CHAPTER 6

Managing Network Devices

This chapter describes how to manage the devices in your network. This chapter contains the following sections:

Managing Network Devices

A network device is an authentication, authorization, and accounting (AAA) client through which AAA service requests are attempted, for example, switches, routers, and so on. The network device definition enables the Cisco Identity Services Engine (ISE) to interact with the network devices that are configured. A network device that is not defined in ISE cannot receive AAA services from ISE.

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

When ISE receives a RADIUS 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 it does not find the device definition, it obtains the shared secret from the default network device and processes the request. If the shared secrets match, network access is granted. A passed authentication report is generated. If they do not match, a reject response is sent to the device. A failed authentication report is generated, which provides the failure reason.

ISE allows you to configure authentication and authorization policies based on device attributes such as device type, location, model name, and so on, which are available in the device dictionary. When you create a new network device group (NDG), a new device attribute is added to the dictionary, which you can use in policy definitions.

The network device definition must include the following:

- Device Name—The device name is a descriptive name that you can provide to the network device. It can be different from the hostname of the device. The device name is a logical identifier.
- IP Address and Subnet Mask—You must specify an IP address and a subnet mask. The following are some guidelines that must be followed while defining the IP addresses and subnet masks:
  - You can define a specific IP address, or a range with a subnet mask.
  - 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.

Note 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.

  When ISE receives a RADIUS request and tries to match the request against a network device, it does the following:

  a. It looks for a specific IP address that matches the one in the request.
  b. It looks up the ranges to see if the IP address in the request falls within the range that is specified.
  c. If both of these fail, it uses the default device definition (if defined) to process the request.

- Network Device Group—NDGs allow you to group devices based on location, type, and other groupings and allow you to define policy conditions based on these groupings. If you do not specifically assign a device to a group when you configure it, it becomes a part of the default All Locations and All Device Types device groups. See the "Managing Network Device Groups" section on page 6-10 for more information.

The following are optional settings that you can define for a network device:

- Model Name—The model name identifies the model of the network device. For example, CAT 6K, Nexus 7K, and so on. You can 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—The version of the software that is running on the network device. For example, Cisco IOS version 12.3, 12.3 (2), and so on. 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.

In addition, you can configure the following settings for network devices:

- Authentication Settings—Configure this setting for RADIUS authentications.
- Simple Network Management Protocol (SNMP) Settings—Configure this setting for the Profiler service in ISE to profile the end points. The ISE Profiler service can communicate with network devices that have SNMP settings defined. The Profiler service uses these settings to initiate SNMP-based communication with the device and obtains device-related information for monitoring purposes.
- Security Group Access (SGA) Settings—For devices that can be part of the Cisco Security Group Access solution. Any switch that supports the SGA solution is an SGA device. For example, the Nexus 7000 Series Switches, Catalyst 6000 Series Switches, Catalyst 4000 Series Switches, Catalyst 3000 Series Switches, and so on. SGA devices are authenticated using the SGA settings that you must define while adding SGA devices. See Chapter 22, "Configuring Cisco Security Group Access Policies" for more information on SGA settings.

You can also generate SGA PAC (Protected Access Credentials) by clicking the **Generate PAC** button. See the "Generating an SGA PAC from the Network Devices List Screen" section on page 22-33 for more information.

- Device Configuration Details—Credentials to edit the configuration of a network device.

You can configure these network devices manually or import a list of devices into ISE using a .csv file.

This section contains the following topics:

Adding and Editing Devices

You can add devices or edit the device definition in the ISE server.

Prerequisites:

- Before you begin this task, you should have a basic understanding of network devices and how they are managed in ISE. See the "Managing Network Devices" section on page 6-1 for more information.
- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add or edit a device, complete the following steps:

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

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears with a list of configured devices.

Step 3 Click **Add**, or check the check box next to a device and click **Edit** to edit it or click **Duplicate** to create a duplicate entry. You can alternatively click **Add new device** from the action icon on the Network Devices navigation pane or click a device name from the list to edit it.

Step 4 In the right pane, enter the values as described in Table 6-1.

Step 5 Check the **Authentication Settings** check box and define the following RADIUS authentication settings:

- Shared Secret—The shared secret can be up to 128 characters in length. The shared secret is the key that you have configured on the device using the **radius-host** command with the **pac** option.
- Enable KeyWrap—This option increases RADIUS protocol security via an AES KeyWrap algorithm to help enable FIPS 140-2 compliance in Cisco ISE.
- Key Encryption Key—This key is used for session encryption (secrecy).

- Message Authenticator Code Key—This key is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
- Key Input Format—Specify the format you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below; shorter values are not permitted.)
  - ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.
  - Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.

