



Shared Profile Components

This chapter contains information about the features in the Shared Profile Components section of the web interface for the Cisco Secure Access Control Server Release 4.1, hereafter referred to as ACS.

This chapter contains the following topics:

- [About Shared Profile Components, page 4-1](#)
- [Network Access Filters, page 4-2](#)
- [RADIUS Authorization Components, page 4-6](#)
- [Downloadable IP ACLs, page 4-13](#)
- [Network Access Restrictions, page 4-18](#)
- [Command Authorization Sets, page 4-25](#)

About Shared Profile Components

You use the Shared Profile Components section to develop and name reusable, shared sets of authorization components that may be applied to one or more users or groups of users, and referenced by name within their profiles. These include network-access filters (NAFs), RADIUS Authorization Components (RACs), downloadable IP access control lists (IP ACLs), Network Access Restrictions (NARs), and command-authorization sets.

The Shared Profile Components section addresses the scalability of selective authorization. Shared profile components can be configured and then applied to many users or groups. Without this ability, you could only accomplish flexible and comprehensive authorization explicitly configuring the authorization of each user group on each device. Creating and applying these named shared-profile components (downloadable IP ACLs, NAFs, RACs, NARs, and command-authorization sets) makes it unnecessary to repeatedly enter long lists of devices or commands when defining network-access parameters.

This section contains the following topic:

[802.1X Example Setup, page 4-2](#)

802.1X Example Setup

Table 4-1 describes an example scenario to help you understand how SPCs are deployed. If, for example, you are deploying 802.1X and Network Admission Control (NAC), you might configure:

Table 4-1 802.1X Example SPC Scenario

Shared Profile Component	Description	Notes
Network Access Filters	NAFs are the most common way of defining which devices will be part of a given network service and, therefore, Network Access Profile (NAP).	<ul style="list-style-type: none"> • If you have switches or routers being upgraded for NAC, you can use a NAF to distinguish between those devices that can and cannot do NAC. • If you have Network Device Groups (NDGs) for groups of devices based on geography, NAFs allow you to aggregate the NDGs. In this case, you might want to set up a NAF for each NAP configured.
ACLs	NAC uses ACLs in order to manage clients that required limited access (for example, if there is no NAC-suppliant or to enforce an upgrade policy).	<ul style="list-style-type: none"> • Create ACLs related to posture and NAC agentless hosts (NAH). • Use ACLs to control access to servers running network applications (such as software for sales, human resource, or accounting) which can be mapped from the users group. For example, the HR group gets an HR ACL.
RACs	Use RACs to set up service-differentiated RADIUS authorization.	<ul style="list-style-type: none"> • Set up RACs for each network service (VPN, WLAN, dial, and so on). For example, set different session-timeouts for VPN and WLAN. • Use NAP templates to save time setting up 802.1X profiles. They require different provisioning and so require SRACs for each.
NARs	Use NARs to create additional conditions that must be met before a user can access the network. ACS applies these conditions by using information from attributes sent by authentication, authorization, and accounting (AAA) clients.	<ul style="list-style-type: none"> • Create a CLI/DNIS NAR listing the MAC addresses of all the non-NAC devices (maybe a printer or legacy system) that are allowed to access the network. This method will protect your network. • With NAC, use NARs for NAH scenarios with MAC and IP exceptions handling. Wildcarding the MAC and IP addresses is allowed.

Network Access Filters

This section describes NAFs and provides instructions for creating and managing them.

This section contains the following topics:

- [About Network Access Filters, page 4-3](#)
- [Adding a Network Access Filter, page 4-3](#)
- [Editing a Network Access Filter, page 4-5](#)
- [Deleting a Network Access Filter, page 4-6](#)

About Network Access Filters

A NAF is a named group of any combination of one or more of the following network elements:

- IP addresses
- AAA clients (network devices)
- Network device groups (NDGs)

Using a NAF to specify a downloadable IP ACL or NAR—based on the AAA clients by which the user may access the network—saves you the effort of listing each AAA client explicitly. NAFs are the most common way of defining which devices will be part of a given network service and, therefore, Network Access Profile (NAP). NAFs exhibit the following characteristics:

- **NAFs in downloadable IP ACLs**—You can associate a NAF with specific ACL contents. A downloadable IP ACL comprises one or more ACL contents (sets of ACL definitions) that are associated with a single NAF or, by default, “All-AAA-Clients”. This pairing of ACL content with a NAF permits ACS to determine which ACL content is downloaded according to the IP address of the AAA client making the access request. For more information on using NAFs in downloadable IP ACLs, see [About Downloadable IP ACLs, page 4-13](#).
- **NAFs in shared Network Access Restrictions**—An essential part of specifying a shared NAR is listing the AAA clients from which user access is permitted or denied. Rather than list every AAA client that makes up a shared NAR, you can simply list one or more NAFs instead of, or in combination with, individual AAA clients. For more information on using NAFs in shared NARs, see [About Network Access Restrictions, page 4-18](#).



Tip

Shared NARs can contain NDGs, or NAFs, or both. NAFs can contain one or more NDGs.

You can add a NAF that contains any combination of NDG, network devices (AAA clients), or IP addresses. For these network devices or NDGs to be selectable you must have previously configured them in ACS.

The network elements that a NAF comprises can be arranged in any order. For best performance, place the elements most commonly encountered at the top of the Selected Items list. For example, in a NAF where the majority of users gain network access through the NDG accounting, but you also grant access to a single technical support AAA client with the IP address 205.205.111.222, you would list the NDG first (higher) in the list of network elements to prevent all NAF members from having to be examined against the specified IP address.

Adding a Network Access Filter

To add a NAF:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Network Access Filtering**.
The Network Access Filtering table page appears.



Tip If Network Access Filtering does not appear as a selection on the Shared Profile Components page, you must enable it on the Advanced Options page of the Interface Configuration section.

Step 3 Click **Add**.

The Network Access Filtering edit page appears.

Step 4 In the **Name** box, type the name of the new network-access filter.



Note The name of a NAF can contain up to 31 characters. Spaces are not allowed. Names cannot contain: left bracket ([), right bracket (]), comma(,), slash (/), dash (-), hyphen (-), quotes (“), apostrophe (‘), right angle bracket (>), left angle bracket (<).

Step 5 In the **Description** box, type a description of the new network-access filter. The description can be up to 1,000 characters.

Step 6 Add network elements to the NAF definition as applicable:

- a. To include an NDG in the NAF definition, from the **Network Device Groups** box, select the NDG; then click -> (right arrow button) to move it to the **Selected Items** box.
- b. To include a AAA client in the NAF definition, from the **Network Device Groups** box, select the applicable NDG and then, from the **Network Devices** box, select the AAA client you want to include. Finally, click --> (right arrow button) to move it to the **Selected Items** box.



Tip If you are using NDGs, the AAA clients appear in the Network Devices box only when you have selected the NDG to which they belong. Otherwise, if you are not using NDGs, you can select the AAA client from the **Network Devices** box with no prior NDG selection.

