CHAPTER 9

Managing Policy Elements

A policy defines the authentication and authorization processing of clients that attempt to access the ACS network. A client can be a user, a network device, or a user associated with a network device.

Policies are sets of rules. Rules contain policy elements, which are sets of conditions and results that are organized in rule tables. See Chapter 3, "ACS 5.x Policy Model" for more information on policy design and how it is implemented in ACS.

Before you configure your policy rules, you must create the policy elements, which are the conditions and results to use in those policies. After you create the policy elements, you can use them in policy rules. See Chapter 10, "Managing Access Policies" for more information on managing services, policies, and policy rules.

These topics contain.

Note When Cisco Security Group Access license is installed, you can also configure Security Groups and Security Group Access Control Lists (SGACLs), which you can then use in Security Group Access authorization policies. For information about configuring security groups for Security Group Access, see Creating Security Groups, page 4-24.

Managing Policy Conditions

You can configure the following items as conditions in a rule table:

- Request/Protocol Attributes—ACS retrieves these attributes from the authentication request that the user issues.
- Identity Attributes—These attributes are related to the identity of the user performing a request. These attributes can be retrieved from the user definition in the internal identity store or from user definitions that are stored in external identity stores, such as LDAP and AD.
- Identity Groups—ACS maintains a single identity group hierarchy that is used for all types of users and hosts. Each internal user or host definition can include an association to a single identity group within the hierarchy.

You can map users and hosts to identity groups by using the group mapping policy. You can include identity groups in conditions to configure common policy conditions for all users in the group. For more information about creating identity groups, see Managing Identity Attributes, page 8-7.

- Network Device Groups (NDGs)—Devices issuing requests are included in one or more of up to 12 device hierarchies. You can include hierarchy elements in policy conditions. For more information about creating NDGs, see Network Device Groups, page 7-2.
- Date and Time Conditions—You can create named conditions that define specific time intervals across specific days of the week. You can also associate expiry dates with date and time conditions.

  A date and time condition is a condition that takes the current date and time and effectively returns either true or false to indicate whether or not the condition is met. There are two components within the date and time condition:

  - Enable Duration—You have the option to limit the duration during which the condition is enabled by specifying an optional start time, end time, or both. This component allows you to create rules with limited time durations that effectively expire.

    If the condition is not enabled, then this component of the date and time condition returns false.
  - Time Intervals—On the ACS web interface, you see a grid of time that shows the days of the week and the hours within each day. Each cell in the grid represents one hour. You can either set or clear the cells.

    If the date and time when a request is processed falls at a time when the corresponding time interval is set, then this component of the date and time condition returns true.

  Both components of the date and time condition are considered while processing a request. The date and time condition is evaluated as true only if both components return a true value.
- Network Conditions—You can create filters of the following types to restrict access to the network:
  - End Station Filters—Based on end stations that initiate and terminate the connection. End stations may be identified by IP address, MAC address, calling line identification (CLI), or dialed number identification service (DNIS) fields obtained from the request.
  - Network Device Filters—Based on the AAA client that processes the request. A network device can be identified by its IP address, by the device name that is defined in the network device repository, or by the NDG.
  - Device Port Filters—Network device definition might be supplemented by the device port that the end station is associated with.

  Each network device condition defines a list of objects that can then be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request.

  The operator that you use in the condition can be either *match,* in which case the value presented must match at least one entry within the network condition, or *no matches,* in which case it should not match any entry in the set of objects that is present in the filter.

You can include Protocol and Identity attributes in a condition by defining them in custom conditions or in compound conditions.

- UserIsInManagementHierarchy—This attribute returns true as a result when the management hierarchy defined for the user equals or contained in the network device's hierarchy. The type of the attribute is boolean and the default value is False.

You define compound conditions in the policy rule properties page and not as a separate named condition. See Configuring Compound Conditions, page 10-41.

Custom conditions and Date and Time conditions are called session conditions.

This section contains the following topics:

See Chapter 3, "ACS 5.x Policy Model" for information about additional conditions that you can use in policy rules, although they are not configurable.

Creating, Duplicating, and Editing a Date and Time Condition

Create date and time conditions to specify time intervals and durations. For example, you can define shifts over a specific holiday period. When ACS processes a rule with a date and time condition, the condition is compared to the date and time information of the ACS instance that is processing the request. Clients that are associated with this condition are subject to it for the duration of their session.

The time on the ACS server is used when making policy decisions. Therefore, ensure that you configure date and time conditions that correspond to the time zone in which your ACS server resides. Your time zone may be different from that of the ACS server.

You can duplicate a session condition to create a new session condition that is the same, or similar to, an existing session condition. After duplication is complete, you access each session condition (original and duplicated) separately to edit or delete them.

To create, duplicate, or edit a date and time condition:

Step 1 Select **Policy Elements > Session Conditions > Date and Time**.

The Date and Time Conditions page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the condition you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the condition that you want to modify and click **Edit**.

The Date and Time Properties page appears.

Step 3 Enter valid configuration data in the required fields as described in Table 9-1:

Table 9-1 Date and Time Properties Page

Option	Description
General	
Name	Enter a name for the date and time condition.
Description	Enter a description, such as specific days and times of the date and time condition.

Table 9-1 Date and Time Properties Page (continued)

Option	Description
Duration	
Start	Click one of the following options: • **Start Immediately**—Specifies that the rules associated with this condition are valid, starting at the current date. • **Start On**—Specify a start date by clicking the calendar icon next to the associated field to choose a specific start date, at which the condition becomes active (at the beginning of the day, indicated by the time 00:00:00 on a 24-hour clock). You can specify time in the *hh*:*mm* format.
End	Click one of the following options: • **No End Date**—Specifies that the rules associated with this date and time condition are always active, after the indicated start date. • **End By**—Specify an end date by clicking the calendar icon next to the associated field to choose a specific end date, at which the date and time condition becomes inactive (at the end of the day, indicated by the time 23:59:59 on a 24-hour clock) You can specify time in the *hh*:*mm* format.
Days and Time	
Days and Time section grid	Each square in the Days and Time grid is equal to one hour. Select a grid square to make the corresponding time active; rules associated with this condition are valid during this time. A green (or darkened) grid square indicates an active hour. Ensure that you configure date and time conditions that correspond to the time zone in which your ACS server resides. Your time zone may be different from that of the ACS server. For example, you may receive an error message if you configure a date and time condition that is an hour ahead of your current time, but that is already in the past with respect to the time zone of your ACS server.
Select All	Click to set all squares in the grid to the active state. Rules associated with this condition are always valid.
Clear All	Click to set all squares in the grid to the inactive state. Rules associated with this condition are always invalid.
Undo All	Click to remove your latest changes for the active and inactive day and time selections for the date and time group.