Step 6 Check the **SNMP** check box to configure SNMP settings on the device. These settings are used by the Profiler service in ISE. Enter the values as described in Table 6-2.

For information on switch-related SNMP settings, see:

- Enable SNMP Traps, page C-8
- Enable SNMP v3 Query for Profiling, page C-8

Step 7 Check the **Security Group Access (SGA)** check box to configure an SGA device. SGA devices do not use the IP address. Instead, you must define other settings so that SGA devices can communicate with ISE. Enter the values as described in Table 22-4.

Step 8 Check the **Device Configuration Deployment** check box to enter user credentials to edit the configuration of the device. Enter the values as described in Table 6-3.

Step 9 Click **Submit** to save the device definition.

Network Devices Page

Table 6-1 lists the fields in the Network Devices page and their descriptions.

Table 6-1 Network Devices Page

Field	Description
Name	(Required) This field is the name of the device. **Note** You cannot edit the name of a device.
Description	This field is the description of the device.
IP Address	(Required) This field includes the IP address and subnet masks that are associated with the device. A single address or a range, the routable IP address should be one with which the ISE appliance can communicate.
Model Name	This field is the device model, for example, the Cisco Catalyst 6K, the Cisco Nexus 7K, and so on.
Software Version	This field is the version of the software on the device, for example, Version 12.2, 12.3, and so on.
Network Device Group	(Required) From the Location and Device Type drop-down list boxes, choose a location and device type to associate with the device. **Note** If you do not choose a device group, the default device groups (root NDGs) are assigned.

Network Devices: SNMP Settings

Table 6-2 lists the SNMP settings in the Network Devices page and their descriptions.

Table 6-2 Network Devices List Page: SNMP Settings

Field	Description
SNMP Version	(Required) This setting is the version of SNMP to be used for requests. Valid options are: • 1—SNMPv1 does not support informs. • 2c • 3—SNMPv3 is the most secure model because it allows packet encryption when you choose the Priv security level. **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report that is provided by the Monitoring service (**Operations > Reports > Catalog > Network Device > Session Status Summary**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Required if you choose SNMP version 1 or 2c) This setting is the Read Only community string. A community string is similar to a password and it provides ISE with a particular type of access to the device.
SNMP Username	(Required if you choose SNMP version 3) This setting is the SNMPv3 username.
Security Level	(Required if you choose SNMP version 3) Choose the security level for SNMPv3. Valid options are the following: • Auth—Enables MD5[1] or Secure Hash Algorithm (SHA) packet authentication • No Auth—No authentication and no privacy security level • Priv—Enables DES[2] packet encryption
Auth Protocol	This setting is the authentication protocol that you want the device to use. Valid options are MD5 or SHA1.
Auth Password	Enter the authentication key. The authentication key must be at least 8 characters in length.
Privacy Protocol	This setting is the privacy protocol that you want the device to use. Valid options are DES, AES128, AES192, AES256, and 3DES.
Privacy Password	Enter the privacy key.
Polling Interval	This setting is the SNMP polling interval in seconds. Default is 3600 seconds.
Link Trap Query	Check this check box for the profiler service to query the device, if it receives the link trap from the NAD[3] connected to the device.

Table 6-2 Network Devices List Page: SNMP Settings (continued)

Field	Description
MAC Trap Query	Check this check box for the profiler service to query the device, if it receives the MAC trap from the NAD connected to the device.
Originating Policy Services Node	This setting indicates which server to use to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.

[1] MD5 = Message Digest 5.

[2] DES = Data Encryption Standard.

[3] NAD = Network Access Device

Network Devices: Device Configuration Deployment Settings

Table 6-3 Network Devices Page: Device Configuration Deployment Settings

Field	Description
Exec Mode Username	Enter the username that has privileges to edit the device configuration.
Exec Mode Password	Enter the device password.
Enable Mode Password	Enter the enable password for the device that would allow you to edit its configuration.

For more information:

- Managing Network Devices, page 6-1
- Managing Network Device Groups, page 6-10
- Importing Network Devices and Network Device Groups, page 6-14
- Exporting Network Devices and Network Device Groups, page 6-21

Deleting a Device

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete network devices, complete the following steps:

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

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices List page appears.

Step 3 Check the check boxes next to the devices that you want to delete and click **Delete > Delete Selected**. You can alternatively choose the network device listed in the navigation pane on the left and from the action icon (⚙), and click **Delete device**.

Note You can click Delete > Delete All to delete all the devices that you have defined.

A dialog box appears with the following message:

Are you sure you want to delete "*Device name*"?

Step 4 Click **OK** to delete the device.