- c. To include an IP address in the NAF definition, type the IP address in the **IP Address** box. Click --> (right arrow button) to move it to the **Selected Items** box.



Note You can use the asterisk (*), which is the wildcard character, to designate a range within an IP address.

Step 7 Ensure that the order of the items is correct. To change the order of items, in the **Selected Items** box, click the name of an item, and then click **Up** or **Down** to move it to the position that you want.



Tip You can also remove an item from the Selected Items box by selecting the item and then clicking <-- (left arrow button) to remove it from the list.

Step 8 To save your NAF and apply it immediately, choose **Submit + Apply**.



Tip To save your NAF and apply it later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.





Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to zero (0).

The Network Access Filtering table page appears, and lists the name and description of the new NAF.

Editing a Network Access Filter

To edit a NAF:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Network Access Filtering**.
The Network Access Filtering table appears.
- Step 3** In the Name column, click the NAF that you want to edit.
The Network Access Filter page appears with information visible for the selected NAF.
- Step 4** Edit the Name or Description of the NAF; type and delete information, as applicable. The description can be up to 1,000 characters.
-
-  **Caution** If you change the name of a NAF, you invalidate all existing references to that NAF; this action might affect the access of users or groups that are associated with NARs or downloadable ACLs that use that NAF.
-
- Step 5** To add a NDG to the NAF definition, from the Network Device Groups box, select the NDG that you want to add. Click --> (right arrow button) to move it to the **Selected Items** box.
- Step 6** To add a AAA client in the NAF definition, from the **Network Device Groups** box select the applicable NDG and then, from the Network Devices box, select the AAA client that you want to add. Click --> (right arrow button) to move it to the Selected Items box.
-
-  **Tip** If you are not using NDGs, you begin by selecting the AAA client from the **Network Devices** box.
-
- Step 7** To add an IP address to the NAF definition, in the **IP Address** box, type the IP address that you want to add. Click --> (right arrow button) to move it to the **Selected Items** box.
- Step 8** To edit an IP address, choose it in the **Selected Items** box and then click <-- (left arrow button) to move it to the IP address box. Type the changes to the IP address and then click --> (right arrow button) to move it back to the **Selected Items** box.
- Step 9** To remove an element from the **Selected Items** box, choose the item and then click <-- (left arrow button) to remove it.
- Step 10** To change the order of items, in the **Selected Items** box, click the name of an item, and then click **Up** or **Down** to move it into the position that you want. For more information on arranging the order of NAFs see [About Network Access Filters, page 4-3](#).

Step 11 To save the changes to your NAF and apply them immediately, click **Submit + Apply**.



Tip

To save your NAF and apply it later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.



Note

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to zero (0).

ACS reenters the NAF with the new information, which takes effect immediately.

Deleting a Network Access Filter

Before You Begin

Before you delete a NAF you should remove its association with any NAR, downloadable IP ACL, or network access profile that uses it. Otherwise, any NAR, downloadable IP ACL, or network access profile that references the deleted NAF will be misconfigured and will produce an error.

To delete a NAF:

Step 1 In the navigation bar, click **Network Access Filtering**.

The Network Access Filtering table page appears.

Step 2 Click the name of the NAF that you want to delete.

The Network Access Filtering edit page appears.

Step 3 Click **Delete** and then click **OK** to confirm.

The Network Access Filtering table page appears with the name and description of the NAF removed from the table.

RADIUS Authorization Components

This section describes RADIUS Authorization Components (RACs) and provides instructions for configuring and managing them.

The following topics are described:

- [About RADIUS Authorization Components, page 4-7](#)
- [Before You Begin Using RADIUS Authorization Components, page 4-8](#)
- [Adding RADIUS Authorization Components, page 4-10](#)
- [Cloning a RADIUS Authorization Component, page 4-10](#)
- [Editing a RADIUS Authorization Component, page 4-11](#)
- [Deleting a RADIUS Authorization Component, page 4-11](#)

About RADIUS Authorization Components

Shared Radius Authorization Components (RACs) contain groups of RADIUS attributes that you can dynamically assign to user sessions based on a policy. Using the Network Access Profile configuration, you can map a policy type with set conditions, such as Network Device Groups and posture, to a shared RAC.

Understanding RACs and NAPs

ACS RACs contain a set of attributes (also referred to as a network-access profile) that can be specific to a single network device, or to several network devices. The authorization policy maps from various groups and postures to a set of RACs and ACLs. For more information on setting up network-access profiles, see [Chapter 14, “Network Access Profiles.”](#)

ACS user groups contain attributes that are related to the type of user (for example, administrators, contractors, and so on) and do not cater to the same groups of users that require authorization for different network services (WLAN and VPN, for example).

RACs hold attributes that can be specific to a single network profile by using authorization policies. RACs also can be used by several different network profiles. You can map from various groups and postures to a set of RACs and ACLs. Use RACs with NAPs when you require service-differentiated RADIUS authorization. For example, when you must set the session-timeout to be several days for VPN and several hours for WLAN.

You can use group attributes so that you can apply service-independent attributes to all users of the group without having to duplicate each RAC for each profile. You can configure RADIUS attributes in three places:

- RAC
- Group level
- User level

You can use the authorization policy to indicate if you want to include attributes from the group, the user, or both.

If your network strategy demands policy-based profiles, we recommend that you use RACs instead of groups. You must define appropriate access services and policies:

- Plan what user group and posture should get which level of authorization.
- Identify all similar authorization cases and create RACs for them.
- Remove any legacy attributes from the user groups if necessary.
- Define appropriate network-access policies and define rules.

You can create a base template authorization at group level and then supply the profile-specific attributes by using RACs. For example, setting a different Session-Timeout for VPN and WLAN.

Vendors

**Note**

RADIUS security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco IOS/PIX 6.0) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco IOS/PIX 6.0) in the Authenticate Using list.

The RADIUS vendor-specific attribute (VSA) sets that ACS supports are:

- **Cisco Aironet**—VSAs for Cisco Aironet Access Point products. *Not* supported for shared RAC; use IETF session timeout instead.
- **Cisco Airespace**—VSAs for Cisco Airespace wireless LAN devices.
- **Cisco BBSM**—VSAs for Cisco Building Broadband Service Manager (BBSM) products.
- **Cisco IOS/PIX 6.0**—VSAs for Cisco IOS products and Cisco PIX firewalls earlier than 6.0 releases.
- **Cisco VPN 3000/ASA/PIX 7.x+**—VSAs for Cisco VPN 3000-series Concentrators, ASA devices, and PIX devices later than 7.x releases.
- **Cisco VPN 5000**—VSAs for Cisco VPN 5000-series Concentrators.
- **Ascend**—VSAs for Ascend products.
- **Microsoft**—VSAs for Microsoft Point-to-Point Encryption and Point-to-Point Compression.
- **Nortel**—VSAs for Nortel products.
- **Juniper**—VSAs for Juniper products.

