Managing Network Resources

The Network Resources drawer defines elements within the network that issue requests to ACS or those that ACS interacts with as part of processing a request. This includes the network devices that issue the requests and external servers, such as a RADIUS server that is used as a RADIUS proxy.

This drawer allows you to configure:

- Network device groups—Logically groups the network devices, which you can then use in policy conditions.
- Network devices—Definition of all the network devices in the ACS device repository that accesses the ACS network.
- Default network device—A default network device definition that ACS can use for RADIUS or TACACS+ requests when it does not find the device definition for a particular IP address.
- External proxy servers—RADIUS servers that can be used as a RADIUS proxy.
- OCSP services—Online Certificate Status Protocol (OCSP) services are used to check the status of x.509 digital certificates and can be used as an alternate to the certificate revocation list (CRL).

When ACS receives a request from a network device to access the network, it searches the network device repository to find an entry with a matching IP address. ACS then compares the shared secret with the secret retrieved from the network device definition.

If they match, the network device groups that are associated with the network device are retrieved and can be used in policy decisions. See ACS 5.x Policy Model, page 3-1 for more information on policy decisions.

The Network Resources drawer contains:

Network Device Groups

In ACS, you can define network device groups (NDGs), which are sets of devices. These NDGs provide logical grouping of devices, for example, Device Location or Type, which you can use in policy conditions.

When the ACS receives a request for a device, the network device groups associated with that device are retrieved and compared against those in the policy table. With this method, you can group multiple devices and assign them the same policies. For example, you can group all devices in a specific location together and assign to them the same policy.

The Device Group Hierarchy is the hierarchical structure that contains the network device groups. Two of these, *Location* and *Device Type*, are predefined; you can edit their names but you cannot delete them. You can add up to 6 additional hierarchies including the root.

An NDG relates to any node in the hierarchy and is the entity to which devices are associated. These nodes can be any node within the hierarchy, not just leaf nodes.

Note You can have a maximum of six nodes in the NDG hierarchy, including the root node.

Related Topics

- Creating, Duplicating, and Editing Network Device Groups, page 7-2
- Deleting Network Device Groups, page 7-3

Creating, Duplicating, and Editing Network Device Groups

To create, duplicate, or edit a network device group:

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

The Network Device Groups page appears. If you have defined additional network device groups, they appear in the left navigation pane, beneath the Network Device Groups option.

Step 2 Do any of the following:

- Click **Create**.
- Check the check box the network device group that you want to duplicate, then click **Duplicate**.
- Click the network device group name that you want to modify, or check the check box the name and click **Edit**.

The Hierarchy - General page appears.

Step 3 Modify the fields in the Hierarchy - General page as described in Table 7-1 on page 2:

Table 7-1 Device Groups - General Page Field Descriptions

Field	Description
Name	Enter a name for the network device group (NDG).
Description	(Optional) Enter a description for the NDG.
Root Node Name/Parent	Enter the name of the root node associated with the NDG. The NDG is structured as an inverted tree, and the root node is at the top of the tree. The root node name can be the same as the NDG name. The NDG name is displayed when you click an NDG in the Network Resources drawer.

Step 4 Click **Submit**.

The network device group configuration is saved. The Network Device Groups page appears with the new network device group configuration.

Related Topics

- Network Device Groups, page 7-1
- Deleting Network Device Groups, page 7-3
- Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3
- Performing Bulk Operations for Network Resources and Users, page 7-8

Deleting Network Device Groups

To delete a network device group:

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

The Network Device Groups page appears.

Step 2 Check one or more check boxes the network device groups you want to delete, and click **Delete**.

The following error message appears:

Error Message `You have requested to delete a network device group. If this group is referenced from a Policy or a Policy Element then the delete will be prohibited. If this group is referenced from a network device definition, the network device will be modified to reference the root node name group.`

Step 3 Click **OK**.

The Network Device Groups page appears without the deleted network device groups.

Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy

You can arrange the network device group node hierarchy according to your needs by choosing parent and child relationships for new, duplicated, or edited network device group nodes. You can also delete network device group nodes from a hierarchy.

To create, duplicate, or edit a network device group node within a hierarchy:

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

The Network Device Groups page appears.

Step 2 Click **Location**, **Device Type**, or another previously defined network device group in which you want to create a new network device group, and add it to the hierarchy of that group.

The Network Device Group hierarchy page appears.

Step 3 Do one of the following:

- Click **Create**. If you click **Create** when you have a group selected, the new group becomes a child of the parent group you selected. You can move a parent and all its children around in the hierarchy by clicking **Select** from the Create screen.
- Check the check box the network device group name that you want to duplicate, then click **Duplicate**.
- Click the network device group name that you want to modify, or check the check box the name and click **Edit**.

The Device Group - General page appears.

Step 4 Modify fields in the Device Groups - General page as shown in Table 7-2:

Table 7-2 Device Groups - General Page Field Descriptions

Field	Description
Name	Enter a name for the NDG.
Description	(Optional) Enter a description for the NDG.
Parent	Enter the name of the parent associated with the NDG. The NDG is structured as an inverted tree, and the parent name is the name of the top of the tree. Click **Select** to open the Groups dialog box from which you can select the appropriate parent for the group.