Filtering Network Devices on the Network Devices Page

You can use the Show drop-down list, or click the filter icon to both invoke a quick filter and close it on the Network Devices page. A quick filter is a simple filter that you can use to filter network devices based on field descriptions, such as the name of network devices, description, location, type, and an IP/Mask on the Network Devices page. Filtering network devices by a single IP address is an exclusive filter that disables all other filter fields in the quick filter.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the Network Devices page. The advanced filter filters network devices based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter. Filtering network devices by a single IP address is an exclusive filter and no other fields can be simultaneously used for filtering in the advanced filter.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved, you can choose a preset filter from the list of filtered results on the Network Devices page. A preset filter has a session lifetime, which displays the filtered results on the Network Devices page. You can also edit preset filters and remove them from the preset filters list.

To filter network devices, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices** (menu window).

The Network Devices menu appears.

Step 2 From the Network Devices menu window, choose **Network Devices**.

The Network Devices page appears, which lists all the network devices.

Step 3 From the Network Devices page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 6-4.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 6-8 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 6-8.

Note To return to the network devices list, choose **All** from the Show drop-down list to display all the network devices without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters network devices based on each field description except the IP/Mask field on the Network devices page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Network Devices page. If you clear the field, it displays the list of all the network devices on the Network devices page. Filtering by IP/Mask disables all other fields in the quick filter.

Step 1 To filter, click the **Go** button within each field to refresh the page with the results that are displayed on the Network Devices page.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter network devices by using variables that are more complex. It contains one or more filters that filter network devices based on the values that match the field descriptions. A filter on a single row filters network devices based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter network devices by using any one or all of the filters within a single advanced filter. Filtering by IP/Mask disables filtering with all other fields simultaneously in the advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

If IP/Mask is selected, then no other filters can be used for simultaneous filtering in the advanced filter.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save.** Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Table 6-4 describes the fields that allow you to filter the network devices on the Network Devices page.

Table 6-4 Filtering Network Devices

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter network devices by the name of the network device.
	IP/Mask	This field enables you to filter network devices by a single IP address. Filtering by part of an IP address can yield many records, and the results includes all IP addresses with that part of the IP address.
	Location	This field enables you to filter network devices by the location of the network device.
	Type	This field enables you to filter network devices by the type of the network device.
	Description	This field enables you to filter network devices by the description of the network device.
Advanced Filter	Choose the field description from the following: • Name • IP/Mask • Location • Type • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter network devices.
	Value	From the Value field, choose the value for the field description that you selected against which the network devices are filtered.

Configuring a Default Device

You can use the default device definition when no specific device definition is found for a RADIUS request.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define a default device, complete the following steps:

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

Step 2 From the Network Devices navigation pane on the left, click **Default Device**.

The Default Network Device page appears.

Step 3 To enable the default network device definition, choose **Enable** from the Default Network Device Status drop-down list box.

Step 4 Define the following RADIUS authentication settings:

- Shared Secret—The shared secret can be up to 128 characters in length. The shared secret is the key that you have configured on the device using the **radius-host** command with the **pac** option.
- Enable KeyWrap—This option increases RADIUS protocol security via an AES KeyWrap algorithm to help enable FIPS 140-2 compliance in Cisco ISE.
- Key Encryption Key—This key is used for session encryption (secrecy).
- Message Authenticator Code Key—This key is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
- Key Input Format—Specify the format you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below; shorter values are not permitted.)
  - ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.
  - Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.

Step 5 Click **Save** to save the default network device definition.

Result:

A dialog box appears with the following message:

The configuration was saved successfully.

For more information, see the "Managing Network Devices" section on page 6-1.

Managing Network Device Groups

A device group is a hierarchical structure that contains the network device groups (NDGs). NDGs logically group the devices based on various criteria such as location or device type. When you create a root NDG node, you must provide the name and the type of the NDG. For all subsequent child NDG nodes, you will need to provide only the name. The type is inherited from the parent NDG and hence all the child NDG nodes under a root NDG will be of the same type.

ISE allows you to create hierarchical NDGs. Thus, a device can be part of multiple NDGs. For example, you can group devices by continent, region, and country such as the following:

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

You can also group devices by device types such as the following:

- Africa -> Southern -> Botswana -> Firewalls
- Africa -> Southern -> Botswana -> Routers

- Africa -> Southern -> Botswana -> Switches

You can use NDGs in policy conditions. There are two predefined root NDGs in ISE (Location and Device Type). You cannot edit or delete these predefined NDGs. Devices can be assigned to a single NDG. After you create an NDG, you can use it while defining policies. When you create a new root NDG, a new device attribute is added to the dictionary. You can use this attribute in authentication and authorization policies.

Note The device type of the root NDG is available as an attribute in the device dictionary. You can define conditions based on this attribute. The name of the NDG is one of the values that this attribute can take.