To add date and time conditions to a policy, you must first customize the rule table. See Customizing a Policy, page 10-4.

Step 4 Click **Submit**.

The date and time condition is saved. The Date and Time Conditions page appears with the new date and time condition that you created or duplicated.

Note ACS has services and resources that are time sensitive. So, it is advised to restart all services after performing operations such as changing the clock, time zone, or NTP. If you do not restart after these operations, there are possibilities that it may break the functionalities such as AD, database connections, and cryptographic materials.

Related Topics

- Creating, Duplicating, and Editing a Custom Session Condition, page 9-5
- Deleting a Session Condition, page 9-6
- Configuring Access Service Policies, page 10-22

Creating, Duplicating, and Editing a Custom Session Condition

The protocol and identity dictionaries contain a large number of attributes. To use any of these attributes as a condition in a policy rule, you must first create a custom condition for the attribute. In this way, you define a smaller subset of attributes to use in policy conditions, and present a smaller focused list from which to choose condition types for rule tables.

You can also include protocol and identity attributes within compound conditions. See Configuring Compound Conditions, page 10-41 for more information on compound conditions.

To create a custom condition, you must select a specific protocol (RADIUS or TACACS+) or identity attribute from one of the dictionaries, and name the custom condition. See Configuring Global System Options, page 18-1 for more information on protocol and identity dictionaries.

When you create a custom condition that includes identity or RADIUS attributes, you can also include the definition of the attributes. You can thus easily view any existing custom conditions associated with a particular attribute.

To create, duplicate, or edit a custom session condition:

Step 1 Select **Policy Elements > Session Conditions > Custom**.

The Custom Conditions page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the condition you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the condition that you want to modify and click **Edit**.

The Custom Condition Properties page appears.

Step 3 Enter valid configuration data in the required fields as shown in Table 9-2:

Table 9-2 Policy Custom Condition Properties Page

Option	Description
General	
Name	Name of the custom condition.
Description	Description of the custom condition.
Condition	
Dictionary	Choose a specific protocol or identity dictionary from the drop-down list box.
Attribute	Click **Select** to display the list of external identity store dictionaries based on the selection you made in the Dictionary field. Select the attribute that you want to associate with the custom condition, then click **OK**. If you are editing a custom condition that is in use in a policy, you cannot edit the attribute that it references.

To add custom conditions to a policy, you must first customize the rule table. See Customizing a Policy, page 10-4.

Step 4 Click **Submit**.

The new custom session condition is saved. The Custom Condition page appears with the new custom session condition. Clients that are associated with this condition are subject to it for the duration of their session.

Related Topics

- Creating, Duplicating, and Editing a Date and Time Condition, page 9-3
- Deleting a Session Condition, page 9-6
- Configuring Access Service Policies, page 10-22

Deleting a Session Condition

To delete a session condition:

Step 1 Select **Policy Elements > Session Conditions > *session condition***, where *session condition* is Date and Time or Custom.

The Session Condition page appears.

Step 2 Check one or more check boxes next to the session conditions that 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 Session Condition page appears without the deleted custom session conditions.

Related Topics

- Creating, Duplicating, and Editing a Date and Time Condition, page 9-3
- Creating, Duplicating, and Editing a Custom Session Condition, page 9-5

Managing Network Conditions

Filters are reusable network conditions that you create for end stations, network devices, and network device ports. Filters enable ACS 5.4 to do the following:

- Decide whether or not to grant network access to users and devices.
- Decide on the identity store, service, and so on to be used in policies.

After you create a filter with a name, you can reuse this filter multiple times across various rules and policies by referring to its name.

Note The filters in ACS 5.4 are similar to the NARs in ACS 4.x. In ACS 4.x, the NARs were based on either the user or user group. In 5.4, the filters are independent conditions that you can reuse across various rules and policies.

ACS offers three types of filters:

- End Station Filter—Filters end stations, such as a laptop or printer that initiates a connection based on the end station's IP address, MAC address, CLID number, or DNIS number.

  The end station identifier can be the IP address, MAC address, or any other string that uniquely identifies the end station. It is a protocol-agnostic attribute of type string that contains a copy of the end station identifier:

  - In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).
  - In a TACACS request, ACS obtains this identifier from the remote address field of the start request (of every phase). It takes the remote address value before the slash (/) separator, if it is present; otherwise, it takes the entire remote address value.

  The end station IP address is either an IPv4 or IPv6 of the end station identifier. The end station MAC is a normalized MAC address of the end station identifier.

- Device Filter—Filters a network device (AAA client) that acts as a Policy Enforcement Point (PEP) to the end station based on the network device's IP address or name, or the network device group that it belongs to.

  The device identifier can be the IP address or name of the device, or it can be based on the network device group to which the device belongs.

  The IP address is a protocol-agnostic attribute of type IPv4 or IPv6, which contains a copy of the device IP address that is obtained from the request:

  - In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, ACS obtains the IP address from Attribute 4; otherwise, if Attribute 32 (NAS-Identifier) is present, ACS obtains the IP address from Attribute 32, or it obtains the IP address from the packet that it receives.
  - In a TACACS request, the IP address is obtained from the packet that ACS receives.

  The device name is an attribute of type string that contains a copy of the device name derived from the ACS repository.

  The device dictionary (the NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes, in turn, contain the groups that the current device is related to.

- Device Port Filter—Filters the physical port of the device that the end station is connected to. Filtering is based on the device's IP address, name, NDG it belongs to, and port.

  The device port identifier is an attribute of type string:

  - In a RADIUS request, if Attribute 5 (NAS-Port) is present in the request, ACS obtains the value from Attribute 5; or, if Attribute 87 (NAS-Port-Id) is present in the request, ACS obtains the request from Attribute 87.
  - In a TACACS request, ACS obtains this identifier from the port field of the start request (of every phase).