Attribute Types

The vendor-specific attributes are not defined. You can find definitions in the vendor’s software documentation. For Cisco vendor-specific attributes, see [Appendix C, “RADIUS Attributes.”](#)

ACS for Windows

You can import vendor-specific attributes by using the **CSUtil** command (see [Appendix D, “CSUtil Database Utility”](#)) or RDBMS Synchronization (see [Custom RADIUS Vendors and VSAs, page 8-19](#)).

ACS Solution Engine

You can import vendor-specific attributes by using RDBMS Synchronization, see [Custom RADIUS Vendors and VSAs, page 8-19](#).

Before You Begin Using RADIUS Authorization Components

For you to use the Shared Profile Components’ RACs, you must ensure that you have properly set up ACS. Review this checklist before you create shared profile components:



Tip

Use the Network Access Profile templates to save time. NAP templates automatically create a set of shared profile components if none are configured. For details, see [Using Profile Templates, page 14-7](#).

1. Add devices to ACS. For ACS to interact with AAA clients and servers you must add their network information. For instructions on how to add devices by using Network Configuration, see [Adding AAA Clients, page 3-11](#).
2. Enable the attributes (VSAs) that you want to use. Disable those attributes that you do not want to use. If attributes are not enabled, they will not appear on the RADIUS Authorization Components page, the Interface Configuration set up pages. For details on enabling VSAs, see [Chapter 2, “Using the Web Interface”](#)

3. Map out your network access profile design. You must identify the network services that require provisioning. You will probably identify at least one shared RADIUS authorization component (SRAC) for each profile. For details on linking a SRAC to a profile, see [Classification of Access Requests, page 14-2](#) or [Using Profile Templates, page 14-7](#).
4. For each profile that you are creating, identify how you plan to classify network-access requests and any exception cases (for example, special users or groups, bad posture status, and so on) and create SRACs for each. See [About RADIUS Authorization Components, page 4-7](#).
5. Decide whether any attributes are user or group-specific (rather than network service-specific). If you must assign attributes to a user or group, regardless of network service, add these to the user or group record and enable attribute merging in the network access profile. For details on attribute merging, see [Merging Attributes, page 14-31](#).

For specific steps on enabling RADIUS Authorization Components, see [Enabling Use of RAC, page 4-9](#).

Enabling Use of RAC

To enable use of RAC:

Step 1 Before setting RADIUS Authorization Components, add your devices by using Network Configuration and configure them to authenticate by using the correct security protocol (such as RADIUS Cisco VPN 3000/ASA/PIX 7.x+).

If your attribute does not appear in the Authenticate Using list, check the Interface Configuration or your User Setup/Group Setup parameters.

Step 2 In the navigation bar, click **Interface Configuration** and select **RADIUS (IETF)**.



Note RADIUS security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) in the Authenticate Using list.

Step 3 Select the desired RADIUS attributes and click **Submit**.

Step 4 Repeat [Step 2](#) and [Step 3](#) for each RADIUS security protocol in your network configuration.

Step 5 Ensure that Tunneling RADIUS attributes are selected in Advanced Options.

- Choose **Interface Configuration > RADIUS (IETF)**.
- Choose the Tunnel attributes.
- Click **Submit**.

Step 6 In the navigation bar, click **Shared Profile Components** and select **RADIUS Authorization Components**.

For details on adding RACs, see [Adding RADIUS Authorization Components, page 4-10](#). For details on changing RACs, see [Editing a RADIUS Authorization Component, page 4-11](#). For details on how to add RACs to network access profiles, see [Configuring an Authorization Rule, page 14-31](#).

Adding RADIUS Authorization Components

Before You Begin

You should have already configured any RADIUS options that you plan to use on ACS. For details on what to configure, see [Vendors, page 4-7](#).

To add a RAC:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **RADIUS Authorization Components**.
The RADIUS Authorization Components Table Page appears.
- Step 3** Click **Add** to create a new RADIUS Authorization Component.
The Edit RADIUS Authorization Component Page appears.
- Step 4** To add a new attribute, select the correct vendor attribute by using the drop-down list and click the **Add** button.
The RAC Attribute Add/Edit Page appears.



Note The vendors that are available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at the group or user level) under Interface Configuration.

- Step 5** Select the attribute value and click **Submit**.
-

Cloning a RADIUS Authorization Component

To make a copy of an existing RAC by using the clone feature:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **RADIUS Authorization Components**.
The RADIUS Authorization Components Table Page appears.
- Step 3** Select the RAC name of the component that you want to clone.
The Edit RADIUS Authorization Component Page appears.
- Step 4** To clone an existing RAC with all of its attributes, click **Clone**.
A clone named Copy of RACname is created in the Edit RADIUS Authorization Component page.
- Step 5** Click **Submit to save the new RAC**.
-

Editing a RADIUS Authorization Component

To edit an existing RAC:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
 - Step 2** Click **RADIUS Authorization Components**.
The RADIUS Authorization Components Table Page appears.
 - Step 3** Select the RAC name of the component that you want to edit.
The Edit RADIUS Authorization Component Page appears.
 - Step 4** To add a new attribute, select the correct vendor attribute by using the drop-down list and click the adjacent **Add** button.
 - Step 5** To alter an existing attribute, select the value in Assigned Attributes.
The RAC Attribute Add/Edit Page appears.
To delete an attribute and its value, click **Delete**.
 - Step 6** Select the attribute value and click **Submit**.
-

Deleting a RADIUS Authorization Component

Before You Begin

You should remove the association of an RAC with any network access profile before deleting the RAC.

To delete an RAC:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
 - Step 2** Click **RADIUS Authorization Components**.
The RADIUS Authorization Components Table Page appears.
 - Step 3** Select the RAC name of the component that you want to delete.
The Edit RADIUS Authorization Component Page appears.
 - Step 4** Click **Delete** to remove the RADIUS Authorization Component.
 - Step 5** Click **OK** to remove the RADIUS Authorization Component.
The current configuration changes. A dialog box appears and asks that you restart ACS by choosing **System Configuration > Service Control** to adopt the new settings.
-

RADIUS Authorization Components Table Page

You use this page to list defined RACs, display defined RAC configurations, or add a new RAC name. [Table 4-2](#) describes the fields on this page.

Table 4-2 RAC Display Fields

Field	Description
Name	Click to display the configuration for the RAC. Opens the Edit RADIUS Authorization Component Page.
Description	Displays the RAC description. The description can be up to 1,000 characters.
Add	Click to add a new RAC. Opens the Edit RADIUS Authorization Component Page.

Edit RADIUS Authorization Component Page

You use this page to configure the RAC. [Table 4-3](#) describes the RAC configuration fields.

