Managing Network Devices

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

- Managing Network Devices, page 6-1
- Managing Network Device Groups, page 6-7
- Importing Network Devices and Device Groups, page 6-11
- Exporting Network Devices and Network Device Groups, page 6-18

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 (Cisco ISE) to interact with the network devices that are configured. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

You can also define a default network device that Cisco ISE can use if it does not find the device definition for a particular IP address. Cisco 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 Cisco 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.

Cisco 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 Cisco 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 6-7 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 Cisco 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 21, “Configuring Cisco Security Group Access Policies” for more information on SGA settings.
Chapter 6      Managing Network Devices

Adding and Editing Devices

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

Prerequisites:

- Before you begin this task, you should have a basic understanding of network devices and how they are managed in Cisco ISE. See the “Managing Network Devices” section on page 6-1 for more information.
- Every Cisco 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 a shared secret for RADIUS authentications. 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 pas option.

Check the SNMP check box to configure SNMP settings on the device. These settings are used by the Profiler service in Cisco 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
Chapter 6  Managing Network Devices

Step 6  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 Cisco ISE. Enter the values as described in Table 21-4.

Step 7  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 8  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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) This field is the name of the device.</td>
</tr>
<tr>
<td>Description</td>
<td>This field is the description of the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>(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.</td>
</tr>
<tr>
<td>Model Name</td>
<td>This field is the device model, for example, the Cisco Catalyst 6K, the Cisco Nexus 7K, and so on.</td>
</tr>
<tr>
<td>Software Version</td>
<td>This field is the version of the software on the device, for example, Version 12.2, 12.3, and so on.</td>
</tr>
<tr>
<td>Network Device Group</td>
<td>(Required) From the Location and Device Type drop-down list boxes, choose a location and device type to associate with the device.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP Version</strong></td>
<td>(Required) This setting is the version of SNMP to be used for requests. Valid options are:&lt;br&gt;• 1—SNMPv1 does not support informs.&lt;br&gt;• 2c&lt;br&gt;• 3—SNMPv3 is the most secure model because it allows packet encryption when you choose the Priv security level.</td>
</tr>
<tr>
<td><strong>SNMP RO Community</strong></td>
<td>(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 Cisco ISE with a particular type of access to the device.</td>
</tr>
<tr>
<td><strong>SNMP Username</strong></td>
<td>(Required if you choose SNMP version 3) This setting is the SNMPv3 username.</td>
</tr>
<tr>
<td><strong>Security Level</strong></td>
<td>(Required if you choose SNMP version 3) Choose the security level for SNMPv3. Valid options are the following:&lt;br&gt;• Auth—Enables MD5 or Secure Hash Algorithm (SHA) packet authentication&lt;br&gt;• No Auth—No authentication and no privacy security level&lt;br&gt;• Priv—Enables DES packet encryption</td>
</tr>
<tr>
<td><strong>Auth Protocol</strong></td>
<td>This setting is the authentication protocol that you want the device to use. Valid options are MD5 or SHA1.</td>
</tr>
<tr>
<td><strong>Auth Password</strong></td>
<td>Enter the authentication key. The authentication key must be at least 8 characters in length.</td>
</tr>
<tr>
<td><strong>Privacy Protocol</strong></td>
<td>This setting is the privacy protocol that you want the device to use. Valid options are DES, AES128, AES192, AES256, and 3DES.</td>
</tr>
<tr>
<td><strong>Privacy Password</strong></td>
<td>Enter the privacy key.</td>
</tr>
<tr>
<td><strong>Polling Interval</strong></td>
<td>This setting is the SNMP polling interval in seconds. Default is 3600 seconds.</td>
</tr>
<tr>
<td><strong>Link Trap Query</strong></td>
<td>Check this check box for the profiler service to query the device, if it receives the link trap from the NAD connected to the device.</td>
</tr>
<tr>
<td><strong>MAC Trap Query</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

1. MD5 = Message Digest 5.<br>2. DES = Data Encryption Standard.<br>3. NAD = Network Access Device
Deleting a Device

Prerequisite:
Every Cisco 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.
Configuring a Default Device

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

**Prerequisite:**
Every Cisco 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** Enter the RADIUS shared secret.
**Step 5** Click Submit 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.

