check the check boxes for the protocols that the device supports. Check the check boxes only for the protocols that you want to actually use. If the network device supports the RADIUS protocol, choose the RADIUS dictionary to be used in the device from **RADIUS Dictionaries** drop-down list.

Step 7 In the **Templates** area, enter relevant details:

a) Click **Authentication/Authorization** to configure the network device's default settings for flow types, attribute aliasing, and host lookup. In the new **Flow Type Conditions** area that is displayed, enter the attributes and values that your device uses for various authentication and authorization flows such as Wired MAB or 802.1X. This enables Cisco ISE to detect the correct flow type for your device according to the attributes it uses. There is no IETF standard for MAB, and different vendors use different values for Service Type. See the device's user guide or use a sniffer trace of a MAB authentication to determine the correct settings. In the **Attribute Aliasing** area, map device-specific attribute names to common names to simplify policy rules. Currently, only the Service Set Identifier (SSID) is defined. If the network device has the concept of wireless SSID, then set this to the attribute it uses. Cisco ISE maps this to an attribute called SSID in the Normalized RADIUS dictionary. This simplifies policy rule configuration because you can refer to SSID in one rule, and it works for multiple devices even if the underlying attributes are different. In the **Host Lookup** area, check the **Process Host Lookup** check box and select the relevant MAB protocols and attributes for your device, based on the instructions provided by the third-party device vendor.

b) Click **Permissions** to configure the network device's default settings for VLAN and ACL. These are automatically mapped based on the authorization profiles that you create in Cisco ISE.

c) Click **Change of Authorization (CoA)** to configure the network device's CoA capabilities.

If you choose **RADIUS** from the **CoA By** drop-down list, in the configurations area that is displayed, you must choose only static attributes. Dynamic attributes are not supported.

d) Click **Redirect** to configure the network device's URL-redirect capabilities. URL redirection is necessary for guest, BYOD, and posture services.

Step 8 Click **Submit**.

Related Topics

How to Create ISE Network Access Device Profiles

Export Network Device Profiles from Cisco ISE

Export single or multiple network device profiles that are configured in Cisco ISE in the form of an XML file. The XML file can then be edited and imported into Cisco ISE file as new network profiles.

Before you begin

See How to Create ISE Network Access Device Profiles.

Step 1 Choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Check the check boxes next to the devices that you want to export, and click **Export Selected**.

Step 3 A file that is named **DeviceProfiles.xml** downloads to your local hard disk.

Import Network Device Profiles into Cisco ISE

Import a single or multiple network device profiles into Cisco ISE using a single XML file with the Cisco ISE XML structure. You cannot concurrently import network device profiles from multiple import files.

Typically, you must first export an existing profile from the Cisco ISE administrator portal to use as a template. Enter your device profile details in the file, and save it as an XML file. Then, import the edited file back into Cisco ISE. To work with multiple network device profiles, export multiple profiles that are structured together as a single XML file, edit the file, and then import the profiles together to create multiple profiles in Cisco ISE.

When you import network device profiles, you can only create new records. You cannot overwrite an existing profile. To update an existing network device profile, export the existing profile from Cisco ISE, delete the profile from Cisco ISE, and then import the profile after you edit it accordingly.

Before you begin

See How to Create ISE Network Access Device Profiles.

Step 1 Choose **Administration** > **Network Resources** > **Network Device Profiles**.

Step 2 Click **Import**.

Step 3 Click **Choose File** to choose the XML file from the system that is running the client browser.

Step 4 Click **Import**.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 9: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

Table 10: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Network Device Groups

Cisco ISE allows you to create hierarchical network device groups. Use network device groups to logically group network devices based on various criteria, such as geographic location, device type, or its relative place in the network (such as Access Layer or Data Center).

To view the Network Device Groups window, choose **Administration** > **Network Resources** > **Network Device Groups**.