Table 4-3 RAC Configuration Fields

Field	Description
Name	Enter the name that you want to assign to the RADIUS Authorization Components.
Description	Enter a description for the RAC. The description can be up to 1,000 characters.
Add New Attribute	Use the Vendor and Service Type fields to add new attribute values. Vendors available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at group level) under Interface Configuration. For details on setting up devices, see Chapter 3, “Network Configuration.” For details on setting up the interface, see Chapter 2, “Using the Web Interface” . Select the vendor attribute from the drop-down list and click Add . This action opens the RAC Attribute Add/Edit Page .
Assigned Attributes	Use this table to view, edit, and select the list of RADIUS attributes assigned to the Authorization Component. To edit or delete an already assigned attribute, click on the attribute value. Opens the RAC Attribute Add/Edit Page .
Vendor Attribute Value	Appears if assigned attributes are present. Click on the value to edit or delete. Opens the RAC Attribute Add/Edit Page .
Submit	Click to submit the RAC configuration to ACS.
Delete	Appears if assigned attributes are present. Click to delete the RAC. To delete a single attribute, go to the RAC Attribute Add/Edit Page .

RAC Attribute Add/Edit Page

You use this page to add or edit RAC attributes. [Table 4-4](#) describes the fields on this page.

Table 4-4 Add or Edit RAC Attributes Fields

Field	Description
RAC	Name assigned to the RADIUS Authorization Component.
Vendor	Name of the organization the vendor-specific attributes.
Clone	Copy an existing RAC attributes into a new RAC named Copy of RAC name.
Attribute	Attribute defined for RAC.
Type	Attribute type of integer or text.
Value	Drop-down box or text value settings.
Submit	Click to submit the RAC configuration to ACS.
Delete	Click to delete this single attribute.

Downloadable IP ACLs

This section describes downloadable ACLs and provides detailed instructions for configuring and managing them.

This section contains the following topics:

- [About Downloadable IP ACLs, page 4-13](#)
- [Adding a Downloadable IP ACL, page 4-15](#)
- [Editing a Downloadable IP ACL, page 4-16](#)
- [Deleting a Downloadable IP ACL, page 4-17](#)

About Downloadable IP ACLs

You can use downloadable IP ACLs to create sets of ACL definitions that you can apply to many users or user groups. These sets of ACL definitions are called ACL contents. Also, by incorporating NAFs, you can control the ACL contents that are sent to the AAA client from which a user is seeking access. That is, a downloadable IP ACL comprises one or more ACL content definitions, each of which is associated with a NAF or (by default) associated to all AAA clients. (The NAF controls the applicability of specified ACL contents according to the AAA client's IP address. For more information on NAFs and how they regulate downloadable IP ACLs, see [About Network Access Filters, page 4-3](#)).

Downloadable IP ACLs operate this way:

1. When ACS grants a user access to the network, ACS determines whether a downloadable IP ACL is assigned to that user or the user's group.
2. If ACS locates a downloadable IP ACL that is assigned to the user or the user's group, it determines whether an ACL content entry is associated with the AAA client that sent the RADIUS authentication request.
3. ACS sends, as part of the user session, RADIUS access-accept packet an attribute specifying the named ACL and the version of the named ACL.

4. If the AAA client responds that it does not have the current version of the ACL in its cache (that is, the ACL is new or has changed), ACS sends the ACL (new or updated) to the device.

Downloadable IP ACLs are an alternative to configuring ACLs in the RADIUS Cisco **cisco-av-pair** attribute [26/9/1] of each user or user group. You can create a downloadable IP ACL once, give it a name, and then assign the downloadable IP ACL to each applicable user or user group by referencing its name. This method is more efficient than configuring the RADIUS Cisco **cisco-av-pair** attribute for each user or user group.

Further, by employing NAFs, you can apply different ACL contents to the same user or group of users, according to the AAA client that they are using. No additional configuration of the AAA client is necessary after you have configured the AAA client to use downloadable IP ACLs from ACS. Downloadable ACLs are protected by the backup or replication regimen that you have established.

While entering the ACL definitions in the ACS web interface, do not use keyword and name entries; in all other respects, use standard ACL command syntax and semantics for the AAA client on which you intend to apply the downloadable IP ACL. The ACL definitions that you enter into ACS comprise one or more ACL commands. Each ACL command must be on a separate line.

You can add one or more named ACL contents to a downloadable IP ACL. By default each ACL content applies to all AAA clients; however, if you have defined NAFs, you can limit the applicability of each ACL content to the AAA clients that are listed in the NAF that you associate to it. That is, by employing NAFs, you can make each ACL content, within a single downloadable IP ACL, applicable to multiple different network devices or network device groups in accordance with your network security strategy. For more information on NAFs, see [About Network Access Filters, page 4-3](#).

Also, you can change the order of the ACL contents in a downloadable IP ACL. ACS examines ACL contents starting from the top of the table and downloads the *first* ACL content that it finds with a NAF that includes the AAA client that is being used. In setting the order, you should seek to ensure system efficiency by positioning the most widely applicable ACL contents higher on the list. You should realize that, if your NAFs include overlapping populations of AAA clients, you must proceed from the more specific to the more general. For example, ACS will download any ACL contents with the **All-AAA-Clients** NAF setting and not consider any that are lower on the list.

To use a downloadable IP ACL on a particular AAA client, the AAA client must:

- Use RADIUS for authentication.
- Support downloadable IP ACLs.

Examples of Cisco devices that support downloadable IP ACLs are:

- PIX Firewalls
- VPN 3000-series concentrators, ASA and PIX devices
- Cisco devices running IOS version 12.3(8)T or greater

[Example 4-1](#) shows the format that you should use to enter PIX Firewall ACLs in the ACL Definitions box.

Example 4-1

```
permit tcp any host 10.0.0.254
permit udp any host 10.0.0.254
permit icmp any host 10.0.0.254
permit tcp any host 10.0.0.253
```

[Example 4-2](#) shows the format that you should use to enter VPN 3000/ASA/PIX 7.x+ ACLs in the **ACL Definitions** box.

Example 4-2

```

permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80

```

For detailed ACL definition information, see the command reference section of your device configuration guide.

Adding a Downloadable IP ACL

Before You Begin

You should have already configured any NAFs that you intend to use in your downloadable IP ACL.

To add a downloadable IP ACL:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Downloadable IP ACLs**.



Tip

If Downloadable IP ACLs does not appear on the Shared Profile Components page, you must enable the User-Level Downloadable ACLs or Group-Level Downloadable ACLs option, or both, on the Advanced Options page of the Interface Configuration section.

Step 3 Click **Add**.

The Downloadable IP ACLs page appears.

Step 4 In the **Name** box, type the name of the new IP ACL.



Note

The name of an IP ACL may contain up to 27 characters. The name must *not* contain spaces nor any of the following characters: hyphen (-), left bracket ([), right bracket (]), slash (/), backslash (\), quotes ("), left angle bracket (<), right angle bracket (>), dash (-).

Step 5 In the **Description** box, type a description of the new IP ACL. The description can be up to 1,000 characters.

Step 6 To add an ACL content to the new IP ACL, click **Add**.

Step 7 In the **Name** box, type the name of the new ACL content.



Note The name of an ACL content may contain up to 27 characters. The name must *not* contain spaces nor any of the following characters: hyphen (-), left bracket ([), right bracket (]), slash (/), backslash (\), quotes ("), left angle bracket (<), right angle bracket (>), dash (-).