  The device name is an attribute of type string that contains a copy of the device name derived from the ACS repository.

The device dictionary (the NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes, in turn, contain the groups that the current device is related to.

You can create, duplicate, and edit these filters. You can also do a bulk import of the contents within a filter from a .csv file and export the filters from ACS to a .csv file. See Importing Network Conditions, page 9-8 for more information on how to do a bulk import of network conditions.

This section contains the following topics:

Importing Network Conditions

You can use the bulk import function to import the contents from the following network conditions:

- End station filters
- Device filters
- Device port filters

For bulk import, you must download the .csv file template from ACS, add the records that you want to import to the .csv file, and save it to your hard drive. Use the Download Template function to ensure that your .csv file adheres to the requirements.

The .csv templates for end station filters, device filters, and device port filters are specific to their type; for example, you cannot use a downloaded template accessed from the End Station Filters page to import device filters or device port filters. 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.

The import process does not add filters to the existing list of filters in ACS, but instead replaces the existing list. When you import records from a .csv file, it replaces the existing filter configuration in ACS and replaces it with the filter configuration from the .csv file.

Step 1 Click the **Replace from File** button on the End Station Filter, Device Filter, or Device Port Filter page of the web interface.

The Replace from File dialog box appears.

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

Step 3 Click **Browse** to navigate to your .csv file.

Step 4 Click **Start Replace** to start the bulk import process.

The import progress is shown on the same page. You can monitor the bulk import progress. Data transfer failures of any records within your .csv file are displayed.

Step 5 Click **Close** to close the Import Progress window.

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

Timesaver Instead of downloading the template and creating an import file, you can use the export file of the particular filter, update the information in that file, save it, and reuse it as your import file.

Exporting Network Conditions

ACS 5.4 offers you a bulk export function to export the filter configuration data in the form of a .csv file. You can export the following filter configurations:

- End Station Filters
- Device Filters
- Device Port Filters

From the create, edit, or duplicate page of any of the filters, click **Export to File** to save the filter configuration as a .csv file on your local hard drive.

Creating, Duplicating, and Editing End Station Filters

Use the End Station Filters page to create, duplicate, and edit end station filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > End Station Filters**.

The End Station Filters page appears with a list of end station filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box next to the end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the end station filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of end station filters in a .csv file. For more information, see Exporting Network Conditions, page 9-9.
- Click **Replace from File** to perform a bulk import of end station filters from a .csv import file. For more information, see Importing Network Conditions, page 9-8.

Step 3 Enter the values for the following fields:

- Name—Name of the end station filter.
- Description—A description of the end station filter.

Step 4 Edit the fields in one or more of the following tabs:

- IP Address—See Defining IP Address-Based End Station Filters, page 9-10 for a description of the fields in this tab.
- MAC Address—See Defining MAC Address-Based End Station Filters, page 9-11 for a description of the fields in this tab.
- CLI/DNIS—See Defining CLI or DNIS-Based End Station Filters, page 9-11 for a description of the fields in this tab.

Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- Managing Network Conditions, page 9-6
- Importing Network Conditions, page 9-8
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Creating, Duplicating, and Editing Device Port Filters, page 9-15

Defining IP Address-Based End Station Filters

You can create, duplicate, and edit the IP addresses of end stations that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box next to the IP-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the IP-based end station filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid address, as follows:
  - IPv4 address in the format *x*.*x*.*x*.*x*, where *x* can be any number from 0 to 255.
  - IPv6 address in the format *x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*, where *x* represents one to four hexadecimal digits of the eight 16-bit pieces of the address. This can be either numbers from 0 to 9 or letters from A to F.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.

Note IPv6 ranges are not supported in ACS 5.4.

Note IPv6 addresses are supported only in TACACS+ protocols.

Step 3 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing End Station Filters, page 9-9

- Defining MAC Address-Based End Station Filters, page 9-11
- Defining CLI or DNIS-Based End Station Filters, page 9-11

Defining MAC Address-Based End Station Filters

You can create, duplicate, and edit the MAC addresses of end stations or destinations that you want to permit or deny access to. To do this:

Step 1 From the MAC Address tab, do one of the following:

- Click **Create**.
- Check the check box next to the MAC address-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the MAC address-based end station filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Check the **End Station MAC** check box to enter the MAC address of the end station.

You can optionally set this field to ANY to refer to any MAC address.

Step 3 Check the **Destination MAC** check box to enter the MAC address of the destination machine.

You can optionally set this field to ANY to refer to any MAC address.

Note You must enter the MAC address in one of the following formats: *xxxxxxxxxxxx*, *xx-xx-xx-xx-xx-xx*, *xx:xx:xx:xx:xx:xx*, or *xxxx.xxxx.xxxx*, where x can be any number from 0 to 9 or A through F. You cannot use wildcard characters for MAC address.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing End Station Filters, page 9-9
- Defining IP Address-Based End Station Filters, page 9-10
- Defining CLI or DNIS-Based End Station Filters, page 9-11

Defining CLI or DNIS-Based End Station Filters

You can create, duplicate, and edit the CLI and DNIS number of the end stations or destinations that you want to permit or deny access to. To do this:

Step 1 From the CLI/DNIS tab, do one of the following:

- Click **Create**.
- Check the check box next to the CLI or DNIS-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the CLI or DNIS-based end station filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Check the **CLI** check box to enter the CLI number of the end station.

You can optionally set this field to ANY to refer to any CLI number.

Step 3 Check the **DNIS** check box to enter the DNIS number of the destination machine.

You can optionally set this field to ANY to refer to any DNIS number.

Note You can use ? and * wildcard characters to refer to any single character or a series of one or more successive characters respectively.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing End Station Filters, page 9-9
- Defining IP Address-Based End Station Filters, page 9-10
- Defining MAC Address-Based End Station Filters, page 9-11

Creating, Duplicating, and Editing Device Filters

Use the Device Filters page to create, duplicate, and edit device filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > Device Filters**.