Cisco 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 Cisco 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 6-8
- Editing a Network Device Group, page 6-9
- Deleting a Network Device Group, page 6-10
- Import Network Device Groups into Cisco ISE, page 6-16
- Exporting Network Device Groups, page 6-18

Creating a Network Device Group

Prerequisite:
Every Cisco 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.
Managing Network Devices

Managing Network Device Groups

- (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 6-9
- Deleting a Network Device Group, page 6-10

---

**Editing a Network Device Group**

**Prerequisite:**

Every Cisco 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.
Deleting a Network Device Group

Prerequisite:
Every Cisco 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 6-8
- Editing a Network Device Group, page 6-9
Importing Network Devices and Device Groups

Cisco 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 Cisco 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 Cisco ISE. When you configure an import job, you can also define whether you want Cisco 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 Cisco 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 Cisco ISE, you must complete the following tasks:

1. Download the Import File Template, page 6-11
2. Create the CSV Import File, page 6-12
3. Import Devices into Cisco ISE, page 6-15 or Import Network Device Groups into Cisco ISE, page 6-16

Download the Import File Template

Prerequisite:
Every Cisco 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 Cisco ISE.

**Prerequisite:**

Every Cisco 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 6-4 lists the fields in the header and provides a description of the fields in the Network Device CSV file template.
- Table 6-5 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**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name</td>
<td>Descriptive IP Address</td>
<td>Model</td>
<td>Software</td>
<td>Network Device</td>
<td>Authentication Method</td>
<td>Authenticator</td>
</tr>
<tr>
<td>2</td>
<td>device_1</td>
<td>64.103.172.2700</td>
<td>2700</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco123</td>
</tr>
<tr>
<td>3</td>
<td>Test_01</td>
<td>10.10.0.01</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco001</td>
</tr>
<tr>
<td>4</td>
<td>Test_02</td>
<td>10.10.0.02</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco002</td>
</tr>
<tr>
<td>5</td>
<td>Test_03</td>
<td>10.10.0.03</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco003</td>
</tr>
<tr>
<td>6</td>
<td>Test_04</td>
<td>10.10.0.04</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco004</td>
</tr>
<tr>
<td>7</td>
<td>Test_05</td>
<td>10.10.0.05</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco005</td>
</tr>
<tr>
<td>8</td>
<td>Test_06</td>
<td>10.10.0.06</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco006</td>
</tr>
<tr>
<td>9</td>
<td>Test_07</td>
<td>10.10.0.07</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco007</td>
</tr>
<tr>
<td>10</td>
<td>Test_08</td>
<td>10.10.0.08</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco008</td>
</tr>
<tr>
<td>11</td>
<td>Test_09</td>
<td>10.10.0.09</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco009</td>
</tr>
<tr>
<td>12</td>
<td>Test_10</td>
<td>10.10.0.10</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco010</td>
</tr>
<tr>
<td>13</td>
<td>Test_11</td>
<td>10.10.0.11</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco011</td>
</tr>
<tr>
<td>14</td>
<td>Test_12</td>
<td>10.10.0.12</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco012</td>
</tr>
<tr>
<td>15</td>
<td>Test_13</td>
<td>10.10.0.13</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco013</td>
</tr>
<tr>
<td>16</td>
<td>Test_14</td>
<td>10.10.0.14</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco014</td>
</tr>
<tr>
<td>17</td>
<td>Test_15</td>
<td>10.10.0.15</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco015</td>
</tr>
<tr>
<td>18</td>
<td>Test_16</td>
<td>10.10.0.16</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco016</td>
</tr>
<tr>
<td>19</td>
<td>Test_17</td>
<td>10.10.0.17</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco017</td>
</tr>
<tr>
<td>20</td>
<td>Test_18</td>
<td>10.10.0.18</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco018</td>
</tr>
<tr>
<td>21</td>
<td>Test_19</td>
<td>10.10.0.19</td>
<td>1801A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco019</td>
</tr>
<tr>
<td>22</td>
<td>Test_20</td>
<td>10.10.0.20</td>
<td>1802A</td>
<td></td>
<td></td>
<td>RADIUS</td>
<td>cisco020</td>
</tr>
</tbody>
</table>