Step 8 In the **ACL Definitions** box, type the new ACL definition.



Tip In entering ACL definitions in the ACS web interface, you do not use keyword and name entries; rather, you begin with a **permit** or **deny** keyword. For examples of the proper format of the ACL definitions, see [Example 4-1 on page 4-14](#) and [Example 4-1 on page 4-14](#).

Step 9 To save the ACL content, click **Submit**.

The Downloadable IP ACLs page appears with the new ACL content listed by name in the ACL Contents column.

Step 10 To associate a NAF to the ACL content, select a NAF from the Network Access Filtering box to the right of the new ACL content. For information on adding a NAF see [Adding a Network Access Filter, page 4-3](#).



Note If you do not assign a NAF, ACS associates the ACL content to all network devices, which is the default.

Step 11 Repeat [Step 3](#) through [Step 10](#) until you have completely specified the new IP ACL.

Step 12 To set the order of the ACL contents, click the radio button for an ACL definition, and then click **Up** or **Down** to reposition it in the list.



Tip The order of ACL contents is significant. Working from top to bottom, ACS downloads only the *first* ACL definition that has an applicable NAF setting (including the **All-AAA-Clients** default setting if used). Typically your list of ACL contents will proceed from the one with the most specific (narrowest) NAF to the one with the most general (**All-AAA-Clients**) NAF.

Step 13 To save the IP ACL, click **Submit**.

ACS enters the new IP ACL, which takes effect immediately. For example, if the IP ACL is for use with PIX Firewalls, it is available to be sent to any PIX Firewall that is attempting authentication of a user who has that downloadable IP ACL assigned to his or her user or group profile. For information on assigning a downloadable IP ACL to user or a user group, see [Assigning a Downloadable IP ACL to a User, page 6-14](#), or [Assigning a Downloadable IP ACL to a Group, page 5-21](#).

Editing a Downloadable IP ACL

Before You Begin

You should have already configured any NAFs that you intend to use in your editing of the downloadable IP ACL.

To edit a downloadable IP ACL:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Downloadable IP ACLs**.
The Downloadable IP ACLs table appears.
- Step 3** In the Name column, click the IP ACL that you want to edit.
The Downloadable IP ACLs page appears and displays with information for the selected ACL.
- Step 4** Edit the Name or Description information, as applicable. The description can be up to 1,000 characters.
- Step 5** To edit ACL content, click on the ACL Contents entry that you want to change. For examples of the proper format of the ACL definitions, see [Example 4-1 on page 4-14](#) and [Example 4-1 on page 4-14](#).
The Downloadable IP ACL Content page appears.
- Step 6** Edit the Name or ACL Definitions, as applicable.



Tip Do not use keyword and name entries in the ACL Definitions box; instead, begin with a permit or deny keyword. For an example of the proper format of the ACL definitions, see [About Downloadable IP ACLs, page 4-13](#).

- Step 7** To save the edited ACL definition, click **Submit**.
- Step 8** To change the NAF that is associated with an ACL content, select a new NAF setting from the corresponding Network Access Filtering box. You can change as many of the NAF associations in a downloadable IP ACL as you want. For more information on NAFs, see [About Network Access Filters, page 4-3](#).
- Step 9** Repeat [Step 3](#) through [Step 8](#) until you are finished.
- Step 10** To change the order of the ACL contents, select the radio button for an ACL definition, and then click **Up** or **Down** to reposition it in the list.
- Step 11** To save the edited IP ACL, click **Submit**.
ACS saves the IP ACL with the new information, which takes effect immediately.
-

Deleting a Downloadable IP ACL

Before You Begin

You should remove the association of a IP ACL with any user, user group profile, or network access profile before deleting the IP ACL.

To delete an IP ACL:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Downloadable IP ACLs**.
- Step 3** Click the name of the downloadable IP ACL that you want to delete.

The Downloadable IP ACLs page appears and displays information for the selected IP ACL.

Step 4 At the bottom of the page, click **Delete**.

A dialog box warns you that you are about to delete an IP ACL.

Step 5 To confirm that you want to delete the IP ACL, click **OK**.

The selected IP ACL is deleted.

Network Access Restrictions

This section describes network access restrictions (NARs), and provides detailed instructions for configuring and managing shared NARs.

This section contains the following topics:

- [About Network Access Restrictions, page 4-18](#)
- [Adding a Shared NAR, page 4-21](#)
- [Editing a Shared NAR, page 4-23](#)
- [Deleting a Shared NAR, page 4-24](#)

About Network Access Restrictions

A network access restriction (NAR) is a definition, which you make in ACS, of additional conditions that you must meet before a user can access the network. ACS applies these conditions by using information from attributes that your AAA clients sent. Although you can set up NARs in several ways, they all are based on matching attribute information that a AAA client sent. Therefore, you must understand the format and content of the attributes that your AAA clients sends if you want to employ effective NARs.

In setting up a NAR you can choose whether the filter operates positively or negatively. That is, in the NAR you specify whether to permit or deny network access, based on information sent from AAA clients when compared to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied access. [Table 4-5](#) shows these conditions.

Table 4-5 NAR Permit or Deny Conditions

	IP-Based	Non-IP Based	Insufficient Information
Permit	Access Granted	Access Denied	Access Denied
Deny	Access Denied	Access Granted	Access Denied

ACS supports two types of NAR filters:

- **IP-based filters**—IP-based NAR filters limit access based on the IP addresses of the end-user client and the AAA client. For more information on this type of NAR filter, see [About IP-Based NAR Filters, page 4-19](#).
- **Non-IP-based filters**—Non-IP-based NAR filters limit access based on simple string comparison of a value sent from the AAA client. The value may be the calling line identification (CLI) number, the Dialed Number Identification Service (DNIS) number, the MAC address, or other value

originating from the client. For this type of NAR to operate, the value in the NAR description must exactly match what is being sent from the client, including whatever format is used. For example, the telephone number (217) 555-4534 does not match 217-555-4534. For more information on this type of NAR filter, see [About Non-IP-based NAR Filters](#), page 4-20.

You can define a NAR for, and apply it to, a specific user or user group. For more information, see [Setting Network Access Restrictions for a User](#), page 6-8, or [Setting Network Access Restrictions for a User Group](#), page 5-6. However, in the Shared Profile Components section of ACS you can create and name a *shared* NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the ACS web interface. Then, when you set up users or user groups, you can select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, you choose one of two access criteria:

- **All selected filters must permit**
- **Any one selected filter must permit**

You must understand the order of precedence that is related to the different types of NARs. The order of NAR filtering is:

1. Shared NAR at the user level
2. Shared NAR at the group level
3. Nonshared NAR at the user level
4. Nonshared NAR at the group level

You should also understand that denial of access at *any* level takes precedence over settings at another level that do not deny access. This is the one exception in ACS to the rule that user-level settings override group-level settings. For example, a particular user might have no NAR restrictions at the user level that apply; but, if that user belongs to a group that is restricted by a shared or nonshared NAR, the user is denied access.