For example, to organize your network devices based on geographic location, group them by continent, region, or country:

- **Africa** > **Southern** > **Namibia**
- **Africa** > **Southern** > **South Africa**
- **Africa** > **Southern** > **Botswana**

Group the network devices based on the device type:

- **Africa** > **Southern** > **Botswana** > **Firewalls**
- **Africa** > **Southern** > **Botswana** > **Routers**
- **Africa** > **Southern** > **Botswana** > **Switches**

Assign network devices to one or more hierarchical network device groups. When Cisco ISE processes the ordered list of configured network device groups to determine the appropriate group to assign to a particular device, it may find that the same device profile applies to multiple device groups. In this case, Cisco ISE applies the first device group that is matched.

There is no limit on the maximum number of network device groups that you can create. You can create up to six levels of hierarchy (including the parent group) for the network device groups.

The device group hierarchy is displayed in two views, **Tree Table** and **Flat Table**. Click **Tree Table** or **Flat Table** above the list of network device groups to organize the list into the corresponding view.

In the **Tree Table** view, the root node appears at the top of the tree followed by the child groups in hierarchical order. Click **Expand All** to view all the device groups in each root group. Click **Collapse All** to view a list of only the root groups.

In the **Flat Table** view, the hierarchy of each device group is displayed in the **Group Hierarchy** column.

In both views, the number of network devices that are assigned to each child group is displayed in the corresponding **No. of Network Devices** column. Click the number to launch a dialog box that lists all the network devices that are assigned to that device group. The dialog box that is displayed also contains two buttons to move network devices from one group to another. Click **Move Devices to Another Group** to move network devices from the current group to another. Click **Add Devices to Group** to move a network device into the chosen network device group.

To add a network device group in the **Network Device Groups** window, click **Add**. In the **Parent Group** drop-down list, choose the parent group to which the network device group must be added, or choose the **Add As Root Group** option to add the new network device group as the parent group.

Note You cannot delete a device group if any devices are assigned to that device group. Before deleting a device group, you must move all the existing devices to another device group.

Root Network Device Groups

Cisco ISE includes two predefined root network device groups, **All Device Types** and **All Locations**. You cannot edit, duplicate, or delete these predefined network device groups, but you can add new device groups under them.

You can create a root Network Device Group (network device group), and then create child network device groups under the root group in the **Network Device Groups** window, as described earlier.

Network Device Attributes Used by Cisco ISE in Policy Evaluation

When you create a new network device group, a new network device attribute is added to the **Device** dictionary in **System Dictionaries** (**Policy** > **Policy Elements** > **Dictionaries**). The added device attributes are then used in policy definitions.

Cisco ISE allows you to configure authentication and authorization policies using **Device** dictionary attributes such as the device type, location, model name, or software version that is running on the network device.

Import Network Device Groups into Cisco ISE

You can import network device groups into a Cisco ISE node using a comma-separated value (CSV) file. Not that you cannot concurrently import network device groups from two different import files.

Download a CSV template from the Cisco ISE administrator portal. Enter your network device group details in the template, save the template as a CSV file, and then import the edited file into Cisco ISE.

When importing device groups, you can create new records or update existing records. When you import device groups, you can also define whether you want Cisco ISE to overwrite the existing device groups with the new groups or stop the import process when Cisco ISE encounters the first error.

Step 1 Choose **Administration** > **Network Resources** > **Network Device Groups**.

Step 2 Click **Import**.

Step 3 In the dialog box, click **Choose File** to choose the CSV file from the system that is running the client browser.

To download a CSV template file for adding network device groups, click **Generate a Template**.

Step 4 To overwrite the existing network device groups, check the **Overwrite Existing Data with New Data** check box.

Step 5 Check the **Stop Import on First Error** check box.

Step 6 Click **Import**.

Export Network Device Groups from Cisco ISE

You can export network device groups that are configured in Cisco ISE in the form of a CSV file. You can then import these network device groups into another Cisco ISE node.