Step 5 Click **Submit**.

The new configuration for the network device group is saved. The Network Device Groups hierarchy page appears with the new network device group configuration.

Related Topics

- Network Device Groups, page 7-1
- Deleting Network Device Groups, page 7-3
- Creating, Duplicating, and Editing Network Device Groups, page 7-2
- Performing Bulk Operations for Network Resources and Users, page 7-8

Deleting Network Device Groups from a Hierarchy

To delete a network device group from within a hierarchy:

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

The Network Device Groups page appears.

Step 2 Click **Location**, **Device Type**, or another previously defined network device group in which you want to edit a network device group node.

The Network Device Groups node hierarchy page appears.

Step 3 Select the nodes that you want to delete and click **Delete**.

The following message appears:

```
You have requested to delete a network device group. If this group is referenced from a
Policy or a Policy Element then the delete will be prohibited. If this group is referenced
from a network device definition, the network device will be modified to reference the
root node name group.
```

Step 4 Click **OK**.

Note Root node of a group cannot be deleted from NDG hierarchy. If you try to do so, the following error message appears:

```
Selected node can be removed only with a root group.
```

The network device group node is removed from the configuration. The Network Device Groups hierarchy page appears without the device group node that you deleted.

Network Devices and AAA Clients

You must define all devices in the ACS device repository that access the network. The network device definition can be associated with a specific IP address or a subnet mask, where all IP addresses within the subnet can access the network.

The device definition includes the association of the device to network device groups (NDGs). You also configure whether the device uses TACACS+ or RADIUS, and if it is a Security Group Access device.

Note When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses.

You can import devices with their configurations into the network devices repository.

When ACS receives a request, it searches the network device repository for a device with a matching IP address; then ACS compares the secret or password information against that which was retrieved from the network device definition. If the information matches, the NDGs associated with the device are retrieved and can be used in policy decisions.

You must install Security Group Access license to enable Security Group Access options. The Security Group Access options only appear if you have installed the Security Group Access license. For more information on Security Group Access licenses, see Licensing Overview, page 18-37.

Viewing and Performing Bulk Operations for Network Devices

You can view the network devices and AAA clients. These are the devices sending access requests to ACS. The access requests are sent via TACACs+ or RADIUS.

To view and import network devices:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Device page appears, with any configured network devices listed. Table 7-3 provides a description of the fields in the Network Device page:

Table 7-3 Network Device Page Field Descriptions

Option	Description
Name	User-specified name of network devices in ACS. Click a name to edit the associated network device (see Displaying Network Device Properties, page 7-14).
IP Address	*Display only.* The IP address or subnet mask of each network device. The first three IP addresses of type IPv4 or IPv6 appear in the field, each separated by a comma (,). If this field contains a subnet mask, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition. When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses that are available through the subnet mask. For example: IPv4—A subnet mask of 255.255.255.0 means you have 256 unique IPv4 addresses. By default, the subnet mask value for IPv4 is 32. IPv6—A subnet mask of 2001:0DB8:0:CD30::/127 means you have 2 unique IPv6 addresses. By default, the subnet mask value for IPv6 is 128. You can see the excluded IP address the specified IP address, if any.
NDG: *string*	Network device group. The two predefined NDGs are Location and Device Type. If you have defined additional network device groups, they are listed here as well.
Description	*Display only.* Descriptions of the network devices.

Step 2 Do any one of the following:

- Click **Create** to create a new network device. See Creating, Duplicating, and Editing Network Devices, page 7-10.
- Check the check box the network device that you want to edit and click **Edit**. See Creating, Duplicating, and Editing Network Devices, page 7-10.
- Check the check box the network device that you want to duplicate and click **Duplicate**. See Creating, Duplicating, and Editing Network Devices, page 7-10.
- Search for the Network devices based on the following categories:
  - Name
  - IP Address
  - Description
  - NDG Location
  - Device Type

You can specify full IP address, or IP address with wildcard "*" or, with IP address range, such as [15-20] in the IP address search field. The wildcard "*" and the IP range [15-20] option can be specified in all the 4 octets of IP address. The Equals option only is listed in the search condition when searching by IP address.

Note When you search for an IP address or IP-Range address, the search result displays all records that match the Search criteria, even if the Search IP Address (or) IP-Range address is in Excluded IP Address (or) Range.

- Click **File Operations** to perform any of the following functions:

- Add—Choose this option to add a list of network devices from the import file in a single shot.
- Update—Choose this option to replace the list of network devices in ACS with the network devices in the import file.
- Delete—Choose this option to delete from ACS the network devices listed in the import file.

See Performing Bulk Operations for Network Resources and Users, page 7-8 for more information.

For information on how to create the import files, refer to Software Developer's Guide for Cisco Secure Access Control System.