This section contains the following topics:

- Creating a Network Device Group, page 6-11
- Editing a Network Device Group, page 6-12
- Deleting a Network Device Group, page 6-13
- Import Network Device Groups into ISE, page 6-19
- Exporting Network Device Groups, page 6-22

Creating a Network Device Group

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create an NDG, complete the following steps:

Note Default NDGs (All Locations and All Device Types) cannot be edited, but you can add new device subgroups under them.

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

From the Network Device Groups navigation pane on the left, click **Group Types**.

The Network Device Groups page appears.

Step 2 Do one of the following:

- To create a root NDG, click **Add**.
- To create a child NDG, from the navigation pane on the left, choose a group to which you want to add a child NDG, and click **Add**.

Step 3 In the right-side pane, enter the following information:

- (Required) Name of the NDG. This name appears in the navigation pane.

  The full name of an NDG can have a maximum of 100 characters. For example, if you are creating a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name should not exceed 100 characters. If the full name of the NDG exceeds 100 characters, the NDG creation fails.

- An optional description.
- (Required) Type of NDG. If this NDG is a root NDG, then this device type will be available as an attribute in the device dictionary. If this NDG is a child NDG, then the name of the parent NDG should appear in this field.

Step 4 Click **Save** to save the NDG configuration.

Result:

On successful creation of the NDG, a pop-up appears at the right bottom corner of your screen with the following message: *NDG_name* has been saved successfully.

Related Topics

- Managing Network Devices, page 6-1
- Editing a Network Device Group, page 6-12
- Deleting a Network Device Group, page 6-13

Editing a Network Device Group

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To edit an NDG, complete the following steps:

Note You cannot edit the predefined Location and Device Type NDGs.

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

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups listing page appears.

Step 3 From the Group Types navigation pane on the left, choose the parent NDG whose child NDG you want to edit.

The Network Device Group listing page appears with a list of child NDGs.

Step 4 Check the check box next to the NDG that you want to edit and click **Edit**.

Step 5 Edit the NDG name or description or both.

You cannot edit the NDG type.

Step 6 Click **Save** to save the changes.

Result:

On successful completion of the edit process, a pop-up appears at the right bottom corner of your screen with the following message: *NDG_name* has been saved successfully.

Related Topics

- Managing Network Devices, page 6-1
- Creating a Network Device Group, page 6-11
- Deleting a Network Device Group, page 6-13

Deleting a Network Device Group

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete an NDG, complete the following steps:

Note You cannot delete an NDG that has a subgroup under it.

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

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups listing page appears.

Step 3 From the Group Types navigation pane on the left, choose the parent NDG whose child NDG you want to delete.

The Network Device Group listing page appears with a list of child NDGs.

Step 4 Check the check box next to the NDG that you want to delete and click **Delete**. Alternatively, you can choose the child NDG that you want to delete from the navigation pane on the left and click **Delete Group** from the action icon.

A dialog box appears with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the NDG.

Result:

On successful completion of the delete process, a pop-up appears at the right bottom corner of your screen with the following message: Group was deleted successfully.

Related Topics

- Managing Network Devices, page 6-1
- Creating a Network Device Group, page 6-11

- Editing a Network Device Group, page 6-12

Importing Network Devices and Network Device Groups

ISE allows you to import a large number of network devices and network device groups using comma-separated value (.csv) files. While importing devices and device groups, you can create new records or update existing records. You can download the .csv import template from the ISE user interface, enter your device or device group details in the template, and save it as a .csv file, which you can then import back into ISE. When you configure an import job, you can also define whether you want ISE to overwrite the existing device definitions with the new definitions or stop the import process when it encounters the first error.

After an import job has begun, you can view the status of the job in the ISE user interface. You cannot run two import jobs of the same resource type at the same time. For example, you cannot concurrently run two import jobs to import network devices from two different import files.

To import devices into ISE, you must complete the following tasks:

1. Download the Import File Template, page 6-14
2. Create the CSV Import File, page 6-15
3. Import Devices into ISE, page 6-18 or Import Network Device Groups into ISE, page 6-19

Download the Import File Template

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To download the import file template, complete the following steps:

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

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears.

Note If you want to download the template for Network Device Groups, then choose **Administration > Network Resources > Network Device Groups** and from the navigation pane on the left, and click **Group Types**.

Step 3 Click **Import**.

The Import page appears.

Step 4 Click **Generate a Template**.

Step 5 Save the template file to your local hard disk.

Result:

The template is downloaded to your local hard disk.