Shared NARs are kept in the ACS internal database. You can use the ACS backup and restore features to back up, and restore them. You can also replicate the shared NARs, along with other configurations, to secondary ACSs.

About IP-Based NAR Filters

For IP-based NAR filters, ACS uses the attributes in [Table 4-6](#), depending on the AAA protocol of the authentication request.

Table 4-6 **Attributes for IP-Based NAR Filters**

Protocol	Attributes
TACACS+	The <code>rem_addr</code> field from the TACACS+ start packet body is used. Note When an authentication request is forwarded by proxy to an ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.
RADIUS IETF	The <code>calling-station-id</code> (attribute 31) must be used.

**Note**

IP-based NAR filters work only if ACS receives the Radius Calling-Station-Id (31) attribute. The Calling-Station-Id (31) must contain a valid IP address. If it does not, it will fall over to DNIS rules.

AAA clients that do not provide sufficient IP address information (for example, some types of firewall) do not support full NAR functionality.

[Table 4-7](#) describes additional attributes for IP-based restrictions, per protocol.

Table 4-7 *Attributes for IP-Based Restrictions*

Protocol	Attributes
TACACS+	<p>The NAR fields in ACS use the following values:</p> <ul style="list-style-type: none"> • AAA client—The <code>NAS-IP-address</code> is taken from the source address in the socket between ACS and the TACACS+ client. • Port—The <code>port</code> field is taken from the TACACS+ start packet body.

About Non-IP-based NAR Filters

A non-IP-based NAR filter (that is, a DNIS/CLI-based NAR filter) is a list of permitted or denied calling or point of access locations that you can use in restricting a AAA client when you do not have an established IP-based connection. The non-IP-based NAR feature generally uses the CLI number and the Dialed Number Identification Service (DNIS) number.

However, by entering an IP address in place of the CLI, you can use the non-IP-based filter; even when the AAA client does not use a Cisco IOS release that supports CLI or DNIS. In another exception to entering a CLI, you can enter a MAC address to permit or deny access; for example, when you are using a Cisco Aironet AAA client. Likewise, you could enter the Cisco Aironet AP MAC address in place of the DNIS. The format of what you specify in the CLI box—CLI, IP address, or MAC address—must match the format of what you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

[Table 4-6](#) shows the attributes for DNIS/CLI-based restrictions, per protocol.

Table 4-8 Attributes for DNIS/CLI-Based Restrictions

Protocol	Attributes
TACACS+	<p>The NAR fields can contain:</p> <ul style="list-style-type: none"> • AAA client—The <code>NAS-IP-address</code> is taken from the source address in the socket between ACS and the TACACS+ client. • Port—The <code>port</code> field in the TACACS+ start packet body is used. • CLI—The <code>rem-addr</code> field in the TACACS+ start packet body is used. • DNIS—The <code>rem-addr</code> field taken from the TACACS+ start packet body is used. In cases in which the <code>rem-addr</code> data begins with the slash (/) the DNIS field contains the <code>rem-addr</code> data without the slash (/). <p>Note When a proxy forwards an authentication request to an ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.</p>
RADIUS	<p>The NAR fields can contain:</p> <ul style="list-style-type: none"> • AAA client—The <code>NAS-IP-address</code> (attribute 4) or, if <code>NAS-IP-address</code> does not exist, <code>NAS-identifier</code> (RADIUS attribute 32) is used. • Port—The <code>NAS-port</code> (attribute 5) or, if <code>NAS-port</code> does not exist, <code>NAS-port-ID</code> (attribute 87) is used. • CLI—The <code>calling-station-ID</code> (attribute 31) must contain a valid IP address. If the <code>Calling-Station-Id</code> (31) does not contain a valid IP address, it will fall over to DNIS rules. • DNIS—The <code>called-station-ID</code> (attribute 30) is used.

When specifying a NAR you can use an asterisk (*) as a wildcard for any value, or as part of any value to establish a range. All the values or conditions in a NAR description must be met for the NAR to restrict access; that is, the values contain a Boolean AND.

Adding a Shared NAR

You can create a shared NAR that contains many access restrictions. Although the ACS web interface does not enforce limits to the number of access restrictions in a shared NAR or to the length of each access restriction, you must adhere to the following limits:

- The combination of fields for each line item cannot exceed 1024 characters.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

Before You Begin

Before defining a NAR, you should be certain ensure that you have established the elements you intend to use in that NAR; you must have specified all NAFs and NDGs, and defined all relevant AAA clients, before making them part of the NAR definition. For more information see [About Network Access Restrictions, page 4-18](#).

To add a shared NAR:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Step 3 Click **Add**.

The Network Access Restriction page appears.

Step 4 In the **Name** box, type a name for the new shared NAR.



Note The name can contain up to 31 characters. Leading and trailing spaces are not allowed. Names cannot contain the following characters: left bracket ([), right bracket (]), comma (,), or slash (/).

Step 5 In the **Description** box, type a description of the new shared NAR. The description can be up to 1,000 characters.

Step 6 If you want to permit or deny access based on IP addressing:

- a. Check the **Define IP-based access descriptions** check box.
- b. To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.
- c. Select or type the applicable information in each of the following boxes:
 - **AAA Client**—Select **All AAA clients**, or the name of the NDG, or the NAF, or the individual AAA client, to which access is permitted or denied.
 - **Port**—Type the number of the port to which you want to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
 - **Src IP Address**—Type the IP address to filter on when performing access restrictions. You can use the asterisk (*) as a wildcard to specify all IP addresses.



Note The total number of characters in the AAA Client list, and the Port and Src IP Address boxes, must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **Enter**.

The AAA client, port, and address information appear as a line item in the table.

e. To enter additional IP-based line items, repeat steps c and d.

Step 7 If you want to permit or deny access based on calling location or values other than IP addresses:

- a. Select the **Define CLI/DNIS based access restrictions** check box.
- b. To specify whether you are listing locations that are permitted or denied from the Table Defines list, select the applicable value.

- c. To specify the clients to which this NAR applies, select one of the following values from the AAA Client list:
- The name of the NDG
 - The name of the particular AAA client
 - All AAA clients



Tip Only NDGs that you have already configured are listed.

- d. To specify the information on which this NAR should filter, type values in the following boxes, as applicable:



Tip You can type an asterisk (*) as a wildcard to specify **all** as a value.

- **Port**—Type the number of the port on which to filter.
- **CLI**—Type the CLI number on which to filter. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see [About Network Access Restrictions, page 4-18](#).
- **DNIS**—Type the number being dialed in to on which to filter.



Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

- e. Click **Enter**.
The information specifying the NAR line item appears in the table.
- f. To enter additional non-IP-based NAR line items, repeat steps c. through e.

Step 8 To save the shared NAR definition, click **Submit**.

ACS saves the shared NAR and lists it in the **Network Access Restrictions** table.