Step 1 Choose **Administration** > **Network Resources** > **Network Device Groups** > **All Groups**.

Step 2 To export the network device groups, you can do one of the following:

- Check the check boxes next to the device groups that you want to export, and choose **Export** > **Export Selected**.
- Choose **Export** > **Export All** to export all the network device groups that are defined.

A CSV file is downloaded into your local hard disk.

Manage Network Device Groups

The following windows enable you to configure and manage network device groups.

Network Device Group Settings

You can also create network device groups in the **Work Centers** > **Device Administration** > **Network Resources** > **Network Device Groups** > **All Groups** window.

Table 11: Fields in the Network Device Group Window

Field Name	Usage Guidelines
Name	Enter a name for the root network device group. For all subsequent child network device groups added to this root network device group, enter the name of this newly created network device group. You can have a maximum of six nodes in a network device group hierarchy, including the root node. Each network device group name can have a maximum of 32 characters.
Description	Enter a description for the root or the child network device group.
No. of Network Devices	The number of network devices in the network group is displayed in this column.

Network Device Group Import Settings

Table 12: Fields in the Network Device Groups Import Window

Field Name	Usage Guidelines
Generate a Template	Click this link to download a CSV template file. Update the template with network device group information in the same format. Save the template locally to import the network device groups into any Cisco ISE deployment.
File	Click **Choose File** and navigate to the location of the CSV file that you want to upload. The file may be new or a file that was exported from another Cisco ISE deployment. You can import network device groups from one Cisco ISE deployment to another, with new and updated network device groups information.

Field Name	Usage Guidelines
Overwrite Existing Data with New Data	Check this check box if you want to replace the existing network device groups with the device groups in your import file. If you do not check this check box, only the new network device groups in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box to discontinue import at the first instance of encountering an error during the import. If this check box is not checked and an error is encountered, Cisco ISE reports the error and continues importing the rest of the device groups.

Import Templates in Cisco ISE

Cisco ISE allows you to import a large number of network devices and network device groups using CSV files. The template contains a header row that defines the format of the fields. You must not edit this header row except to add columns mentioned in the table below.

Use the **Generate a Template** link in the relevant import flow for network devices and network device groups to download a CSV file to your local system.

Network Devices Import Template Format

The following table lists and describes the fields in the header of the import network device CSV template file.

Table 13: CSV Template Fields and Descriptions for Network Devices

Field	Usage Guidelines
Name:String(32)	Enter a name for the network device. The name must be an alphanumeric string with a maximum of 32 characters.
Description:String(256)	(Optional) Enter a description for the network device with a maximum of 256 characters.
IP Address:Subnets(a.b.c.d/m|...)	Enter the IP address and subnet mask of the network device. You can enter more than one value separated by a pipe (|) symbol. IPv4 and IPv6 addresses are supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configurations. **Note** IPv4 and IPv6 are supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configurations. When entering an IPv4 address, you can use ranges and subnet masks. Ranges are not supported for IPv6.