Create the CSV Import File

You must first create the CSV import file before you can import it into ISE.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create the CSV import file, complete the following steps:

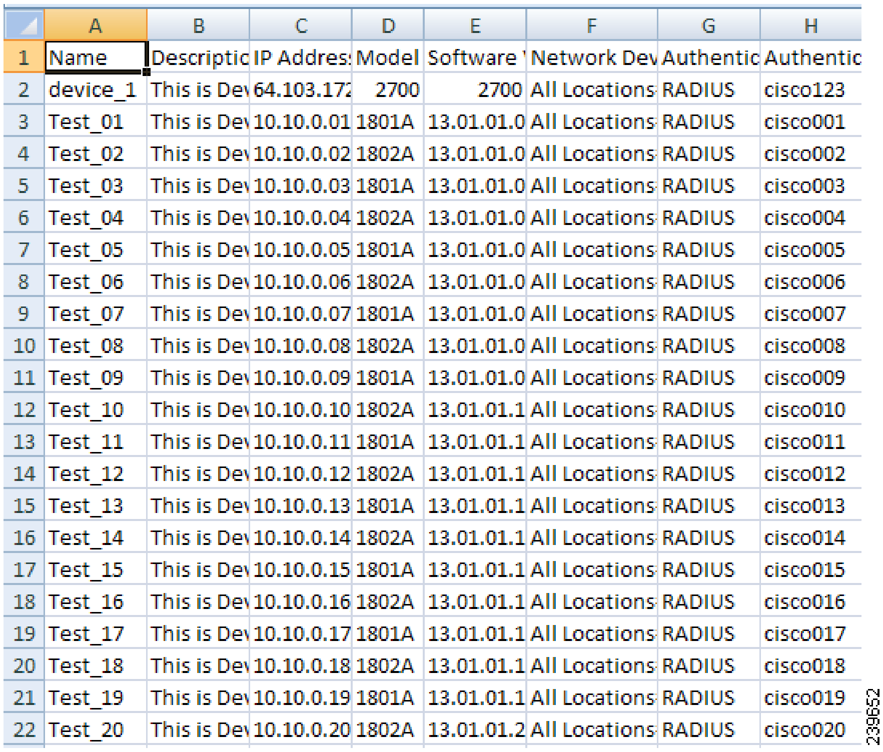
Step 1 Open the CSV template that you downloaded using Microsoft Excel or any spreadsheet application.

The first line in your CSV template is the header and it defines the format of the fields in the file. This header should not be edited and should be used as is.

- Table 6-5 lists the fields in the header and provides a description of the fields in the Network Device CSV file template.
- Table 6-6 lists the fields in the header and provides a description of these fields in the Network Device Group CSV file template.

Step 2 Enter the data for your network devices as shown in Figure 6-1 or network device groups as shown in Figure 6-2.

Figure 6-1 Sample CSV File for Importing Network Devices



	A	B	C	D	E	F	G	H
1	Name	Descriptic	IP Addres:	Model	Software '	Network Dev	Authentic	Authentic
2	device_1	This is Dev	64.103.172	2700	2700	All Locations	RADIUS	cisco123
3	Test_01	This is Dev	10.10.0.01	1801A	13.01.01.0	All Locations	RADIUS	cisco001
4	Test_02	This is Dev	10.10.0.02	1802A	13.01.01.0	All Locations	RADIUS	cisco002
5	Test_03	This is Dev	10.10.0.03	1801A	13.01.01.0	All Locations	RADIUS	cisco003
6	Test_04	This is Dev	10.10.0.04	1802A	13.01.01.0	All Locations	RADIUS	cisco004
7	Test_05	This is Dev	10.10.0.05	1801A	13.01.01.0	All Locations	RADIUS	cisco005
8	Test_06	This is Dev	10.10.0.06	1802A	13.01.01.0	All Locations	RADIUS	cisco006
9	Test_07	This is Dev	10.10.0.07	1801A	13.01.01.0	All Locations	RADIUS	cisco007
10	Test_08	This is Dev	10.10.0.08	1802A	13.01.01.0	All Locations	RADIUS	cisco008
11	Test_09	This is Dev	10.10.0.09	1801A	13.01.01.0	All Locations	RADIUS	cisco009
12	Test_10	This is Dev	10.10.0.10	1802A	13.01.01.1	All Locations	RADIUS	cisco010
13	Test_11	This is Dev	10.10.0.11	1801A	13.01.01.1	All Locations	RADIUS	cisco011
14	Test_12	This is Dev	10.10.0.12	1802A	13.01.01.1	All Locations	RADIUS	cisco012
15	Test_13	This is Dev	10.10.0.13	1801A	13.01.01.1	All Locations	RADIUS	cisco013
16	Test_14	This is Dev	10.10.0.14	1802A	13.01.01.1	All Locations	RADIUS	cisco014
17	Test_15	This is Dev	10.10.0.15	1801A	13.01.01.1	All Locations	RADIUS	cisco015
18	Test_16	This is Dev	10.10.0.16	1802A	13.01.01.1	All Locations	RADIUS	cisco016
19	Test_17	This is Dev	10.10.0.17	1801A	13.01.01.1	All Locations	RADIUS	cisco017
20	Test_18	This is Dev	10.10.0.18	1802A	13.01.01.1	All Locations	RADIUS	cisco018
21	Test_19	This is Dev	10.10.0.19	1801A	13.01.01.1	All Locations	RADIUS	cisco019
22	Test_20	This is Dev	10.10.0.20	1802A	13.01.01.2	All Locations	RADIUS	cisco020