Note To perform a bulk add, edit, or delete operation on any of the ACS objects, you can use the export file of that object, retain the header row, and create the .csv import file.
However, to add an updated name or MAC address to the ACS objects, must to download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

Related Topics:

- Network Devices and AAA Clients, page 7-5
- Performing Bulk Operations for Network Resources and Users, page 7-8
- Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3

Exporting Network Devices and AAA Clients

Note You must turn off the popup blockers in your browser to ensure that the export process completes successfully.

To export a list of network devices:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Device page appears.

Step 2 Choose the filter condition and the Match if operator, and enter the filter criterion that you are looking for in the text box.

Step 3 Click **Go**.

A list of records that match your filter criterion appears. You can export this list to a .csv file.

Step 4 Click **Export** to export the records to a .csv file.

A system message box appears, prompting you for an encryption password to encrypt the .csv file during file transfer.

Step 5 To encrypt the export .csv file, check the **Password** check box and enter the encryption password. You can optionally choose to not encrypt the file during transfer.

Step 6 Click **Start Export** to begin the export process.

The Export Progress window appears, displaying the progress of the export process. If any errors are encountered during this process, they are displayed in the Export Progress window.

You can terminate the export process at any time during this process. All the reports, till you abort the export process, get exported. To resume, you have to start the export process all over again.

Step 7 After the export process is complete, Click **Save File** to save the export file to your local disk.

The export file is a .csv file that is compressed as export.zip.

Performing Bulk Operations for Network Resources and Users

You can use the file operation function to perform bulk operations (add, update, and delete) for the following on your database:

- Internal users
- Internal hosts
- Network devices

For bulk operations, you must download the .csv file template from ACS and add the records that you want to add, update, or delete to the .csv file and save it to your local disk. Use the Download Template function to ensure that your .csv file adheres to the requirements.

The .csv templates for users, internal hosts, and network devices are specific to their type; for example, you cannot use a downloaded template accessed from the Users page to add internal hosts or network devices. Within the .csv file, you must adhere to these requirements:

- Do not alter the contents of the first record (the first line, or row, of the .csv file).
- Use only one line for each record.
- Do not imbed new-line characters in any fields.
- For non-English languages, encode the .csv file in utf-8 encoding, or save it with a font that supports Unicode.

Before you begin the bulk operation, ensure that your browser's popup blocker is disabled.

Step 1 Click **File Operations** on the Users, Network Devices, or MAC Address page of the web interface.

The Operation dialog box appears.

Step 2 Click **Next** to download the .csv file template if you do not have it.

Step 3 Click any one of the following operations if you have previously created a template-based .csv file on your local disk:

- Add—Adds the records in the .csv file to the records currently available in ACS.
- Update—Overwrites the records in ACS with the records from the .csv file.
- Delete—Removes the records in the .csv file from the list in ACS.

Step 4 Click **Next** to move to the next page.

Step 5 Click **Browse** to navigate to your .csv file.

Step 6 Choose either of the following options that you want ACS to follow in case of an error during the import process:

- Continue processing remaining records; successful records will be imported.
- Stop processing the remaining records; only the records that were successfully imported before the error will be imported.

Step 7 Check the **Password** check box and enter the password to decrypt the .csv file if it is encrypted in GPG format.

Step 8 Click **Finish** to start the bulk operation.

The Import Progress window appears. Use this window to monitor the progress of the bulk operation. Data transfer failures of any records within your .csv file are displayed.

You can click the Abort button to stop importing data that is under way; however, the data that was successfully transferred is not removed from your database.

When the operation completes, the Save Log button is enabled.

Step 9 Click **Save Log** to save the log file to your local disk.

Step 10 Click **OK** to close the Import Progress window.

You can submit only one .csv file to the system at one time. If an operation is under way, an additional operation cannot succeed until the original operation is complete.

Note Internal users whose password type is NAC Profiler can also be imported when NAC Profiler is not installed in ACS.

For information on how to create the import files, refer to Software Developer's Guide for Cisco Secure Access Control System.

Note To perform a bulk add, edit, or delete operation on any of the ACS objects, you can use the export file of that object, retain the header row, and create the .csv import file. However, to add an updated name or MAC address to the ACS objects, you must download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

Exporting Network Resources and Users

To export a list of network resources or users:

Step 1 Click **Export** on the Users, Network Devices, or MAC Address page of the web interface.

The Network Device page appears.

Step 2 Choose the filter condition and the Match if operator, and enter the filter criterion that you are looking for in the text box.

Step 3 Click **Go**.

A list of records that match your filter criterion appears. You can export these to a .csv file.

Step 4 Click **Export** to export the records to a .csv file.

A system message box appears, prompting you for an encryption password to encrypt the .csv file during file transfer.

Step 5 To encrypt the export .csv file, check the **Password** check box and enter the encryption password. You can optionally choose to not encrypt the file during transfer.

Step 6 Click **Start Export** to begin the export process.

The Export Progress window appears, displaying the progress of the export process. If any errors are encountered during this process, they are displayed in the Export Progress window.

You can terminate the export process at any time during this process. If you terminate the export process, all the reports till the termination of the process are exported. If you want to resume, you have to start the export process all over again.