The Device Filters page appears with a list of device filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box next to the device filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the device filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of device filters in a .csv file. For more information, see Exporting Network Conditions, page 9-9.
- Click **Replace from File** to perform a bulk import of device filters from a .csv import file. For more information, see Importing Network Conditions, page 9-8.

Step 3 Enter the values for the following fields:

- Name—Name of the device filter.
- Description—A description of the device filter.

Step 4 Edit the fields in any or all of the following tabs:

- IP Address—See Defining IP Address-Based Device Filters, page 9-13 for a description of the fields in this tab.
- Device Name—See Defining Name-Based Device Filters, page 9-14 for a description of the fields in this tab.
- Network Device Group—See Defining NDG-Based Device Filters, page 9-14 for a description of the fields in this tab.

Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- Managing Network Conditions, page 9-6
- Importing Network Conditions, page 9-8
- Creating, Duplicating, and Editing End Station Filters, page 9-9
- Creating, Duplicating, and Editing Device Port Filters, page 9-15

Defining IP Address-Based Device Filters

You can create, duplicate, and edit the IP addresses of network devices that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box next to the IP-based device filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the IP-based device filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid address, as follows:
  - IPv4 address in the format *x*.*x*.*x*.*x*, where *x* can be any number from 0 to 255.
  - IPv6 address in the format *x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*, where *x* represents one to four hexadecimal digits of the eight 16-bit pieces of the address. This can be either numbers from 0 to 9 or letters from A to F.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 or IPv6 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.

Note IPv6 ranges are not supported in ACS 5.4.

Step 3 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining Name-Based Device Filters, page 9-14
- Defining NDG-Based Device Filters, page 9-14

Defining Name-Based Device Filters

You can create, duplicate, and edit the name of the network device that you want to permit or deny access to. To do this:

Step 1 From the Device Name tab, do one of the following:

- Click **Create**.
- Check the check box next to the name-based device filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the name-based device filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Click **Select** to choose the network device that you want to filter.

Step 3 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining IP Address-Based Device Filters, page 9-13
- Defining NDG-Based Device Filters, page 9-14

Defining NDG-Based Device Filters

You can create, duplicate, and edit the name of the network device group type that you want to permit or deny access to. To do this:

Step 1 From the Network Device Group tab, do one of the following:

a. Click **Create**.

b. Check the check box next to the NDG-based device filter that you want to duplicate, then click **Duplicate**.

c. Check the check box next to the NDG-based device filter that you want to edit, then click **Edit**.

   A dialog box appears.

Step 2 Click **Select** to choose the network device group type that you want to filter.

Step 3 Click **Select** to choose the network device group value that you want to filter.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining IP Address-Based Device Filters, page 9-13
- Defining Name-Based Device Filters, page 9-14

Creating, Duplicating, and Editing Device Port Filters

Use the Device Port Filters page to create, duplicate, and edit device port filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > Device Port Filters**.

The Device Port Filters page appears with a list of device port filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box next to the device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the device port filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of device port filters in a .csv file. For more information, see Exporting Network Conditions, page 9-9.
- Click **Replace from File** to perform a bulk import of device port filters from a .csv import file. For more information, see Importing Network Conditions, page 9-8.

Step 3 Enter the values for the following fields:

- Name—Name of the device port filter.
- Description—A description of the device port filter.

Step 4 Edit the fields in any or all of the following tabs:

- IP Address—See Defining IP Address-Based Device Port Filters, page 9-15 for a description of the fields in this tab.
- Device Name—See Defining NDG-Based Device Port Filters, page 9-17 for a description of the fields in this tab.
- Network Device Group—See Defining NDG-Based Device Port Filters, page 9-17 for a description of the fields in this tab.

Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- Managing Network Conditions, page 9-6
- Importing Network Conditions, page 9-8
- Creating, Duplicating, and Editing End Station Filters, page 9-9
- Creating, Duplicating, and Editing Device Filters, page 9-12

Defining IP Address-Based Device Port Filters

You can create, duplicate, and edit the IP addresses of the network device ports that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.

- Check the check box next to the IP-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the IP-based device port filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid address, as follows:
  - IPv4 address in the format *x*.*x*.*x*.*x*, where *x* can be any number from 0 to 255.
  - IPv6 address in the format *x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*, where *x* represents one to four hexadecimal digits of the eight 16-bit pieces of the address. This can be either numbers from 0 to 9 or letters from A to F.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 or IPv6 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.

Note IPv6 ranges are not supported in ACS 5.4.

Step 3 Check the **Port** check box and enter the port number. This field is of type string and can contain numbers or characters. You can use the following wildcard characters:

- ?—match a single character
- *—match a set of characters

For example, the string "p*1*" would match any word that starts with the letter "p" and contains the number 1, such as port1, port15, and so on.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing Device Port Filters, page 9-15
- Defining Name-Based Device Port Filters, page 9-16
- Defining NDG-Based Device Port Filters, page 9-17

Defining Name-Based Device Port Filters

You can create, duplicate, and edit the name of the network device and the port to which you want to permit or deny access. To do this:

Step 1 From the Device Name tab, do one of the following:

- Click **Create**.
- Check the check box next to the name-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the name-based device port filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Click **Select** to choose the network device that you want to filter.

Step 3 Check the **Port** check box and enter the port number.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing Device Port Filters, page 9-15
- Defining IP Address-Based Device Port Filters, page 9-15
- Defining NDG-Based Device Port Filters, page 9-17

Defining NDG-Based Device Port Filters

You can create, duplicate, and edit the network device group type and the port to which you want to permit or deny access. To do this:

Step 1 From the Network Device Group tab, do one of the following:

- Click **Create**.
- Check the check box next to the NDG-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the NDG-based device port filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Click **Select** to choose the network device group type that you want to filter.

Step 3 Click **Select** to choose the network device group value that you want to filter.

Step 4 Check the **Port** check box and enter the port number.

Step 5 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-6
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining IP Address-Based Device Filters, page 9-13
- Defining Name-Based Device Filters, page 9-14

Managing Authorizations and Permissions

You define authorizations and permissions to determine the results associated with a specific policy rule.

You can define:

- Authorization profiles for network access authorization (for RADIUS).
- Shell profiles for TACACS+ shell sessions and command sets for device administration.
- Downloadable ACLs.