Field	Usage Guidelines
Model Name:String(32)	Enter the network device's model name with a maximum of 32 characters.
Software Version:String(32)	Enter the network device's software version with a maximum of 32 characters.
Network Device Groups:String(100)	Enter the names of existing network device groups. If it is a subgroup, it must include both the parent and subgroup, separated by a space. The string must be a maximum of 100 characters, for example, *Location>All Location>US*.
Authentication:Protocol:String(6)	Enter the authentication protocol that you want to use. The only valid value is **RADIUS** (not case-sensitive).
Authentication:Shared Secret:String(128)	(Required only if you enter a value in the **Authentication:Protocol:String(6)** field) Enter a string with a maximum of 128 characters.
EnableKeyWrap:Boolean(true|false)	This field is enabled only if KeyWrap is supported in the network device. Enter **true** or **false**.
EncryptionKey:String(ascii:16|hexa:32)	(Required if you enable KeyWrap) Enter the encryption key that is used for session encryption. ASCII values: 16 characters (bytes) long. Hexadecimal values: 32 characters (bytes) long.
AuthenticationKey:String(ascii:20|hexa:40)	(Required if you enable KeyWrap.) Enter the keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages. ASCII values: 20 characters (bytes) long. Hexadecimal values: 40 characters (bytes) long.
InputFormat:String(32)	Enter the encryption and authentication keys input format. ASCII and hexadecimal values are accepted.
SNMP:Version:Enumeration (|2c|3)	Enter the version of the SNMP protocol that the profiler service must use—1, 2c, or 3.
SNMP:RO Community:String(32)	(Required if you enter a value in the **SNMP:Version:Enumeration (|2c|3)** field). Enter a string for Read Only Community with a maximum of 32 characters
SNMP:RW Community:String(32)	(Required if you enter a value in the **SNMP:Version:Enumeration (|2c|3)** field). Enter a string for Read Write Community with a maximum of 32 characters.
SNMP:Username:String(32)	Enter a string with a maximum of 32 characters.

Field	Usage Guidelines
	(Required if you enter SNMP version 3 in the **SNMP:Version:Enumeration (|2c|3)** field) Enter **Auth**, **No Auth**, or **Priv**.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	(Required if you have entered **Auth** or **Priv** for the SNMP security level.) Enter **MD5** or **SHA**.
SNMP:Authentication Password:String(32)	(Required if you have entered **Auth** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter a string with a maximum of 32 characters.
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	(Required if you have entered **Priv** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter **DES**, **AES128**, **AES192**, **AES256**, or **3DES**.
SNMP:Privacy Password:String(32)	(Required if you have entered **Priv** in the **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** field.) Enter a string with a maximum of 32 characters.
SNMP:Polling Interval:Integer:600-86400 seconds	Enter the SNMP polling interval, in seconds. A valid value is an integer from 600 to 86400.
SNMP:Is Link Trap Query:Boolean(true|false)	Enable or disable the SNMP link trap by entering **true** or **false**.
SNMP:Is MAC Trap Query:Boolean(true|false)	Enable or disable the SNMP MAC trap by entering **true** or **false**.
SNMP:Originating Policy Services Node:String(32)	Indicate which Cisco ISE server must be used to poll for SNMP data. It is automatic by default, but you can overwrite the setting by assigning different values in this field.
Trustsec:Device Id:String(32)	Enter a Cisco Trustsec device ID, which is a string with a maximum of 32 characters.
Trustsec:Device Password:String(256)	(Required if you have entered a Cisco TrustSec device ID.) Enter a Cisco TrustSec device password, which is a string with a maximum of 256 characters.
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec environment data download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec peer authorization policy download interval. A valid value is an integer from 1 to 2147040000.
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec reauthentication interval. A valid value is an integer from 1 to 2147040000.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	Enter the Cisco TrustSec security group ACL list download interval. A valid value is an integer from 1 to 2147040000.

Field	Usage Guidelines
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	Indicate whether a Cisco TrustSec device is trusted by entering **true** or **false**.
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	Notify Cisco TrustSec configuration changes to the Cisco TrustSec device by entering **ENABLE_ALL** or **DISABLE_ALL** .
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	Indicate if the Cisco TrustSec device is included in security group tag by entering **true** or **false**.
Deployment:Execution Mode Username:String(32)	Enter the user name that has privileges to edit the network device configuration. It is a string with a maximum of 32 characters.
Deployment:Execution Mode Password:String(32)	Enter the device password, which is a string with a maximum of 32 characters.
Deployment:Enable Mode Password:String(32)	Enter the password of the device that allows you to edit its configuration. It is a string with a maximum of 32 characters.
Trustsec:PAC issue date:Date	Enter the issuing date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Trustsec:PAC expiration date:Date	Etner the expiration date of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device.
Trustsec:PAC issued by:String	Enter the name of the issuer (a Cisco TrustSec administrator) of the last Cisco TrustSec PAC that was generated by Cisco ISE for the Cisco TrustSec device. It must be a string value.