Step 7 After the export process is complete, Click **Save File** to save the export file to your local disk.

The export file is a .csv file that is compressed as export.zip.

Creating, Duplicating, and Editing Network Devices

You can use the bulk import feature to import a large number of network devices in a single operation; see Performing Bulk Operations for Network Resources and Users, page 7-8 for more information. Alternatively, you can use the procedure described in this topic to create network devices.

To create, duplicate, or edit a network device:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Devices page appears, with a list of your configured network devices, if any.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the network device name that you want to duplicate, then click **Duplicate**.
- Click the network device name that you want to modify, or check the check box the name and click **Edit**.

The first page of the Create Network Device process appears if you are creating a new network device. The Network Device Properties page for the selected device appears if you are duplicating or editing a network device.

Step 3 Modify the fields as required. For field descriptions, see Configuring Network Device and AAA Clients, page 7-10.

Step 4 Click **Submit**.

Your new network device configuration is saved. The Network Devices page appears, with your new network device configuration listed.

Related Topics

- Viewing and Performing Bulk Operations for Network Devices, page 7-5
- Configuring Network Device and AAA Clients, page 7-10

Configuring Network Device and AAA Clients

To display this page, choose **Network Resources > Network Devices and AAA Clients**, then click **Create**.

Table 7-4 Creating Network Devices and AAA Clients

Option	Description
General	
Name	Name of the network device. If you are duplicating a network device, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	Description of the network device.
Network Device Groups[1]	
Location	Click **Select** to display the Network Device Groups selection box. Click the radio button the Location network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type	Click **Select** to display the Network Device Groups selection box. Click the radio button the Device Type network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
IP Address The IP addresses and subnet masks that are associated with the network device. Select to enter a single IP address or to define a range.	
Single IP Address	Choose to enter a single IP address. The IP address can be either IPv4 or IPv6. ACS 5.8 validates the IP address if the address is entered in the supported format. It displays an error message if the entered format is not correct. In ACS 5.8, you can configure a network device with a single static IP address that can be part of a IP subnet or range configured on another network device. For more information, see Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges, page 7-17. **Note** IPv6 addresses are supported only in TACACS+ protocols.
IP Subnets	Choose to enter an IP address range. You can configure up to 40 IP addresses or subnet masks for each network device. If you use a subnet mask in this field, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition. When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128. The first six IP addresses appear in the field; use the scroll bar to see any additional configured IP addresses. A mask is needed only for wildcards, if you want an IP address range. You cannot use an asterisk (*) as a wildcard.

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
IP Range(s)	Choose to enter single or multiple ranges of IP address. You can configure up to 40 IP addresses or subnet masks for each network device. You can also exclude a subnet of IP address range from the configured range in a scenario where that subset has already been added. You can use a hyphen (-) to specify a range of IP addresses. A maximum of 40 IP addresses are allowed in a single IP range. You can also add IP addresses with wildcards. You can use asterisks (*) as wildcards. Some examples of entering IP address ranges are: • A single range—10.77.10.1-10,,,, 192.120.10-12.10 • Multiple ranges—10.*.1-20.10, 192.1-23.*.100-150 • Exclusions from a range—10.10.1-255.* exclude 10.10.10-200.100-150 Using dynamic device IP address ranges (for example: 1-5.*.7.9) can have performance implications on both the run-time and the management. Therefore, we recommend using IP address and subnet mask whenever possible. The dynamic IP address ranges should be used only when the range cannot be described using IP address and subnet mask. **Note** AAA clients with wildcards are migrated from 4.x to 5.x.
Authentication Options	
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall. Check TACACS+ if you use IPv4 or IPv6 IP addresses.
TACACS+ Shared Secret	Shared secret of the network device, if you enabled the TACACS+ protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Single Connect Device	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one: • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support If you disable this option, a new TCP connection is used for every TACACS+ request.
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device. Uncheck this option if you use an IPv6 address.
RADIUS Shared Secret	Shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
CoA Port	Used to set up the RAIUS CoA port for session directory, for user authentication. This session directory can be launched from Monitoring and Troubleshooting Viewer page. By default, the CoA port value is filled as 1700.
Enable KeyWrap	Check to enable the shared secret keys for RADIUS KeyWrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique, and must also be distinct from the RADIUS shared key. These shared keys are configurable for each AAA Client. The default key mode for KeyWrap is hexadecimal string.
Key Encryption Key (KEK)	Used for encryption of the Pairwise Master Key (PMK). In ASCII mode, enter a key length of exactly 16 characters; in hexadecimal mode, enter a key length of 32 characters.
Message Authentication Code Key (MACK)	Used to calculate the keyed hashed message authentication code (HMAC) over the RADIUS message. In ASCII mode, enter a key length with 20 characters. In hexadecimal mode, enter a key with 40 characters.
Key Input Format	Enter the keys as ASCII or hexadecimal strings. The default is hexadecimal.
Security Group Access	Appears only when you enable the Cisco Security Group Access feature. Check to use Security Group Access functionality on the network device. If the network device is the seed device (first device in the Security Group Access network), you must also check the RADIUS check box.
Use Device ID for Security Group Access Identification	Check this check box to use the device ID for Security Group Access Identification. When you check this check box, the following field, Device ID, is disabled.
Device ID	Name that will be used for Security Group Access identification of this device. By default, you can use the configured device name. If you want to use another name, clear the Use device name for Security Group Access identification check box, and enter the name in the Identification field.
Password	Security Group Access authentication password.
Security Group Access Advanced Settings	Check to display additional Security Group Access fields.
Other Security Group Access devices to trust this device (SGA trusted)	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for the peer authorization policy. ACS returns this information to the device in the response to a peer policy request. The default is 1 day.
Download SGACL lists every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for SGACL lists. ACS returns this information to the device in the response to a request for SGACL lists. The default is 1 day.