- Security groups and security group ACLs for Cisco Security Group Access. See ACS and Cisco Security Group Access, page 4-23, for information on configuring these policy elements.

These topics describe how to manage authorizations and permissions:

Creating, Duplicating, and Editing Authorization Profiles for Network Access

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

An authorization profile defines the set of attributes and values that the Access-Accept response returns. You can specify:

- Common data, such as VLAN information, URL for redirect, and more. This information is automatically converted to the raw RADIUS parameter information.
- RADIUS authorization parameters—You can select any RADIUS attribute and specify the corresponding value to return.

You can duplicate an authorization profile to create a new authorization profile that is the same, or similar to, an existing authorization profile. After duplication is complete, you access each authorization profile (original and duplicated) separately to edit or delete them.

After you create authorization profiles, you can use them as results in network access session authorization policies.

To create, duplicate, or edit an authorization profile:

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profile**.

The Authorization Profiles page appears with the fields described in Table 9-3:

Table 9-3 Authorization Profiles Page

Option	Description
Name	List of existing network access authorization definitions.
Description	*Display only.* The description of the network access authorization definition.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the authorization profile that you want to duplicate and click **Duplicate**.

- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

The Authorization Profile Properties page appears.

Step 3 Enter valid configuration data in the required fields in each tab. See:

- Specifying Authorization Profiles, page 9-19
- Specifying Common Attributes in Authorization Profiles, page 9-19
- Specifying RADIUS Attributes in Authorization Profiles, page 9-22

Step 4 Click **Submit**.

The authorization profile is saved. The Authorization Profiles page appears with the authorization profile that you created or duplicated.

Specifying Authorization Profiles

Use this tab to configure the name and description for a network access authorization profile.

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition.
- **Duplicate** to duplicate a network access authorization definition.
- **Edit** to edit a network access authorization definition.

Step 2 Complete the required fields of the Authorization Profile: General page as shown in Table 9-4:

Table 9-4 Authorization Profile: General Page

Option	Description
Name	The name of the network access authorization definition.
Description	The description of the network access authorization definition.

Step 3 Click one of the following:

- **Submit** to save your changes and return to the Authorization Profiles page.
- The **Common Tasks** tab to configure common tasks for the authorization profile; see Specifying Common Attributes in Authorization Profiles, page 9-19.
- The **RADIUS Attributes** tab to configure RADIUS attributes for the authorization profile; see Specifying RADIUS Attributes in Authorization Profiles, page 9-22.

Specifying Common Attributes in Authorization Profiles

Use this tab to specify common RADIUS attributes to include in a network access authorization profile. ACS converts the specified values to the required RADIUS attribute-value pairs and displays them in the RADIUS attributes tab.

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition, then click the **Common Tasks** tab.
- **Duplicate** to duplicate a network access authorization definition, then click the **Common Tasks** tab.
- **Edit** to edit a network access authorization definition, then click the **Common Tasks** tab.

Step 2 Complete the required fields of the Authorization Profile: Common Tasks page as shown in Table 9-5:

Table 9-5 Authorization Profile: Common Tasks Page

Option	Description
ACLS	
Downloadable ACL Name	Includes a defined downloadable ACL. See Creating, Duplicating, and Editing Downloadable ACLs, page 9-32 for information about defining a downloadable ACL.
Filter-ID ACL	Includes an ACL Filter ID.
Proxy ACL	Includes a proxy ACL.
Voice VLAN	
Permission to Join	Select **Static**. A value for this parameter is displayed.
VLAN	
VLAN ID/Name	Includes a VLAN assignment.
Reauthentication	
Reauthentication Timer	Select whether to use a session timeout value. • If you select **Static**, you must enter a value in the Seconds field. The default value is 3600 seconds. • If you select **Dynamic**, you must select the dynamic parameters.
Maintain Connectivity during Reauthentication	Click **Yes** to ensure connectivity is maintained while reauthentication is performed. By default, **Yes** is selected. This field is enabled only if you define the Reauthentication Timer.
QoS	
Input Policy Map	Includes a QoS input policy map.
Output Policy Map	Includes a QoS output policy map.
802.1X-REV	
LinkSec Security Policy	If you select **Static**, you must select a value for the 802.1X-REV LinkSec security policy. Valid options are: • must-not-secure • should-secure • must-secure
URL Redirect When a URL is defined for Redirect an ACL must also be defined	
URL for Redirect	Includes a URL redirect.
URL Redirect ACL	Includes the name of the access control list (ACL) for URL redirection. When you define a URL redirect, you must also define an ACL for the URL redirection.

Specifying RADIUS Attributes in Authorization Profiles

Use this tab to configure which RADIUS attributes to include in the Access-Accept packet for an authorization profile. This tab also displays the RADIUS attribute parameters that you choose in the Common Tasks tab.

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition, then click the **RADIUS Attributes** tab.
- Check the check box next to the authentication profile that you want to duplicate, click **Duplicate**, and then click the **RADIUS Attributes** tab.
- Check the check box next to the authentication profile that you want to duplicate, click **Edit**, and then click the **RADIUS Attributes** tab.

Step 2 Complete the required fields of the Authorization Profile: RADIUS Attributes page as shown in Table 9-6:

Table 9-6 Authorization Profile: RADIUS Attributes Page

Option	Description
Common Tasks Attributes	Displays the names, values, and types for the attributes that you defined in the Common Tasks tab.
Manually Entered	Use this section to define RADIUS attributes to include in the authorization profile. As you define each attribute, its name, value, and type appear in the table. To: • Add a RADIUS attribute, fill in the fields below the table and click **Add**. • Edit a RADIUS attribute, select the appropriate row in the table and click **Edit**. The RADIUS parameters appear in the fields below the table. Edit as required, then click **Replace**.
Dictionary Type	Choose the dictionary that contains the RADIUS attribute you want to use.