**Step 3**
Save the .csv file.
Description of the Fields in the Network Device CSV Template

Table 6-4 CSV Template Fields and Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:String(32):Required</td>
<td>(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>Description:String(256)</td>
<td>This field is an optional description for the network device. A string, with a maximum of 256 characters.</td>
</tr>
<tr>
<td>IP Address:Subnets(a.b.c.d/m</td>
<td>...):Required</td>
</tr>
<tr>
<td>Model Name:String(32):Required</td>
<td>(Required) This field is the network device model name. It is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>Software Version:String(32):Required</td>
<td>(Required) This field is the network device software version. It is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>Network Device Groups:String(100):Required</td>
<td>(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</td>
</tr>
<tr>
<td>Authentication:Protocol:String(6)</td>
<td>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).</td>
</tr>
<tr>
<td>Authentication:Shared Secret:String(128)</td>
<td>(Required if you have entered a value for the Authentication Protocol field) This is a string, with a maximum of 128 characters.</td>
</tr>
<tr>
<td>SNMP:Version:Enumeration(1</td>
<td>2c</td>
</tr>
<tr>
<td>SNMP:RO Community:String(32)</td>
<td>(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.</td>
</tr>
<tr>
<td>SNMP:RW Community:String(32)</td>
<td>(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.</td>
</tr>
<tr>
<td>SNMP:Username:String(32)</td>
<td>This is an optional field. It is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>SNMP:Security Level:Enumeration(Auth</td>
<td>No Auth</td>
</tr>
<tr>
<td>SNMP:Authentication Protocol:Enumeration(MD5</td>
<td>SHA)</td>
</tr>
<tr>
<td>SNMP:Authentication Password:String(32)</td>
<td>(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>SNMP:Privacy Protocol:Enumeration(DES</td>
<td>AES128</td>
</tr>
</tbody>
</table>
Table 6-4  CSV Template Fields and Description (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP:Privacy Password:String(32)</td>
<td>(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>SNMP:Polling Interval:Integer:600-86400 seconds</td>
<td>This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.</td>
</tr>
<tr>
<td>SNMP:Is Link Trap Query:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>SNMP:Is MAC Trap Query:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>SGA:Device Id:String(32)</td>
<td>This is an optional field. It is the security group access device ID, and is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>SGA:Device Password:String(256)</td>
<td>(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.</td>
</tr>
<tr>
<td>SGA:Environment Data Download Interval:Integer</td>
<td>This is an optional field. It is the security group access environment data download interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>SGA:Peer Authorization Policy Download Interval:Integer</td>
<td>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.</td>
</tr>
<tr>
<td>SGA:Reauthentication Interval:Integer</td>
<td>This is an optional field. It is the security group access reauthentication interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>SGA:SGACL List Download Interval:Integer</td>
<td>This is an optional field. It is the security group access SGACL list download interval. Valid value is an integer between 1 and 24850.</td>
</tr>
<tr>
<td>SGA:Is Other SGA Devices Trusted:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>SGA:Is Device Included on SGT Mapping:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>Deployment:Execution Mode Username:String(32)</td>
<td>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.</td>
</tr>
<tr>
<td>Deployment:Execution Mode Password:String(32)</td>
<td>This is an optional field. It is the device password and is a string, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>Deployment:Enable Mode Password:String(32)</td>
<td>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.</td>
</tr>
</tbody>
</table>

For a detailed description of each of these fields, see Table 6-1, Table 6-2, Table 21-4, and Table 6-3.

**Result:**
You now have the .csv file to begin the import process.
Related Topics

- Importing Network Devices and Device Groups, page 6-11
- Import Devices into Cisco ISE, page 6-15

Import Devices into Cisco ISE

Prerequisite:
Every Cisco 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.

Step 3 Click Import.