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
Download environment data every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for environment data. ACS returns this information to the device in the response to a request for environment data. The default is 1 day.
Re-authentication every: Weeks Days Hours Minutes Seconds	Specifies the dot1x (.1x) reauthentication period. ACS configures this for the supplicant and returns this information to the authenticator. The default is 1 day.

1. The Device Type and Location network device groups are predefined at installation. You can define an additional 10 network device groups. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information on how to define network device groups. If you have defined additional network device groups, they appear in alphabetical order in the Network Device Groups page and in the Network Resources drawer in the left navigation pane.

Displaying Network Device Properties

Choose **Network Resources > Network Devices and AAA Clients**, then click a device name or check the check box a device name, and click **Edit** or **Duplicate**.

The Network Devices and AAA Clients Properties page appears, displaying the information described in Table 7-5:

Table 7-5 Network Devices and AAA Clients Properties Page

Option	Description
Name	Name of the network device. If you are duplicating a network device, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	Description of the network device.
Network Device Groups[1]	
Location: Select	Click **Select** to display the Network Device Groups selection box. Click the radio button the network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type: Select	Click **Select** to display the Network Device Groups selection box. Click the radio button the device type network device group that you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
IP Address	
The IP addresses and subnet masks associated with the network device. Select to enter a single IP address or to define a range.	
Single IP Address	Choose to enter a single IP address. In ACS 5.8, you can configure a network device with a single static IP address that can be part of a IP subnet or range configured on another network device. For more information, see Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges, page 7-17

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
IP Subnets	Choose to enter an IP address range. You can configure up to 40 IP addresses or subnet masks for each network device. If you use a subnet mask in this field, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition. When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses. The first six IP addresses appear in the field; use the scroll bar to see any additional configured IP addresses. A mask is needed only for wildcards—if you want an IP address range. You cannot use asterisk (*) as wildcards.
IP Range(s)	Choose to enter single or multiple ranges of IP address. You can configure up to 40 IP addresses or subnet masks for each network device. You can also exclude a subnet of IP address range from the configured range in a scenario where that subset has already been added. You can use a hyphen (-) to specify a range of IP address. You can also add IP addresses with wildcards. You can use asterisks (*) as wildcards. Some examples of entering IP address ranges are: • A single range—10.77.10.1-10,,,, 192.120.10-12.10 • Multiple ranges—10.*.1-20.10, 192.1-23.*.100-150 • Exclusions from a range—10.10.1-255.* exclude 10.10.10-200.100-150 Using dynamic device IP address ranges (for example: 1-5.*.7.9) can have performance implications on both the run-time and the management. Therefore, we recommend using IP address and subnet mask whenever possible. The dynamic IP address ranges should be used only when the range cannot be described using IP address and subnet mask.
Authentication Options	
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.
TACACS+ Shared Secret	Shared secret of the network device, if you enabled the TACACS+ protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Single Connect Device	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one: • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support If you disable this option, a new TCP connection is used for every TACACS+ request.
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
RADIUS Shared Secret	Shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
CoA Port	Used to set up the RAIUS CoA port for session directory, for user authentication. This session directory can be launched from Monitoring and Troubleshooting Viewer page. By default, the CoA port value is filled as 1700.
Enable KeyWrap	Check to enable the shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique and be distinct from the RADIUS shared key. You can configure these shared keys for each AAA Client.
Key Encryption Key (KEK)	Used to encrypt the Pairwise Master Key (PMK). In ASCII mode, enter a key with 16 characters. In hexadecimal mode, enter a key with 32 characters.
Message Authentication Code Key (MACK)	Used to calculate the keyed hashed message authentication code (HMAC) over the RADIUS message. In ASCII mode, enter a key length with 20 characters. In hexadecimal mode, enter a key with 40 characters.
Key Input Format	Enter the keys as ASCII or hexadecimal strings. The default is hexadecimal.
Security Group Access	Appears only when you enable the Cisco Security Group Access feature. Check to use Security Group Access functionality on the network device. If the network device is the seed device (first device in the Security Group Access network), you must also check the RADIUS check box.
Identification	Name that will be used for Security Group Access identification of this device. By default, you can use the configured device name. If you want to use another name, clear the Use device name for Security Group Access identification check box, and enter the name in the Identification field.
Password	Security Group Access authentication password.
Security Group Access Advanced Settings	Check to display additional Security Group Access fields.
Other Security Group Access devices to trust this device	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for the peer authorization policy. ACS returns this information to the device in the response to a peer policy request. The default is 1 day.
Download SGACL lists every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for SGACL lists. ACS returns this information to the device in the response to a request for SGACL lists. The default is 1 day.