Table 9-6 Authorization Profile: RADIUS Attributes Page (continued)

Option	Description
RADIUS Attribute	Name of the RADIUS attribute. Click **Select** to choose a RADIUS attribute from the specified dictionary. You must manually add VPN attributes to the authorization profile to authenticate VPN devices in your network. ACS can work with different Layer 2 and Layer 3 protocols, such as: • IPSec—Operates at Layer 3; no mandatory attributes need to be configured in the ACS authorization profile, but you can configure optional attributes. • L2TP—For L2TP tunneling, you must configure ACS with: – CVPN3000/ASA/PIX7.x-Tunneling Protocols—This attribute specifies the type of tunneling to be used. – CVPN3000/ASA/PIX7.x-L2TP-Encryption—This attribute, when set, enables VPN3000 to communicate to the client the type of Microsoft Point-to-Point Encryption (MPPE) key that must be used, either the MSCHAPv1 or MSCHAPv2 authentication method. • PPTP—For PPTP tunneling, you must configure ACS with: – CVPN3000/ASA/PIX7.x-Tunneling Protocols—This attribute specifies the type of tunneling to be used. – CVPN3000/ASA/PIX7.x-PPTP-Encryption—This attribute, when set, enables VPN3000 to communicate to the client the type of Microsoft Point-to-Point Encryption (MPPE) key that must be used, either the MSCHAPv1 or MSCHAPv2 authentication method.
Attribute Type	Client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.
Attribute Value	Value of the attribute. Click **Select** for a list of attribute values. For a description of the attribute values, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients. For tunneled protocols, ACS provides for attribute values with specific tags to the device within the access response according to RFC 2868. If you choose Tagged Enum or Tagged String as the RADIUS Attribute type, the Tag field appears. For the tag value, enter a number that ACS will use to group attributes belonging to the same tunnel. For the Tagged Enum attribute type: • Choose an appropriate attribute value. • Enter an appropriate tag value (0–31). For the Tagged String attribute type: • Enter an appropriate string attribute value (up to 256 characters). • Enter an appropriate tag value (0–31).

Step 3 To configure:

- Basic information of an authorization profile; see Specifying Authorization Profiles, page 9-19.
- Common tasks for an authorization profile; see Specifying Common Attributes in Authorization Profiles, page 9-19.

Creating and Editing Security Groups

Use this page to view names and details of security groups and security group tags (SGTs), and to open pages to create, duplicate, and edit security groups.

When you create a security group, ACS generates a unique SGT. Network devices can query ACS for SGT information. The network device uses the SGT to tag, or paint, packets at ingress, so that the packets can be filtered at Egress according to the Egress policy. See Egress Policy Matrix Page, page 10-46, for information on configuring an Egress policy.

Step 1 Select **Policy Elements > Authorizations and Permissions > Network Access > Security Groups**.

The Security Groups page appears as described in Table 9-7:

Table 9-7 Security Groups Page

Option	Description
Name	The name of the security group.
SGT (Dec / Hex)	Representation of the security group tag in decimal and hexadecimal format.
Description	The description of the security group.

Step 2 Click:

- **Create** to create a new security group.
- **Duplicate** to duplicate a security group.
- **Edit** to edit a security group.

Step 3 Enter the required information in the Name and Description fields, then click **Submit**.

Related Topic

- Creating Security Groups, page 4-24

Creating, Duplicating, and Editing a Shell Profile for Device Administration

You can configure Cisco IOS shell profile and command set authorization. Shell profiles and command sets are combined for authorization purposes. Shell profile authorization provides decisions for the following capabilities for the user requesting authorization and is enforced for the duration of a user's session:

- Privilege level.
- General capabilities, such as device administration and network access.

Shell profile definitions are split into two components:

- Common tasks
- Custom attributes

The Common Tasks tab allows you to select and configure the frequently used attributes for the profile. The attributes that are included here are those defined by the TACACS protocol draft specification that are specifically relevant to the shell service. However, the values can be used in the authorization of requests from other services.

The Custom Attributes tab allows you to configure additional attributes. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. Custom attributes can be defined for nonshell services.

For a description of the attributes that you specify in shell profiles, see Cisco IOS documentation for the specific release of Cisco IOS software that is running on your AAA clients.

After you create shell profiles and command sets, you can use them in authorization and permissions within rule tables.

You can duplicate a shell profile if you want to create a new shell profile that is the same, or similar to, an existing shell profile.

After duplication is complete, you access each shell profile (original and duplicated) separately to edit or delete them.

To create, duplicate, or edit a shell profile:

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**.

The Shell Profiles page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the shell profile that you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

The Shell Profile Properties page General tab appears.

Step 3 Enter valid configuration data in the required fields in each tab. As a minimum configuration, you must enter a unique name for the shell profile; all other fields are optional. See:

- Defining General Shell Profile Properties, page 9-26
- Defining Common Tasks, page 9-26
- Defining Custom Attributes, page 9-29

Step 4 Click **Submit**.

The shell profile is saved. The Shell Profiles page appears with the shell profile that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29
- Deleting an Authorizations and Permissions Policy Element, page 9-33
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-35

Defining General Shell Profile Properties

Use this page to define a shell profile's general properties.

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then do one of the following:

- Click **Create**.
- Check the check box next to the shell profile that you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

Step 2 Complete the Shell Profile: General fields as described in Table 9-8:

Table 9-8 Shell Profile: General Page

Option	Description
Name	The name of the shell profile.
Description	(Optional) The description of the shell profile.

Step 3 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **Common Tasks** tab to configure privilege levels for the authorization profile; see Defining Common Tasks, page 9-26.
- The **Custom Attributes** tab to configure RADIUS attributes for the authorization profile; see Defining Custom Attributes, page 9-29.

Related Topics

- Defining Common Tasks, page 9-26
- Defining Custom Attributes, page 9-29

Defining Common Tasks

Use this page to define a shell profile's privilege level and attributes. The attributes are defined by the TACACS+ protocol.

For a description of the attributes, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then click:

- **Create** to create a new shell profile, then click **Common Tasks**.
- **Duplicate** to duplicate a shell profile, then click **Common Tasks**.
- **Edit** to edit a shell profile, then click **Common Tasks**.