Step 3 Save the .csv file.

Description of the Fields in the Network Device CSV Template

Table 6-5 CSV Template Fields and Description

Field	Description
Name:String(32):Required	(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters.
Description:String(256)	This field is an optional description for the network device. A string, with a maximum of 256 characters.
IP Address:Subnets(a.b.c.d/m|...):Required	(Required) This field is the IP address and subnet mask of the network device (can take on more than one value separated by a pipe “|” symbol).
Model Name:String(32):Required	(Required) This field is the network device model name. It is a string, with a maximum of 32 characters.
Software Version:String(32):Required	(Required) This field is the network device software version. It is a string, with a maximum of 32 characters.
Network Device Groups:String(100):Required	(Required) This field should be an existing network device group. It can be a subgroup, but must include both the parent and subgroup separated by a space. It is a string, with a maximum of 100 characters, for example, Location#All Location#US
Authentication:Protocol:String(6)	This is an optional field. It is the protocol that you want to use for authentication. The only valid value is RADIUS (not case sensitive).
Authentication:Shared Secret:String(128)	(Required if you have entered a value for the Authentication Protocol field) This is a string, with a maximum of 128 characters.
SNMP:Version:Enumeration (1|2c|3)	This is an optional field, used by the Profiler service. It is the version of the SNMP protocol. Valid values are 1, 2c, or 3.
SNMP:RO Community:String(32)	(Required if you have entered a value for the SNMP Version field) SNMP RO Community. It is a string, with a maximum of 32 characters.
SNMP:RW Community:String(32)	(Required if you have entered a value for the SNMP Version field) SNMP RW Community. It is a string, with a maximum of 32 characters.
SNMP:Username:String(32)	This is an optional field. It is a string, with a maximum of 32 characters.
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)	(Required if you have chosen SNMP version 3) Valid values are Auth, No Auth, Priv.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	(Required if you have entered Auth or Priv for the SNMP security level) Valid values are MD5 or SHA.
SNMP:Authentication Password:String(32)	(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters.

Table 6-5 CSV Template Fields and Description (continued)

Field	Description
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	(Required if you have entered Priv for the SNMP security level) Valid values are DES, AES128, AES192, AES256, or 3DES.
SNMP:Privacy Password:String(32)	(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters.
SNMP:Polling Interval:Integer:600-86400 seconds	This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.
SNMP:Is Link Trap Query:Boolean(true|false)	This is an optional field to enable or disable the SNMP link trap. Valid values are true or false.
SNMP:Is MAC Trap Query:Boolean(true|false)	This is an optional field to enable or disable the SNMP MAC trap. Valid values are true or false.
SGA:Device Id:String(32)	This is an optional field. It is the security group access device ID, and is a string, with a maximum of 32 characters.
SGA:Device Password:String(256)	(Required if you have entered SGA device ID) It is the security group access device password and is a string, with a maximum of 256 characters.
SGA:Environment Data Download Interval:Integer	This is an optional field. It is the security group access environment data download interval. Valid value is an integer between 1 and 24850.
SGA:Peer Authorization Policy Download Interval:Integer	This is an optional field. It is the security group access peer authorization policy download interval. Valid value is an integer between 1 and 24850.
SGA:Reauthentication Interval:Integer	This is an optional field. It is the security group access reauthentication interval. Valid value is an integer between 1 and 24850.
SGA:SGACL List Download Interval:Integer	This is an optional field. It is the security group access SGACL list download interval. Valid value is an integer between 1 and 24850.
SGA:Is Other SGA Devices Trusted:Boolean(true|false)	This is an optional field. Indicates whether security group access is trusted or not. Valid value is true or false.
SGA:Is Device Included on SGT Mapping:Boolean(true|false)	This is an optional field. It is the security group access device included on SGT. Valid value is true or false.
Deployment:Execution Mode Username:String(32)	This is an optional field. It is the username that has privileges to edit the device configuration. It is a string, with a maximum of 32 characters.
Deployment:Execution Mode Password:String(32)	This is an optional field. It is the device password and is a string, with a maximum of 32 characters.
Deployment:Enable Mode Password:String(32)	This is an optional field. It is the enable password of the device that would allow you to edit its configuration and is a string, with a maximum of 32 characters.