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
Download environment data every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for environment data. ACS returns this information to the device in the response to a request for environment data. The default is 1 day.
Re-authentication every: Weeks Days Hours Minutes Seconds	Specifies the dot1x (.1x) reauthentication period. ACS configures this for the supplicant and returns this information to the authenticator. The default is 1 day.

1. The Device Type and Location network device groups are predefined at installation. You can define an additional 10 network device groups. See Creating, Duplicating, and Editing Network Device Groups, page 7-2, for information on how to define network device groups. If you have defined additional network device groups, they appear in the Network Device Groups page and in the Network Resources drawer in the left navigation pane, in alphabetical order.

Related Topics:

- Viewing and Performing Bulk Operations for Network Devices, page 7-5
- Creating, Duplicating, and Editing Network Device Groups, page 7-2

Deleting Network Devices

To delete a network device:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

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

Step 2 Check one or more check boxes the network devices you want to delete.

Step 3 Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 4 Click **OK**.

The Network Devices page appears, without the deleted network devices listed. The network device is removed from the device repository.

Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges

ACS 5.8 allows you to configure a network device with a single static IP address that can be part of an IP subnet or range configured on another network device.

For example, when you have network devices with the IP range 1.0-10.0-10.1 in ACS, the administrator can configure another network device with the IP address 1.1.1.1.

ACS allows you to use single static IPv4 or IPv6 addresses that are also a part of IP subnets and single static IPv4 addresses that are a part of IP ranges.

When ACS receives an access request, it searches the single static IP addresses first. If a match is not found, ACS searches the IP subnets and IP ranges for the network device. An IP address with a subnet mask of 32 resolves to the IP address itself. Therefore, ACS does not allow you to configure a single static IP address on a network device if the same IP address with a subnet mask of 32 is configured on another network device.

ACS displays all the occurrences of an IP address (Single IP address, IP subnet, and IP ranges) when you filter network devices on the Network Device and AAA Clients page.

Configuring a Default Network Device

While processing requests, ACS searches the network device repository for a network device whose IP address matches the IP address presented in the request. If the search does not yield a match, ACS uses the default network device definition for RADIUS or TACACS+ requests.

The default network device defines the shared secret to be used and also provides NDG definitions for RADIUS or TACACS+ requests that use the default network device definition.

Choose **Network Resources > Default Network Device** to configure the default network device. The Default Network Device page appears, displaying the information described in Table 7-6 on page 18.

Table 7-6 Default Network Device Page

Option	Description
Default Network Device	
The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address.	
Default Network Device Status	Choose **Enabled** from the drop-down list box to move the default network device to the active state.
Network Device Groups	
Location	Click **Select** to display the Network Device Groups selection box. Click the radio button the Location network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type	Click **Select** to display the Network Device Groups selection box. Click the radio button the Device Type network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Authentication Options	
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.

Table 7-6 Default Network Device Page (continued)

Option	Description
Shared Secret	Shared secret of the network device, if you enabled the TACACS+ protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Single Connect Device	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one: • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support If you disable this option, ACS uses a new TCP connection for every TACACS+ request.
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.
Shared Secret	Shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
CoA Port	Used to set up the RAIUS CoA port for session directory, for user authentication. This session directory can be launched from Monitoring and Troubleshooting Viewer page. By default, the CoA port value is filled as 1700.
Enable KeyWrap	Check to enable the shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique and be distinct from the RADIUS shared key. You can configure these shared keys for each AAA Client.
Key Encryption Key (KEK)	Used to encrypt the Pairwise Master Key (PMK). In ASCII mode, enter a key with 16 characters. In hexadecimal mode, enter a key with 32 characters.
Message Authentication Code Key (MACK)	Used to calculate the keyed hashed message authentication code (HMAC) over the RADIUS message. In ASCII mode, enter a key length with 20 characters. In hexadecimal mode, enter a key with 40 characters.
Key Input Format	Enter the keys as ASCII or hexadecimal strings. The default is hexadecimal.

Related Topics

- Network Device Groups, page 7-1
- Network Devices and AAA Clients, page 7-5
- Creating, Duplicating, and Editing Network Device Groups, page 7-2

Working with External Proxy Servers

ACS 5.8 can function both as a RADIUS and TACACS+ server and as a RADIUS and TACACS+ proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards them to the external RADIUS or TACACS+ server.

ACS accepts the results of the requests and returns them to the NAS. You must configure the external RADIUS or TACACS+ servers in ACS to enable ACS to forward requests to them. You can define the timeout period and the number of connection attempts.

ACS can simultaneously act as a proxy server to multiple external RADIUS or TACACS+ servers.