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 Cisco 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 Cisco 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 Cisco 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 Cisco ISE

Prerequisite:

Every Cisco 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Is Root</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocationAll Locations</td>
<td>All Locations</td>
<td>Location</td>
<td>TRUE</td>
</tr>
<tr>
<td>Device TypeAll Device Types</td>
<td>All Device Types</td>
<td>Device Type</td>
<td>TRUE</td>
</tr>
<tr>
<td>LocationAll Locations#World</td>
<td>Location</td>
<td>FALSE</td>
<td></td>
</tr>
<tr>
<td>DeviceGroup1#DeviceGroup1</td>
<td>THIS IS DEVICEGROUP 1</td>
<td>DeviceGroup1</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup2#DeviceGroup2</td>
<td>THIS IS DEVICEGROUP 2</td>
<td>DeviceGroup2</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup3#DeviceGroup3</td>
<td>THIS IS DEVICEGROUP 3</td>
<td>DeviceGroup3</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup4#DeviceGroup4</td>
<td>THIS IS DEVICEGROUP 4</td>
<td>DeviceGroup4</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup5#DeviceGroup5</td>
<td>THIS IS DEVICEGROUP 5</td>
<td>DeviceGroup5</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup6#DeviceGroup6</td>
<td>THIS IS DEVICEGROUP 6</td>
<td>DeviceGroup6</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup7#DeviceGroup7</td>
<td>THIS IS DEVICEGROUP 7</td>
<td>DeviceGroup7</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup8#DeviceGroup8</td>
<td>THIS IS DEVICEGROUP 8</td>
<td>DeviceGroup8</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup9#DeviceGroup9</td>
<td>THIS IS DEVICEGROUP 9</td>
<td>DeviceGroup9</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup10#DeviceGroup10</td>
<td>THIS IS DEVICEGROUP 10</td>
<td>DeviceGroup10</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup11#DeviceGroup11</td>
<td>THIS IS DEVICEGROUP 11</td>
<td>DeviceGroup11</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup12#DeviceGroup12</td>
<td>THIS IS DEVICEGROUP 12</td>
<td>DeviceGroup12</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup13#DeviceGroup13</td>
<td>THIS IS DEVICEGROUP 13</td>
<td>DeviceGroup13</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup14#DeviceGroup14</td>
<td>THIS IS DEVICEGROUP 14</td>
<td>DeviceGroup14</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup15#DeviceGroup15</td>
<td>THIS IS DEVICEGROUP 15</td>
<td>DeviceGroup15</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup16#DeviceGroup16</td>
<td>THIS IS DEVICEGROUP 16</td>
<td>DeviceGroup16</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup17#DeviceGroup17</td>
<td>THIS IS DEVICEGROUP 17</td>
<td>DeviceGroup17</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup18#DeviceGroup18</td>
<td>THIS IS DEVICEGROUP 18</td>
<td>DeviceGroup18</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup19#DeviceGroup19</td>
<td>THIS IS DEVICEGROUP 19</td>
<td>DeviceGroup19</td>
<td>TRUE</td>
</tr>
<tr>
<td>DeviceGroup20#DeviceGroup20</td>
<td>THIS IS DEVICEGROUP 20</td>
<td>DeviceGroup20</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

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 Cisco 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 Cisco 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 Cisco 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 6-5  Network Device Groups CSV Template Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:String(100):Required</td>
<td>(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 &gt; 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.</td>
</tr>
<tr>
<td>Description:String(1024)</td>
<td>This is an optional network device group description. It is a string, with a maximum of 1024 characters.</td>
</tr>
<tr>
<td>Type:String(64):Required</td>
<td>(Required) This field is the network device group type. It is a string, with a maximum of 64 characters.</td>
</tr>
<tr>
<td>Is Root:Boolean(true</td>
<td>false):Required</td>
</tr>
</tbody>
</table>

**Related Topics**

- Importing Network Devices and Device Groups, page 6-11
- Create the CSV Import File, page 6-12
Exporting Network Devices and Network Device Groups

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

This section contains the following topics:

- Exporting Network Devices, page 6-18
- Exporting Network Device Groups, page 6-18

Exporting Network Devices

Prerequisite:
Every Cisco 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 Cisco ISE node.

Exporting Network Device Groups

Prerequisite:
Every Cisco 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 Cisco ISE node, which can now be imported into another Cisco ISE node.