Network Device Groups Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device Group CSV file.

Table 14: CSV Template Fields and Descriptions for Network Device Groups

Field	Description
Name:String(100):	(Required) This field is the network device group name. It is a string with a maximum of 100 characters in length. The full name of an NDG can have a maximum of 100 characters in length. For example, if you create a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you create would be Global#Asia#India. The full name cannot exceed 100 characters in length. If the full name of the NDG exceeds 100 characters in length, the NDG creation fails.
Description:String(1024)	This is an optional field. It is a string, with a maximum of 1024 characters in length.
Type:String(64):	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.

Field	Description
Is Root:Boolean(true|false):	(Required) This is a field that determines if the specific network device group is a root group. Valid value is true or false.

IPSec Security to Secure Communication Between Cisco ISE and NAD

IPSec is a set of protocols that provides security to IP. The AAA, RADIUS, and TACACS+ protocols use the MD5 hashing algorithm. For greater security, Cisco ISE offers the IPSec feature. IPSec provides secure communication by authenticating the sender, discovering any changes in data during transmission, and encrypting the data that is sent.

Cisco ISE supports IPSec in tunnel and transport modes. When you enable IPSec on a Cisco ISE interface and configure the peers, an IPSec tunnel is created between Cisco ISE and the NAD to secure the communication.

You can define a pre-shared key or use X.509 certificates for IPSec authentication. IPSec can be enabled on Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces. You can configure IPSec on only one Cisco ISE interface per PSN.

Smart licensing is enabled by default on Gigabit Ethernet 2 (e0/2—> eth2) interface. Hence, if you want to enable IP security on this interface, you must configure a different interface for smart licensing.

Note Gigabit Ethernet 0 and Bond 0 (when Gigabit Ethernet 0 and Gigabit Ethernet 1 interfaces are bonded) are management interfaces in the Cisco ISE CLI. IPSec is not supported on Gigabit Ethernet 0 and Bond 0.

Cisco ISE Releases 2.2 and later support IPSec.

Note the following points while configuring IPSec on Cisco ISE:

- Cisco ISE Releases 2.2 and later support IPSec.
- Cisco IOS Software, C5921 ESR Software (C5921_I86-UNIVERSALK9-M): The ESR 5921 configuration, by default, supports IPSec in tunnel and transport modes. Diffie-Hellman Group 14 and Group 16 are supported.

Note The C5921 ESR software is bundled with Cisco ISE, Releases 2.2 and later. You need an ESR license to enable it. See Cisco 5921 Embedded Services Router Integration Guide for ESR licensing information.

For more information on IPSec configuration, restrictions, and support, see the Security Configuration Guide, Cisco IOS XE Cupertino 17.7.x (Catalyst 9300 Switches).

Configure RADIUS IPSec on Cisco ISE

To configure RADIUS IPSec on Cisco ISE, you must:

Step 1 Configure IP address on the interface from the Cisco ISE CLI.

Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces (Bond 1 and Bond 2) support IPSec. However, IPSec can be configured only on one interface in a Cisco ISE node.

Step 2 Add a directly connected network device to the IPSec network device group.

Note RADIUS IPSec requires the static route gateway to be directly connected through an interface of the device.

a) Choose **Administration** > **Network Resources** > **Network Devices**.
b) In the **Network Devices** window, click **Add**.
c) Enter the name and IP address and subnet of the network device that you want to add in the corresponding fields.
d) From the IPSEC drop-down list, choose **Yes**.
e) Check the **RADIUS Authentication Settings** check box.
f) In the **Shared Secret** field, enter the shared secret key that you have configured on the network device.
g) Click **Submit**.