RADIUS proxy server can handle the looping scenario whereas TACACS+ proxy server cannot.

Note You can use the external RADIUS or TACACS+ servers that you configure here in access services of the RADIUS or TACACS+ proxy service type.

This section contains the following topics:

Creating, Duplicating, and Editing External Proxy Servers

To create, duplicate, or edit an external proxy server:

Step 1 Choose **Network Resources > External Proxy Servers**.

The External Proxy Servers page appears with a list of configured servers.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the external proxy server that you want to duplicate, then click **Duplicate**.
- Click the external proxy server name that you want to edit, or check the check box the name and click **Edit**.

The External Proxy Servers page appears.

Step 3 Edit fields in the External Proxy Servers page as shown in Table 7-7 on page 20.

Table 7-7 External Policy Servers Page

Option	Description
General	
Name	Name of the external RADIUS or TACACS+ server.
Description	(Optional) The description of the external RADIUS or TACACS+ server.
Server Connection	
Server IP Address	IP address of the external RADIUS or TACACS+ server. It can be either an IPv4 or IPv6 address. ACS 5.8 validates the IP address, if the address is entered in the supported format. It displays an error message if the entered format is not correct.

Table 7-7 External Policy Servers Page

Option	Description
Shared Secret	Shared secret between ACS and the external RADIUS or TACACS+ server that is used for authenticating the external RADIUS or TACACS+ server. A shared secret is an expected string of text that a user must provide to enable the network device to authenticate a username and password. The connection is rejected until the user supplies the shared secret. **Show/Hide** button is available to view the Shared secret in plain text or hidden format.
Advanced Options	
RADIUS	Choose to create a RADIUS proxy server. RADIUS supports only IPv4 addresses.
TACACS+	Choose to create a TACACS+ proxy server. TACACS+ supports IPv4 and IPv6 addresses.
Cisco Secure ACS	Default choice. Supports both RADIUS and TACACS+. You can choose Cisco Secure ACS if you use an IPv4 or IPv6 address.
Authentication Port	RADIUS authentication port number. The default is 1812.
Accounting Port	RADIUS accounting port number. The default is 1813.
Server Timeout	Number of seconds ACS waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 1 to 300.
Connection Attempts	Number of times ACS attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 99.
Connection Port	TACACS+ connection port. The default is 49.
Network Timeout	Number of seconds ACS waits for a response from the external TACACS+ server. The default is 20 seconds.

Step 4 Click **Submit** to save the changes.

The external Proxy Server configuration is saved. The External Proxy Server page appears with the new configuration.

Note If you want ACS to forward unknown RADIUS attributes you have to define VSAs for proxy.

Related Topics

- RADIUS and TACACS+ Proxy Services, page 3-7
- RADIUS and TACACS+ Proxy Requests, page 4-27
- Configuring General Access Service Properties, page 10-13
- Deleting External Proxy Servers, page 7-21

Deleting External Proxy Servers

To delete an external proxy server:

Step 1 Choose **Network Resources > External Proxy Servers**.

The External Proxy Servers page appears with a list of configured servers.

Step 2 Check one or more check boxes the external RADIUS or TACACS+ servers you want to delete, and click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 3 Click **OK.**

The External Proxy Servers page appears without the deleted server(s).

Working with OCSP Services

ACS 5.8 introduces a new protocol, Online Certificate Status Protocol (OCSP), which is used to check the status of x.509 digital certificates. This protocol can be used as an alternate to the certificate revocation list (CRL). It can also address the issues that result when handling CRLs.

ACS 5.8 communicates with OCSP services over HTTP to validate the status of the certificates in authentications. OCSP is configured in a reusable configuration object, and OCSP can be referenced from any certificate authority (CA) certificate that is configured in ACS. Multiple CA objects can reference the same OCSP service.

You can configure up to two OCSP servers in ACS, which are called the primary and secondary OCSP servers. ACS communicates with the secondary OCSP server when a timeout occurs while it is communicating with the primary OCSP server.

OCSP can return the following three values for a given certificate request:

- Good—The certificate is good for usage.
- Revoked—The certificate is revoked.
- Unknown —The certificate status is unknown.
  The status of the certificate is unknown if the OCSP is not configured to handle the given certificate CA. In this case, the certificate is handled as an unknown certificate; that is, the validation process checks the *Reject the request if no status* flag. If the flag is set in such a way that the request should not be rejected, then OCSP continues to CRL to check whether the certificate is configured in ACS.

ACS caches all OCSP responses. This is to maximize the performance and reduce the load in the OCSP servers. At the time of OCSP verification, ACS looks for the relevant information in the cache first. If the relevant information is not found, then ACS establishes a connection to the OCSP server. ACS defines a lifetime for all OCSP records in each OCSP service. In addition, each OCSP response has a Time to Live that defines the interval after which a new request should be made. Each cache entry is retained for either the Time to Live or the cache lifetime, whichever is shorter. Click **Clear Cache** to clear all the cached records that are associated with this OCSP service. Clear Cache also clears the records in the secondary ACS servers in a distributed system.