For a detailed description of each of these fields, see Table 6-1, Table 6-2, Table 22-4, and Table 6-3.

Result:

You now have the .csv file to begin the import process.

Related Topics

- Importing Network Devices and Network Device Groups, page 6-14
- Import Devices into ISE, page 6-18

Import Devices into ISE

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

After you have created your .csv import file, complete the following steps:

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

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears.

Step 3 Click **Import**.

The Import page appears.

Step 4 Click **Browse** to choose the .csv file from the system that is running the client browser.

Step 5 Check or uncheck the following options:

a. Overwrite Existing Data with New Data—Check this check box if you want ISE 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.

b. Stop Import on First Error—Check this check box if you want ISE to discontinue the import process when it encounters an error in the import process. The records that were processed until that time are imported. If this check box is not checked and an error is encountered, the error is reported and ISE continues the import process.

Step 6 Click **Import**.

The Import Progress window appears and provides the status of the import process. The page appears with a summary of the number of devices that are imported and also reports any errors that were found during the import process.

Step 7 Click **Network Devices** from the navigation pane or the **Network Devices List** link at the top of this screen to view the imported devices.

Result:

On successful completion of the import process, a dialog box appears with the “Import Completed” message.

Import Network Device Groups into ISE

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To import NDGs, complete the following steps:

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

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups page appears.

Step 3 Click **Import**. You can alternatively click **Import** from the action icon on the navigation pane.

The Import page appears.

Step 4 Click **Generate a Template** to download the template for creating the import file.

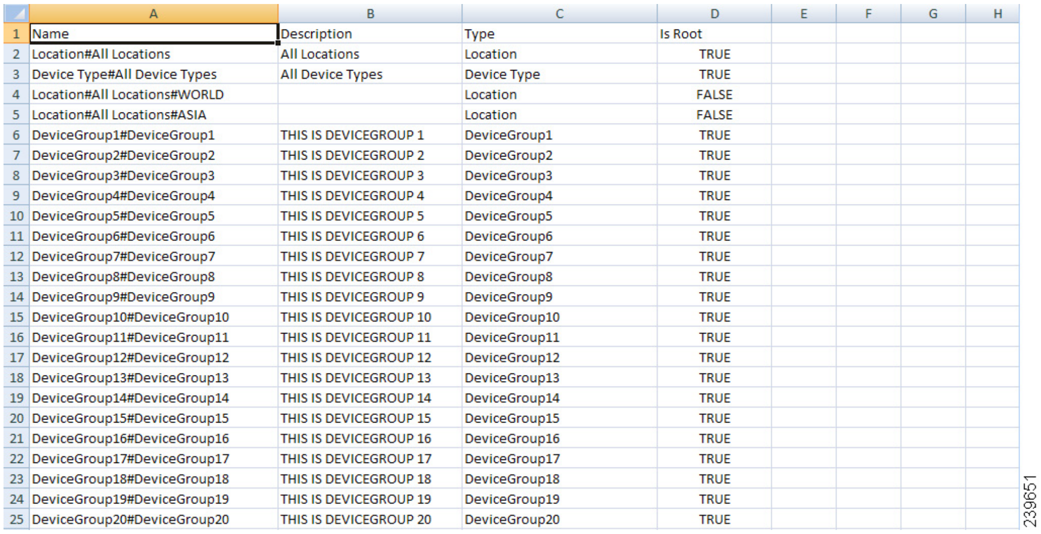
Step 5 Save the template to your local hard disk.

Step 6 Open this template in Microsoft Excel or any spreadsheet application.

The first line in your CSV template is the header and it defines the format of the fields in the file. This header should not be edited and should be used as is.

Step 7 Enter the details as shown in Figure 6-2.