Step 2 Complete the Shell Profile: Common Tasks page as described in Table 9-9:

Table 9-9 Shell Profile: Common Tasks

Option	Description
Privilege Level	
Default Privilege	(Optional) Enables the initial privilege level assignment that you allow for a client, through shell authorization. If disabled, the setting is not interpreted in authorization and permissions.
	The **Default Privilege Level** specifies the default (initial) privilege level for the shell profile. If you select **Static** as the Enable Default Privilege option, you can select the default privilege level; the valid options are 0 to 15. If you select **Dynamic** as the Enable Default Privilege option, you can select attribute from dynamic ACS dictionary, for a substitute attribute.
Maximum Privilege	(Optional) Enables the maximum privilege level assignment for which you allow a client after the initial shell authorization.
	The **Maximum Privilege Level** specifies the maximum privilege level for the shell profile. If you select the Enable Change of Privilege Level option, you can select the maximum privilege level; the valid options are 0 to 15. If you choose both default and privilege level assignments, the default privilege level assignment must be equal to or lower than the maximum privilege level assignment.
Shell Attributes	
Select **Not in Use** for the options provided below if you do not want to enable them. If you select **Dynamic**, you can substitute the static value of a TACACS+ attribute with a value of another attribute from one of the listed dynamic dictionaries	
Access Control List	(Optional) Choose **Static** to specify the name of the access control list to enable it. The name of the access control list can be up to 27 characters, and cannot contain the following: A hyphen (-), left bracket ([), right bracket, (]) forward slash (/), back slash (\), apostrophe (‘), left angle bracket (<), or right angle bracket (>). Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
Auto Command	(Optional) Choose **Static** and specify the command to enable it. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
No Callback Verify	(Optional) Choose **Static** to specify whether or not you want callback verification. Valid options are: • True—Specifies that callback verification is not needed. • False—Specifies that callback verification is needed. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
No Escape	(Optional) Choose **Static** to specify whether or not you want escape prevention. Valid options are: • True—Specifies that escape prevention is enabled. • False—Specifies that escape prevention is not enabled. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
No Hang Up	(Optional) Choose **Static** to specify whether or not you want any hangups. Valid options are: • True—Specifies no hangups are allowed. • False—Specifies that hangups are allowed. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.

Table 9-9 Shell Profile: Common Tasks

Option	Description
Timeout	(Optional) Choose **Static** to enable and specify, in minutes, the duration of the allowed timeout in the value field. The valid range is from 0 to 999. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
Idle Time	(Optional) Choose **Static** to enable and specify, in minutes, the duration of the allowed idle time in the value field. The valid range is from 0 to 999. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
Callback Line	(Optional) Choose **Static** to enable and specify the callback phone line in the value field. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.
Callback Rotary	(Optional) Choose **Static** to enable and specify the callback rotary phone line in the value field. Choose **Dynamic** to select attribute from dynamic ACS dictionary, for a substitute attribute.

Step 3 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **General** tab to configure the name and description for the authorization profile; see Defining General Shell Profile Properties, page 9-26.
- The **Custom Attributes** tab to configure Custom Attributes for the authorization profile; see Defining Custom Attributes, page 9-29.

To substitute the static value of a TACACS+ attribute with a value of another attribute from one of the listed dynamic dictionaries, complete the following steps.

Step 1 Select **System Administration > Configuration > Dictionaries > Identity > Internal Users** to add attributes to the Internal Users Dictionary.

Step 2 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** to create a Shell Profile.

Step 3 Select **Custom Attributes** tab to create a new attribute and choose **Dynamic** as Attribute Value and correlate it to created attribute in Internal Users Dictionary.

Step 4 Create a new rule in **Access Policies > Access Services > Default Device Admin > Authorization** and choose the Results created as Shell Profile instead.

After authorization you will see the response as dynamic attribute value from Internal ID Store.

Related Topics

- Defining Custom Attributes, page 9-29
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-35

Defining Custom Attributes

Use this tab to define custom attributes for the shell profile. This tab also displays the Common Tasks Attributes that you have chosen in the Common Tasks tab.

Step 1 Edit the fields in the Custom Attributes tab as described in Table 9-10:

Table 9-10 Shell Profile: Custom Attributes Page

Option	Description
Common Tasks Attributes	Displays the names, requirements, and values for the Common Tasks Attributes that you have defined in the Common Tasks tab.
Manually Entered	Use this section to define custom attributes to include in the authorization profile. As you define each attribute, its name, requirement, and value appear in the table. To: • Add a custom attribute, fill in the fields below the table and click **Add**. • Edit a custom attribute, select the appropriate row in the table and click **Edit**. The custom attribute parameters appear in the fields below the table. Edit as required, then click **Replace**.
Attribute	Name of the custom attribute.
Requirement	Choose whether this custom attribute is Mandatory or Optional.
Attribute Value	Choose whether the custom attribute is Static or Dynamic.

Step 2 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **General** tab to configure the name and description for the authorization profile; see Defining General Shell Profile Properties, page 9-26.
- The **Common Tasks** tab to configure the shell profile's privilege level and attributes for the authorization profile; see Defining Common Tasks, page 9-26.

Related Topics

- Defining General Shell Profile Properties, page 9-26
- Defining Common Tasks, page 9-26

Creating, Duplicating, and Editing Command Sets for Device Administration

Command sets provide decisions for allowed commands and arguments for device administration. You can specify command sets as results in a device configuration authorization policy. Shell profiles and command sets are combined for authorization purposes, and are enforced for the duration of a user's session.

You can duplicate a command set if you want to create a new command set that is the same, or similar to, an existing command set. After duplication is complete, you access each command set (original and duplicated) separately to edit or delete them.

After you create command sets, you can use them in authorizations and permissions within rule tables. A rule can contain multiple command sets. See Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24.

Note Command sets support TACACS+ protocol attributes only.

To create, duplicate, or edit a new command set:

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Command Sets**.

The Command Sets page appears.

Step 2 Do one of the following:

- Click **Create**.

  The Command Set Properties page appears.

- Check the check box next to the command set that you want to duplicate and click **Duplicate**.

  The Command Set Properties page appears.

- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

  The Command Set Properties page appears.

- Click **File Operations** to perform any of the following functions:
  - Add—Choose this option to add command sets from the import file to ACS.
  - Update—Choose this option to replace the list of command sets in ACS with the list of command sets in the import file.
  - Delete—Choose this option to delete the command sets listed in the import file from ACS.

  See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.

- Click **Export** to export the command sets from ACS to your local hard disk.