ACS does not support replicating the cached responses database. The caches are not persistent; therefore, the cached responses are cleared after you restart the ACS application.

ACS verifies the user certificates and the CA certificates and creates a set of logs for both the certificates in RADIUS Authentication reports page. Therefore, OCSP logs appear twice in the RADIUS Authentication reports page for the passed authentications whereas for the failed authentications, it appears only once.

The following logs are displayed twice when ACS communicates with the OCSP server for the first time:

- 12568 Lookup user certificate status in OCSP cache.
- 12569 User certificate status was not found in OCSP cache.
- 12550 Sent an OCSP request to the primary OCSP server for the CA.
- 12553 Received OCSP response.
- 12554 OCSP status of user certificate is good.

The following logs are displayed twice when ACS communicates searches the cached OCSP responses for the subsequent verifications based on either the cache Time to Live or the cache Lifetime options:

- 12568 Lookup user certificate status in OCSP cache.
- 12570 Lookup user certificate status in OCSP cache succeeded.
- 12554 OCSP status of user certificate is good.

This section contains the following topics:

- Creating, Duplicating, and Editing OCSP Servers, page 7-23
- Deleting OCSP Servers, page 7-25

Creating, Duplicating, and Editing OCSP Servers

To create, duplicate, or edit an OCSP server:

Step 1 Choose **Network Resources > OCSP Services**.

The OCSP Services page appears with a list of configured OCSP servers.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the OCSP server that you want to duplicate, then click **Duplicate**.
- Click the OCSP server name that you want to edit, or check the check box the name and click **Edit**.

The OCSP Servers page appears.

Step 3 Edit fields in the OCSP Servers page as shown in Table 7-8 on page 23.

Table 7-8 OCSP Servers Page

Option	Description
Name	Name of the OCSP server.
Description	(Optional) The description of the OCSP server.
Server Connection	
Enable Secondary Server	Check this check box to enable the secondary server configuration, such as Always Access Primary Server First and Failback options.
Always Access Primary Server First	Enable this option to check the primary server first before moving on to the secondary server, even if there was no previous response from the primary server.
Failback To Primary Server	Enable this option to use the secondary server for the given amount of time when the primary is completely down. The time range is 1 to 1440 minutes.
Primary Server	
URL	Enter the URL or the IP address of the primary server.

Table 7-8 OCSP Servers Page

Option	Description
Enable Nonce Extension Support	Check this check box to use a nonce in the OCSP request. This option includes a random number in the OCSP request. When you select this option, it compares the number that is received in the response with the number that is included in the request. This method ensures that old communications are not reused. You can configure a nonce in Windows 2008 and 2012 servers. If the nonce from the ACS server is not matched with the Windows server, Windows returns an unauthorized response. As a result, ACS fails the request and considers this to be an unknown certificate.
Validate Response Signature	Check this check box to instruct the OCSP responder to include one of the following signatures in the response: • The CA certificate • A different certificate from the CA certificate ACS validates the response certificate based on the OCSP response signature. If there is no OCSP response signature, then ACS fails the response, and the status of the certificate cannot be determined.
Network Timeout	Enter the number of seconds that ACS should wait for a response from the primary OCSP server. The default is 5 seconds. Valid values are from 1 to 300 seconds.
Secondary Server	
URL	Enter the URL or the IP address of the secondary server.
Enable Nonce Extension Support	Check this check box to use a nonce in the OCSP request. This option includes a random number in the OCSP request. When you select this option, it compares the number that is received in the response with the number that is included in the request. This method ensures that old communications are not reused. You can configure a nonce in Windows 2008 and 2012 servers. If the nonce from the ACS server is not matched with the Windows server, Windows returns an unauthorized response. As a result, ACS fails the request and considers this to be an unknown certificate.
Validate Response Signature	Check this check box to instruct the OCSP responder to include one of the following signatures in the response: • The CA certificate • A different certificate from the CA certificate ACS validates the response certificate based on the OCSP response signature. If there is no OCSP response signature, then ACS fails the response, and the status of the certificate cannot be determined.
Network Timeout	Enter the number of seconds that ACS should wait for a response from the primary OCSP server. The default is 5 seconds. Valid values are from 1 to 300.
Response Cache	
Cache Entry Time To Live	Defines the interval after which the a new OCSP request should be made. Enter the value in number of minutes. The default value is 300 minutes.
Clear Cache	Clears the Cache of the selected OCSP service for all the associated Certificate Authorities. The Clear Cache option can interact with all the nodes that are associated with this OCSP service within a deployment. This option also shows the updated status when you select it.

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

The OCSP Server configuration is saved. The OCSP Server page appears with the new configuration.

Related Topics

- Deleting OCSP Servers, page 7-25

Deleting OCSP Servers

To delete an OCSP server, complete the following steps:

Step 1 Choose **Network Resources > OCSP Services**.

The OCSP Services page appears with a list of configured OCSP servers.

Step 2 Check one or more check boxes the OCSP servers you want to delete, and click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 3 Click **OK.**

The OCSP Servers page appears without the deleted server(s).