Step 3 (Optional; required only for Smart Licensing) Add a separate management interface to interact with the Cisco Smart Software Manager (CSSM). See Smart Software Manager satellite for information on Embedded Services Router (ESR). To do this, from the Cisco ISE CLI, run the following command to select the corresponding management interface (Gigabit Ethernet 1 to 5 (or Bond 1 or 2)):

ise/admin# **license esr smart** {*interface*}

This interface must be able to reach Cisco.com to access the Cisco online licensing server.

To disable ise/admin# **license esr smart** on an existing interface:

- Add a new management interface.
- Choose **Administration** > **System** > **Settings** > **Protocols** > **IPSec**. **Enable** and **Disable** IPSec on the new interface.

Step 4 Add a network device to a directly connected gateway from the Cisco ISE CLI.

ip route [*destination network*] [*network mask*] **gateway** [*next-hop address*]

Step 5 Activate IPSec on Cisco ISE nodes.

a) Choose **Administration** > **System** > **Settings** > **Protocols** > **IPSec**..

All the Cisco ISE nodes in the deployment are listed in this window.

b) Check the check box next to the Cisco ISE node on which you want to activate IPSec, and then click the **Enable** radio button.
c) Choose the interface that you want to use for IPSec communication from the **IPSec Interface for selected nodes:** drop-down list.
d) Click the radio button for one the following authentication type for the selected Cisco ISE node:

- **Pre-shared Key**: If you choose this option, you must enter the pre-shared key and configure the same key on the network device. Use alphanumeric characters for the pre-shared key. Special characters are not supported. For instructions on how to configure the pre-shared key on the network device, see the network device

documentation. For an example of the pre-shared key configuration output, see Example: Output of Pre-shared Key Configuration on Cisco Catalyst 3850 Series Switches, on page 43.

- **X.509 Certificates**: If you choose this option, from the Cisco ISE CLI, go to the ESR shell and configure and install X.509 Certificates for ESR 5921. Then, configure the network device for IPSec. For instructions, see Configure and Install X.509 Certificates on ESR-5921, on page 37.

e) Click **Save**.

Note You cannot modify IPSec configurations directly. To modify the IPSec tunnel or authentication when IPSec is enabled, disable the current IPSec tunnel, modify the IPSec configuration, and then re-enable the IPSec tunnel with a different configuration.

Note When enabled, IPSec removes the IP address from the Cisco ISE interface and shuts down the interface. When the user logs in from Cisco ISE CLI, the interface is displayed with no IP address and in shutdown state. This IP address will be configured on the ESR-5921 interface.

Step 6 Type **esr** to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

Note For FIPS compliance, you must configure a secret password that is at least eight characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

Note If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the configured RADIUS ports:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

Step 7 (Optional; required only if you have not enabled Smart Licensing in Step 3) Add a Cisco ISE Classic license or an Evaluation license (that is valid for 90 days) to the Cisco ISE appliances.

- Run the following command from the Cisco ISE CLI to download the license file:

  ```
  ise/admin# license esr classic import esr.lic repository esrrepo
  ```

  For more information on Cisco ISE Classic licensing, see the section: Licensing the Software with Classic Licensing in Cisco 5921 Embedded Services Router Integration Guide.

Step 8 Verify IPSec tunnel and RADIUS authentication over IPSec tunnel.

a) Add a user in Cisco ISE and assign the user to a user group (**Administration** > **Identity Management** > **Identities** > **Users**).

b) Carry out the following steps to verify if the IPSec tunnel is established between Cisco ISE and the NAD:

