



Shared Profile Components

This chapter addresses the Cisco Secure ACS Solution Engine features found in the Shared Profile Components section of the HTML interface.

This chapter contains the following topics:

- [About Shared Profile Components, page 5-1](#)
- [Network Access Filters, page 5-2](#)
- [Downloadable IP ACLs, page 5-7](#)
- [Network Access Restrictions, page 5-14](#)
- [Command Authorization Sets, page 5-25](#)

About Shared Profile Components

The Shared Profile Components section enables you 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), downloadable IP access control lists (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 once and then applied to many users or groups. Without this ability, flexible and comprehensive authorization could only be accomplished by explicitly configuring the authorization of each user group on each device. Creating and applying these

named shared profile components (downloadable IP ACLs, NAFs, NARs, and command authorization sets) makes it unnecessary to repeatedly enter long lists of devices or commands when defining network access parameters.

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 5-2](#)
- [Adding a Network Access Filter, page 5-3](#)
- [Editing a Network Access Filter, page 5-5](#)
- [Deleting a Network Access Filter, page 5-7](#)

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 in downloadable IP ACLs**—You can associate a NAF with specific ACL contents. A downloadable IP ACL consists of one or more ACL contents (sets of ACL definitions) that are associated with either a single NAF or, by default, “All-AAA-Clients”. This pairing of ACL content with a NAF permits Cisco Secure 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 5-8](#).

- **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 5-15](#).

**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 Cisco Secure ACS.

The network elements that make up a NAF 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, follow these steps:

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 the following 10 characters:
[] , / — - “ ‘ > <

Step 5 In the **Description** box, type a description of the new network access filter.

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 wildcard (*) to designate a range within an IP address.

Step 7 Ensure that the order of the items is what you want. 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 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, click **Submit + Restart**.

**Tip**

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

**Note**

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

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, follow these steps:

-
- 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 you want to edit.
The Network Access Filter page appears with information displayed for the selected NAF.
- Step 4** Edit the Name or Description of the NAF, type and delete information, as applicable.

**Caution**

If you change the name of a NAF, you invalidate all existing references to that NAF; this may affect the access of users or groups 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 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 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 you want to add. Click --> (right arrow button) to move it to the Selected Items box.
- Step 8** To edit an IP address, select 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, select 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 you want. For more information on arranging the order of NAFs see [About Network Access Filters, page 5-2](#).
- Step 11** To save the changes to your NAF and apply them immediately, click **Submit + Restart**.

**Tip**

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



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

Cisco Secure ACS re-enters 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 or downloadable IP ACL that uses it. Otherwise, any NAR or downloadable IP ACL that references the deleted NAF will be misconfigured and will produce an error.

To delete a NAF, follow these steps:

-
- 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 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.
-

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 5-8](#)
- [Adding a Downloadable IP ACL, page 5-10](#)
- [Editing a Downloadable IP ACL, page 5-13](#)
- [Deleting a Downloadable IP ACL, page 5-14](#)

About Downloadable IP ACLs

Downloadable IP ACLs enable you 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 consists of one or more ACL content definitions, each of which is either 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 5-2](#)).

Downloadable IP ACLs operate as follows:

1. When Cisco Secure ACS grants a user access to the network, Cisco Secure ACS determines whether a downloadable IP ACL is assigned to that user or to that user's group.
2. If Cisco Secure ACS locates a downloadable IP ACL assigned to the user or the user's group, it determines whether there is an ACL content entry associated with the AAA client that sent the RADIUS authentication request.
3. Cisco Secure 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), Cisco Secure 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 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 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 Cisco Secure ACS. Downloadable ACLs are protected by the backup or replication regimen you have established.

While entering the ACL definitions in the Cisco Secure ACS HTML 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 Cisco Secure ACS consist of 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 listed in the NAF 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 5-2](#).

Also, you can change the order of the ACL contents listed within a downloadable IP ACL. Cisco Secure ACS examines ACL contents starting from the top of the table and downloads the *first* ACL content 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 arranging the most widely applicable ACL contents higher on the list; but also realize that if your NAFs include overlapping populations of AAA clients you must proceed from the more specific to the more general. For example, Cisco Secure 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 following requirements must be met:

- The AAA client must use RADIUS for authentication.
- The AAA client must support downloadable IP ACLs.