Editing a Shared NAR

To edit a shared NAR:

- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Network Access Restrictions**.
The Network Access Restrictions table appears.
- Step 3** In the Name column, click the shared NAR that you want to edit.
The Network Access Restriction page appears and displays information for the selected NAR.
- Step 4** Edit the Name or Description of the NAR, as applicable. The description can be up to 1,000 characters.

Step 5 To edit a line item in the IP-based access-restrictions table:

- a. Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

- b. Edit the information, as necessary.



Note The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and ACS cannot accurately apply it to users.

- c. Click **Enter**.

The edited information for this line item is written to the IP-based access-restrictions table.

Step 6 To remove a line item from the IP-based access-restrictions table:

- a. Select the line item.
- b. Below the table, click **Remove**.

The line item is removed from the IP-based access-restrictions table.

Step 7 To edit a line item in the CLI/DNIS access-restrictions table:

- a. Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

- b. Edit the information, as necessary.



Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and ACS cannot accurately apply it to users.

- c. Click **Enter**.

The edited information for this line item is written to the CLI/DNIS access-restrictions table.

Step 8 To remove a line item from the CLI/DNIS access-restrictions table:

- a. Select the line item.
- b. Below the table, click **Remove**.

The line item is removed from the CLI/DNIS access-restrictions table.

Step 9 To save the changes you have made, click **Submit**.

ACS reenters the filter with the new information, which takes effect immediately.

Deleting a Shared NAR

Before You Begin

Ensure that you remove the association of a shared NAR to any user or group before you delete that NAR.

To delete a shared NAR:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Network Access Restrictions**.
- Step 3** Click the **Name** of the shared NAR that you want to delete.
The Network Access Restriction page appears and displays information for the selected NAR.
- Step 4** At the bottom of the page, click **Delete**.
A dialog box warns you that you are about to delete a shared NAR.
- Step 5** To confirm that you want to delete the shared NAR, click **OK**.
The selected shared NAR is deleted.
-

Command Authorization Sets

This section describes command-authorization sets and pattern matching, and provides detailed instructions for configuring and managing them.

This section contains the following topics:

- [About Command Authorization Sets, page 4-25](#)
 - [Command Authorization Sets Description, page 4-26](#)
 - [Command Authorization Sets Assignment, page 4-27](#)
 - [Case Sensitivity and Command Authorization, page 4-27](#)
 - [Arguments and Command Authorization, page 4-28](#)
 - [About Pattern Matching, page 4-28](#)
- [Adding a Command Authorization Set, page 4-29](#)
- [Editing a Command Authorization Set, page 4-30](#)
- [Deleting a Command Authorization Set, page 4-31](#)

About Command Authorization Sets

This section contains the following topics:

- [Command Authorization Sets Description, page 4-26](#)
- [Command Authorization Sets Assignment, page 4-27](#)
- [Case Sensitivity and Command Authorization, page 4-27](#)
- [Arguments and Command Authorization, page 4-28](#)
- [About Pattern Matching, page 4-28](#)

Command Authorization Sets Description

Command authorization sets provide a central mechanism to control the authorization of each command that is issued on any given network device. This feature greatly enhances the scalability and manageability of setting authorization restrictions. In ACS, the default command-authorization sets include Shell Command Authorization Sets and PIX Command Authorization Sets. Cisco device-management applications, such as Management Center for Firewalls, can instruct ACS to support additional command-authorization set types.



Note

PIX Command Authorization Sets require that the TACACS+ command-authorization request identify the service as **pixshell**. Verify that this service has been implemented in the version of PIX OS that your firewalls use; if not, use Shell Command Authorization Sets to perform command authorization for PIX devices. For information, see [Configuring a Shell Command Authorization Set for a User Group, page 5-23](#).



Tip

As of PIX OS version 6.3, the `pixshell` service has not been implemented.

To offer more control of device-hosted, administrative Telnet sessions, a network device using TACACS+ can request authorization for each command line before its execution. You can define a set of commands that are permitted or denied for execution by a particular user on a given device. ACS has further enhanced this capability with:

- **Reusable Named Command Authorization Sets**—Without directly citing any user or user group, you can create a named set of command authorizations. You can define several command-authorization sets, each delineating different access profiles. For example:
 - A **Help desk** command-authorization set could permit access to high level browsing commands, such as **show run**, and deny any configuration commands.
 - An **All network engineers** command-authorization set could contain a limited list of permitted commands for any network engineer in the enterprise.
 - A **Local network engineers** command-authorization set could permit all commands, including IP address configuration.
- **Fine Configuration Granularity**—You can create associations between named command-authorization sets and NDGs. Thus, you can define different access profiles for users depending on which network devices they access. You can associate the same named command-authorization set with more than one NDG and use it for more than one user group. ACS enforces data integrity. Named command-authorization sets are kept in the ACS internal database. You can use the ACS Backup and Restore features to back up and restore them. You can also replicate command-authorization sets to secondary ACSs along with other configuration data.

For command-authorization set types that support Cisco device-management applications, the benefits of using command-authorization sets are similar. You can enforce authorization of various privileges in a device-management application by applying command-authorization sets to ACS groups that contain users of the device-management application. The ACS groups can correspond to different roles within the device-management application and you can apply different command-authorization sets to each group, as applicable.

ACS has three sequential stages of command-authorization filtering. Each command-authorization request is evaluated in the following order:

1. **Command Match**—ACS determines whether the command being processed matches a command listed in the command-authorization set. If no matching command is found, command-authorization is determined by the Unmatched Commands setting: permit or deny. Otherwise, if the command is matched, evaluation continues.
2. **Argument Match**—ACS determines whether the command arguments presented match the command arguments listed in the command-authorization set.
 - If any argument is unmatched, command authorization is determined by whether the Permit Unmatched Args option is enabled. If unmatched arguments are permitted, the command is authorized and evaluation ends; otherwise, the command is not authorized and evaluation ends.
 - If all arguments are matched, evaluation continues.
3. **Argument Policy**—Having determined that the arguments in the command being evaluated match the arguments listed in the command-authorization set, ACS determines whether each command argument is explicitly permitted. If all arguments are explicitly permitted, ACS grants command authorization. If any arguments is not permitted, ACS denies command authorization.

Command Authorization Sets Assignment

For information on assigning command-authorization sets, see the following procedures:

- **Shell Command Authorization Sets**—See one of the following:
 - [Configuring a Shell Command Authorization Set for a User Group, page 5-23](#)
 - [Configuring a Shell Command Authorization Set for a User, page 6-17](#)
- **PIX Command Authorization Sets**—See one of the following:
 - [Configuring a PIX Command Authorization Set for a User Group, page 5-25](#)
 - [Configuring a PIX Command Authorization Set for a User, page 6-18](#)
- **Device Management Command Authorization Sets**—See one of the following:
 - [Configuring Device Management Command Authorization for a User Group, page 5-26](#)
 - [Configuring Device-Management Command Authorization for a User, page 6-19](#)

Case Sensitivity and Command Authorization

When performing command authorization, ACS evaluates commands and arguments in a case-sensitive manner. For successful command authorization, you must configure command-authorization sets with case-sensitive commands and arguments.