1. Use the **ping** command to test if Cisco ISE is connected to the NAD.
2. Run the following command from the ESR shell or the NAD CLI to verify if the connection is in the active state:

   show crypto isakmp sa

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.30.1    192.168.30.3    QM_IDLE           1001 ACTIVE
```

3. Run the following command from the ESR shell or the NAD CLI to verify if the tunnel is established:

   show crypto ipsec sa

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: radius, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={}
    #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
    #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x393783B6(959939510)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8EA0F6EE(2392913646)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237963/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x393783B6(959939510)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237970/2229)
        IV size: 16 bytes
        replay detection support: Y
```

```
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

c) Verify the RADIUS authentication using one of the following methods:

- Log in to the network device using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the **Live Authentications** window.
- Connect the end host with the network device and configure 802.1X authentication. Log in to the end host using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the **Live Authentications** window.

Configure and Install X.509 Certificates on ESR-5921

Step 1 Type **esr** to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE
 (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

Note For FIPS compliance, you must configure a secret password that is at least eight characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

Note If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the RADIUS ports that are configured:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

Step 2 Generate an RSA key pair using the following command:

Example:

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

Step 3 Create a trustpoint using the following command:

Example:

```
crypto pki trustpoint trustpoint-name
```

```
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

Step 4 Generate a certificate signing request using the following command:

Example:

```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

Step 5 Copy the output of the certificate signing request to a text file, submit it to an external CA for signing, and obtain the signed certificate and the CA certificate.

Step 6 Import the Certificate Authority (CA) certificate using the following command:

Example:

```
crypto pki authenticate rsaca-mytrustpoint
```

Copy and paste the contents of the CA certificate, including the "**—BEGIN—**" and "**—-End—**" lines.

Step 7 Import the signed certificate using the following command:

Example:

```
crypto pki import rsaca-mytrustpoint
```

Copy and paste the contents of the signed certificate, including the "**—BEGIN—**" and "**—-End—**" lines.

The following is an example of the output that is displayed when you configure and install X.509 Certificates on Cisco 5921 ESR:

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address
to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip cef
no ipv6 cef
!
```

```
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
  30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
  61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
  03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
  040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
  6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
  335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
  6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
  73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
  194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
  8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
  22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
  5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
  F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
  B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
  5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
  86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
  66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
```

```
  F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
  EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
  01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
  1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
  EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
  5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
  2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
  69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
  BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
  CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
  89AE82F6 A37E51D6 EECD
        quit
certificate ca 008DD3A81106B14664
  308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
  F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
  024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
  4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
  65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
  30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
  04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
  4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
  63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
  0382010F 00308201 0A028201 0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190
  16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225
  0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
  B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
  D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
  E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
  B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
  DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
  A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
  0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
  16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
  30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
  00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
  220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
  86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
  43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
  95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
  12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
  60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
  3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
  D0BD055F 65A8
        quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
!
redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
  address 0.0.0.0
  key-string
  quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
crypto isakmp policy 20
encr aes
hash sha256
group 14
```

```
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(s) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
```

The following is an example of the output that is displayed when you configure and install X.509 certificates on Cisco Catalyst 3850 Series Switches:

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!

crypto isakmp policy 10

encr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel

!

crypto ipsec profile radius-profile

!

crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius

match address 100

!

interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius

!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

key secret
```

Example: Output of Pre-shared Key Configuration on Cisco Catalyst 3850 Series Switches

The following is an example of the output that is displayed when you configure the pre-shared key on Cisco Catalyst 3850 Series Switches:

```
cat3850#show running-config

enable password lab
 !
 username lab password 0 lab
 aaa new-model
 !
 aaa group server radius ise
 server name ise-vm
 deadtime 60
 !
 aaa authentication login default group radius local

 aaa authentication enable default group radius enable

!

crypto isakmp policy 10

 encr aes

 hash sha256
 authentication pre-share
 group 16
 crypto isakmp key 123456789 address 0.0.0.0
 !
 crypto ipsec security-association lifetime seconds 86400
 !
 crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
 !
 crypto ipsec profile radius-profile
 !
 crypto map radius 10 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set radius
 match address 100
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.20.2 255.255.255.0

 crypto map radius
!
 access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
 !
 snmp-server community public RO
 snmp-server community private RW
 !
 radius server rad-ise
 address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

 key secret
```