  A dialog box appears, prompting you to enter an encryption password to securely export the command sets:

a. Check the **Password** check box and enter the password to encrypt the file during the export process, then click **Start Export**.

b. Click **Start Export** to export the command sets without any encryption.

Step 3 Enter valid configuration data in the required fields.

As a minimum configuration, you must enter a unique name for the command set; all other fields are optional. You can define commands and arguments; you can also add commands and arguments from other command sets.

See Table 9-11 for a description of the fields in the Command Set Properties page.

Table 9-11 Command Set Properties Page

Field	Description
Name	Name of the command set.
Description	(Optional) The description of the command set.
Permit any command that is not in the table below	Check to allow all commands that are requested, unless they are explicitly denied in the Grant table. Uncheck to allow only commands that are explicitly allowed in the Grant table.
Command Set table	Use this section to define commands to include in the authorization profile. As you define each command, its details appear in the table. To: • Add a command, fill in the fields below the table and click **Add**. • Edit a command, select the appropriate row in the table, and click **Edit**. The command parameters appear in the fields below the table. Edit as required, then click **Replace**. The order of commands in the Command Set table is important; policy rule table processing depends on which command and argument are matched first to make a decision on policy result choice. Use the control buttons at the right of the Command Set table to order your commands.
Grant	Choose the permission level of the associated command. Options are: • Permit—The associated command and arguments are automatically granted. • Deny—The associated command and arguments are automatically denied. • Deny Always—The associated command and arguments are always denied.
Command	Enter the command name. This field is not case sensitive. You can use the asterisk (*) to represent zero (0) or more characters in the command name, and you can use the question mark (?) to represent a single character in a command name. Examples of valid command name entries: • SHOW • sH* • sho? • Sh*?
Arguments (field)	Enter the argument associated with the command name. This field is not case sensitive. ACS 5.4 uses standard UNIX-type regular expressions.
Select Command/ Arguments from Command Set	To add a command from another command set: 1. Choose the command set. 2. Click **Select** to open a page that lists the available commands and arguments. 3. Choose a command and click **OK**.

Step 4 Click **Submit**.

The command set is saved. The Command Sets page appears with the command set that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24
- Deleting an Authorizations and Permissions Policy Element, page 9-33
- Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24

Creating, Duplicating, and Editing Downloadable ACLs

You can define downloadable ACLs for the Access-Accept message to return. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols, and more by using the RADIUS protocol.

After you create downloadable ACLs as named permission objects, you can add them to authorization profiles, which you can then specify as the result of an authorization policy.

You can duplicate a downloadable ACL if you want to create a new downloadable ACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each downloadable ACL (original and duplicated) separately to edit or delete them.

To create, duplicate or edit a downloadable ACL:

Step 1 Select **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs**.

The Downloadable ACLs page appears.

Step 2 Do one of the following:

- Click **Create**.

  The Downloadable ACL Properties page appears.

- Check the check box next to the downloadable ACL that you want to duplicate and click **Duplicate**.

  The Downloadable ACL Properties page appears.

- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

  The Downloadable ACL Properties page appears.

- Click **File Operations** to perform any of the following functions:
  - Add—Choose this option to add ACLs from the import file to ACS.
  - Update—Choose this option to replace the list of ACLs in ACS with the list of ACLs in the import file.
  - Delete—Choose this option to delete the ACLs listed in the import file from ACS.

  See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.

- Click **Export** to export the DACLs from ACS to your local hard disk.

  A dialog box appears, prompting you to enter an encryption password to securely export the DACLs:
  - Check the **Password** check box and enter the password to encrypt the file during the export process, then click **Start Export**.

– Click **Start Export** to export the DACLs without any encryption.

Step 3 Enter valid configuration data in the required fields as shown in Table 9-12, and define one or more ACLs by using standard ACL syntax.

Table 9-12 Downloadable ACL Properties Page

Option	Description
Name	Name of the DACL.
Description	Description of the DACL.
Downloadable ACL Content	Define the ACL content. Use standard ACL command syntax and semantics. The ACL definitions comprise one or more ACL commands; each ACL command must occupy a separate line. For detailed ACL definition information, see the command reference section of your device configuration guide.

Step 4 Click **Submit**.

The downloadable ACL is saved. The Downloadable ACLs page appears with the downloadable ACL that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Configuring a Session Authorization Policy for Network Access, page 10-30
- Deleting an Authorizations and Permissions Policy Element, page 9-33

Deleting an Authorizations and Permissions Policy Element

To delete an authorizations and permissions policy element:

Step 1 Select **Policy Elements > Authorization and Permissions;** then, navigate to the required option.

The corresponding page appears.

Step 2 Check one or more check boxes next to the items that 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 page appears without the deleted object.

Configuring Security Group Access Control Lists

Security group access control lists (SGACLs) are applied at Egress, based on the source and destination SGTs. Use this page to view, create, duplicate and edit SGACLs. When you modify the name or content of an SGACL, ACS updates its generation ID. When the generation ID of an SGACL changes, the relevant Security Group Access network devices reload the content of the SGACL.

SGACLs are also called role-based ACLs (RBACLs).

Step 1 Select **Policy Elements > Authorizations and Permissions > Named Permissions Objects > Security Group ACLs**.

The Security Group Access Control Lists page appears with the fields described in Table 9-13:

Table 9-13 Security Group Access Control Lists Page

Option	Description
Name	The name of the SGACL.
Description	The description of the SGACL.

Step 2 Click one of the following options:

- **Create** to create a new SGACL.
- **Duplicate** to duplicate an SGACL.
- **Edit** to edit an SGACL.

Step 3 Complete the fields in the Security Group Access Control Lists Properties page as described in Table 9-14:

Table 9-14 Security Group Access Control List Properties Page

Option	Description
General	
Name	Name of the SGACL. You cannot use spaces, hyphens (-), question marks (?), or exclamation marks (!) in the name. After you create an SGACL, its generation ID appears.
Generation ID	*Display only.* ACS updates the generation ID of the SGACL if you change the: • Name of the SGACL. • Content of the SGACL (the ACEs). Changing the SGACL description does not affect the generation ID.
Description	Description of the SGACL.
Security Group ACL Content	Enter the ACL content. Ensure that the ACL definition is syntactically and semantically valid.

Step 4 Click **Submit**.