As an additional complication, a device requesting command authorization might send commands and arguments by using a case different from the one you typed to issue the command.

For example, if you type the following command during a router-hosted session:

```
interface FASTETHERNET 0/1
```

the router might submit the command and arguments to ACS as:

```
interface FastEthernet 0 1
```

If, for the **interface** command, the command-authorization set explicitly permits the FastEthernet argument by using the spelling **fastethernet**, ACS fails the command-authorization request. If the command-authorization rule instead permits the argument **FastEthernet**, ACS grants the command-authorization request. The case used in command-authorization sets must match what the device sends, which might or might not match the case you use when you type the command.

Arguments and Command Authorization

When you explicitly permit or deny arguments rather than rely on ACS to permit unmatched arguments, you must make certain that you know how devices send arguments to ACS. A device requesting command authorization might send different arguments than what the user typed to issue the command.

For example, if during a router-hosted session a user typed the following command:

```
interface FastEthernet0/1
```

the router might send the following command and arguments ACS:

```
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd=interface
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=FastEthernet
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=0
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=1
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=<cr>
```

In this example, the router sees multiple arguments where the user typed one string of characters without spaces after the command. It also omits the slash (/) that separated 0 and 1 when the user issued the command.

If the command-authorization rule for the **interface** command explicitly permits the FastEthernet argument to use the spelling **FastEthernet0/1**, ACS fails the command-authorization request because it does not match what the router submitted to ACS. If the command-authorization rule instead permits the argument **FastEthernet 0 1**, ACS grants the command-authorization request. The case of arguments specified in command-authorization sets must match what the device sends, which might or might not match the case that you use when you type the arguments.

About Pattern Matching

For **permit** or **deny** command arguments, ACS applies pattern matching. That is, the argument **permit wid** matches any argument that contains the string **wid**. Thus, for example, **permit wid** would allow not only the argument **wid** but also the arguments **anywid** and **widget**.

To limit the extent of pattern matching you can add the following expressions:

- **Dollarsign (\$)**—Expresses that the argument must end with what has gone before. Thus **permit wid\$** would match **wid** or **anywid**, but not **widget**.
- **Caret (^)**—Expresses that the argument must begin with what follows. Thus **permit ^wid** would match **wid** or **widget**, but not **anywid**.

You can combine these expressions to specify absolute matching. In the example given, you would use **permit ^wid\$** to ensure that only **wid** was permitted, and not **anywid** or **widget**.

To **permit** or **deny** commands that carry no arguments, you can use absolute matching to specify the null argument condition. For example, you use **permit ^\$** to permit a command with no arguments. Alternatively, entering **permit <cr>** has the same effect. You can use either method, with the **Permit Unmatched Args** option unchecked, to match and permit or deny commands that have no argument.

Adding a Command Authorization Set

To add a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page lists the command-authorization set types that are available. These always include Shell Command Authorization Sets and may include others, such as command-authorization set types that support Cisco device-management applications.

Step 2 Click one of the listed command-authorization set types, as applicable.
The selected Command Authorization Sets table appears.

Step 3 Click **Add**.
The applicable Command Authorization Set page appears. Depending on the type of command-authorization set that you are adding, the contents of the page vary. Below the Name and Description boxes, ACS displays additional boxes or an expandable checklist tree. The expandable checklist tree appears for device command set types that support a Cisco device-management application.

Step 4 In the **Name** box, type a name for the command-authorization set.



Note The set name can contain up to 27 characters. Names cannot contain the following characters: pound sign (#), question mark (?), quotes ("), asterisk (*), right angle bracket (>), left angle bracket (<). Leading and trailing spaces are not allowed.

Step 5 In the **Description** box, type a description of the command-authorization set. The description can be up to 1,000 characters.

Step 6 If ACS displays an expandable checklist tree below the Name and Description boxes, use the checklist tree to specify the actions permitted by the command-authorization set:

- a. To expand a checklist node, click the plus sign (+) to its left.
- b. To enable an action, select its check box. For example, to enable a Device View action, select the **View** check box under the Device checklist node.



Tip Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

- c. To enable other actions in this command-authorization set, repeat Step a and Step b, as needed.

Step 7 If ACS displays additional boxes below the Name and Description boxes, use the boxes to specify the commands and arguments permitted or denied by the command-authorization set:

- a. To specify how ACS should handle unmatched commands, select the **Permit** or **Deny** option, as applicable.



Note The default setting is **Deny**.

- b. In the box just above the Add Command button, type a command that is to be part of the set.

**Caution**

Enter the full command; if you use command abbreviations, authorization control might not function.

**Note**

Enter only the command portion of the command/argument string here. Arguments are added only after the command is listed. For example, with the command/argument string **show run** you would type only the command **show**.

c. Click Add Command.

The typed command is added to the command list box.

d. To add an argument to a command, in the Command List box, select the command and then type the argument in the box to the right of the command.**Note**

The correct format for arguments is <permit | deny> <argument>. For example, with the command **show** already listed, you might enter **permit run** as the argument.

**Tip**

You can list several arguments for a single command by pressing **Enter** between arguments.

e. To allow arguments, which you have not listed, to be effective with this command, select the Permit Unmatched Args check box.**f. To add other commands to this command-authorization set, repeat Step a through Step e.****Step 8 To save the command-authorization set, click Submit.**

ACS displays the name and description of the new command-authorization set in the applicable Command Authorization Sets table.

Editing a Command Authorization Set

To edit a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types available.

Step 2 Click a command-authorization set type, as applicable.

The selected Command Authorization Sets table appears.

Step 3 From the Name column, click the name of the set you want to change.

Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 If an expandable checklist tree appears below the Name and Description boxes, you can do any or all of the following:

- To expand a checklist node, click the plus (+) symbol to its left. To collapse an expanded checklist node, click the minus (-) symbol to its left.

- To enable an action, check its check box. For example, to enable a Device View action, check the **View** check box under the Device checklist node.



Tip Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

- To disable an action, uncheck its check box. For example, to disable a Device View action, uncheck the **View** check box under the Device checklist node.

Step 5 If additional boxes appear below the Name and Description boxes, you can do any or all of the following:

- To change the set Name or Description, edit the words in the corresponding box. The description can be up to 1,000 characters.
- To remove a command from the set, from the Matched Commands list, select the command, and then click **Remove Command**.
- To edit arguments of a command, from the command list box, select the command and then type changes to the arguments in the box to the right of the command list box.

Step 6 To save the set, click **Submit**.

Deleting a Command Authorization Set

To delete a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types available.

Step 2 Click a command-authorization set type, as applicable.

The selected Command Authorization Sets table appears.

Step 3 From the Name column, click the name of the command set that you want to delete.

Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 Click **Delete**.

A dialog box warns you that you are about to delete a command-authorization set.

Step 5 To confirm that you want to delete that command-authorization set, click **OK**.

ACS displays the applicable Command Authorization Sets table. The command-authorization set is no longer listed.