Figure 6-2 NDG Import File



	A	B	C	D	E	F	G	H
1	Name	Description	Type	Is Root				
2	Location#All Locations	All Locations	Location	TRUE				
3	Device Type#All Device Types	All Device Types	Device Type	TRUE				
4	Location#All Locations#WORLD		Location	FALSE				
5	Location#All Locations#ASIA		Location	FALSE				
6	DeviceGroup1#DeviceGroup1	THIS IS DEVICEGROUP 1	DeviceGroup1	TRUE				
7	DeviceGroup2#DeviceGroup2	THIS IS DEVICEGROUP 2	DeviceGroup2	TRUE				
8	DeviceGroup3#DeviceGroup3	THIS IS DEVICEGROUP 3	DeviceGroup3	TRUE				
9	DeviceGroup4#DeviceGroup4	THIS IS DEVICEGROUP 4	DeviceGroup4	TRUE				
10	DeviceGroup5#DeviceGroup5	THIS IS DEVICEGROUP 5	DeviceGroup5	TRUE				
11	DeviceGroup6#DeviceGroup6	THIS IS DEVICEGROUP 6	DeviceGroup6	TRUE				
12	DeviceGroup7#DeviceGroup7	THIS IS DEVICEGROUP 7	DeviceGroup7	TRUE				
13	DeviceGroup8#DeviceGroup8	THIS IS DEVICEGROUP 8	DeviceGroup8	TRUE				
14	DeviceGroup9#DeviceGroup9	THIS IS DEVICEGROUP 9	DeviceGroup9	TRUE				
15	DeviceGroup10#DeviceGroup10	THIS IS DEVICEGROUP 10	DeviceGroup10	TRUE				
16	DeviceGroup11#DeviceGroup11	THIS IS DEVICEGROUP 11	DeviceGroup11	TRUE				
17	DeviceGroup12#DeviceGroup12	THIS IS DEVICEGROUP 12	DeviceGroup12	TRUE				
18	DeviceGroup13#DeviceGroup13	THIS IS DEVICEGROUP 13	DeviceGroup13	TRUE				
19	DeviceGroup14#DeviceGroup14	THIS IS DEVICEGROUP 14	DeviceGroup14	TRUE				
20	DeviceGroup15#DeviceGroup15	THIS IS DEVICEGROUP 15	DeviceGroup15	TRUE				
21	DeviceGroup16#DeviceGroup16	THIS IS DEVICEGROUP 16	DeviceGroup16	TRUE				
22	DeviceGroup17#DeviceGroup17	THIS IS DEVICEGROUP 17	DeviceGroup17	TRUE				
23	DeviceGroup18#DeviceGroup18	THIS IS DEVICEGROUP 18	DeviceGroup18	TRUE				
24	DeviceGroup19#DeviceGroup19	THIS IS DEVICEGROUP 19	DeviceGroup19	TRUE				
25	DeviceGroup20#DeviceGroup20	THIS IS DEVICEGROUP 20	DeviceGroup20	TRUE				

Step 8 Save the import file to your local hard disk.

Step 9 Click **Browse** from the Import page to choose your import file.

Step 10 Check or uncheck the following options:

a. Overwrite Existing Data with New Data—Check this check box if you want ISE to replace the existing network device groups with the device groups in your import file. If you do not check this check box, new network device group definitions that are available in the import file are added to the network device group repository. Duplicate entries are ignored.

b. Stop Import on First Error—Check this check box if you want ISE to discontinue the import process when it encounters an error in the import process. The records that were processed until that time are imported. If this check box is not checked and an error is encountered, the error is reported and ISE continues the import process.

Step 11 Click **Import**.

The import progress is displayed on the screen and the result appears at the end of the import process.

Description of Fields in the Network Device Groups CSV Template

Table 6-6 Network Device Groups CSV Template Fields

Field	Description
Name:String(100):Required	(Required) This field is the network device group name. It is a string with a maximum of 100 characters. The full name of an NDG can have a maximum of 100 characters. For example, if you are creating a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name should not exceed 100 characters. If the full name of the NDG exceeds 100 characters, the NDG creation fails.
Description:String(1024)	This is an optional network device group description. It is a string, with a maximum of 1024 characters.
Type:String(64):Required	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters.
Is Root:Boolean(true|false):Required	(Required) This is a field that determines if the specific network device group is a root group or not. Valid value is true or false.

Related Topics

- Importing Network Devices and Network Device Groups, page 6-14
- Create the CSV Import File, page 6-15

Exporting Network Devices and Network Device Groups

You can export the list of network devices and network device groups configured in Cisco ISE in the form of a .csv file that you can import into another ISE node.

This section contains the following topics:

- Exporting Network Devices, page 6-21
- Exporting Network Device Groups, page 6-22

Exporting Network Devices

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To export the network device configuration, complete the following steps:

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

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears with a list of device configurations.

Step 3 Check the check boxes next to the devices that you want to export, and choose **Export > Export Selected**.

Note To export all the network devices that are defined, choose **Export > Export All**.

Step 4 Save the export.csv file to your local hard disk.

Result:

You have your network device configuration in the form of a .csv file that you can import into another ISE node.

Exporting Network Device Groups

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To export network device groups, complete the following steps:

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

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups page appears.

Step 3 Click **Export**. Alternatively, you can click **Export** from the action icon on the navigation pane.

Step 4 Save the export.csv file to your local hard disk.

Result:

You have exported the network device group configuration from an ISE node, which can now be imported into another ISE node.