Examples of Cisco devices that support downloadable IP ACLs are:

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

An example of the format you should use to enter PIX Firewall ACLs in the ACL Definitions box follows:

```
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
```

An example of the format you should use to enter VPN 3000 ACLs in the ACL Definitions box follows:

```
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, follow these steps:

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 either 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:

- [] / \ " < > —

Step 5 In the **Description** box, type a description of the new IP ACL.

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:

- [] / \ " < > —

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



Tip

In entering ACL definitions in the Cisco Secure ACS HTML interface, you do not use keyword and name entries; rather, you begin with a permit/deny keyword. For an example of the proper format of the ACL definitions, see [About Downloadable IP ACLs, page 5-8](#).

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 5-3.



Note If you do not assign a NAF, Cisco Secure 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, select 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, Cisco Secure 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**.


Cisco Secure 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 7-21, or [Assigning a Downloadable IP ACL to a Group](#), page 6-30.

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, follow these steps:

-
- 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 you want to edit.
The Downloadable IP ACLs page appears with information displayed for the selected ACL.
- Step 4** Edit the Name or Description information, as applicable.
- Step 5** To edit ACL content, click on the ACL Contents entry you want to change.
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/deny keyword. For an example of the proper format of the ACL definitions, see [About Downloadable IP ACLs, page 5-8](#).
-
- Step 7** To save the edited ACL definition, click **Submit**.
- Step 8** To change the NAF 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 like. For more information on NAFs see [About Network Access Filters, page 5-2](#).
- 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**.

Cisco Secure 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 or user group profile before deleting the IP ACL.

To delete an IP ACL, follow these steps:

- 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 you want to delete.
The Downloadable IP ACLs page appears with information displayed 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 5-15](#)
- [Adding a Shared Network Access Restriction, page 5-19](#)
- [Editing a Shared Network Access Restriction, page 5-22](#)
- [Deleting a Shared Network Access Restriction, page 5-24](#)

About Network Access Restrictions

A NAR is a definition, which you make in Cisco Secure ACS, of additional conditions that must be met before a user can access the network. Cisco Secure ACS applies these conditions using information from attributes sent by your AAA clients. Although there are several ways you can set up NARs, they all are based on matching attribute information sent by a AAA client. Therefore, you must understand the format and content of the attributes your AAA clients send 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 comparison of information sent from AAA clients to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied access. This is shown in [Table 5-1](#).

Table 5-1 NAR Permit/Deny Conditions

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

Cisco Secure ACS supports two types of NAR filters:

- **IP-based filters**—IP-based NAR filters limit access based upon 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 5-17](#).
- **Non-IP-based filters**—Non-IP-based NAR filters limit access based upon simple string comparison of a value sent from the AAA client. The value may be the calling line ID (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, (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 5-18](#).

You can define a NAR for, and apply it to, a specific user or user group. For more information on this, see [Setting Network Access Restrictions for a User, page 7-11](#), or [Setting Network Access Restrictions for a User Group, page 6-8](#). However, in the Shared Profile Components section of Cisco Secure 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 Cisco Secure ACS HTML 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: either “All selected filters must permit”, or “Any one selected filter must permit”.

It is important to understand the order of precedence related to the different types of NARs. The order of NAR filtering is as follows:

1. Shared NAR at the user level
2. Shared NAR at the group level
3. Non-shared NAR at the user level
4. Non-shared NAR at the group level

You should also note 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 Cisco Secure ACS to the rule that user-level settings override group-level settings. For example, a particular user may have no NAR restrictions at the user level that apply, but if that user belongs to a group that is restricted by either a shared or non-shared NAR, the user is denied access.

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

About IP-based NAR Filters

For IP-based NAR filters, ACS uses the following attributes, depending upon the AAA protocol of the authentication request:

- **If you are using TACACS+**—The `rem_addr` field from the TACACS+ start packet body is used.



Note

When an authentication request is forwarded by proxy to a Cisco Secure 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.

- **If you are using RADIUS IETF**—The `calling-station-id` (attribute 31) and `called-station-id` (attribute 30) fields are used.

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

Other attributes for **IP-based** restrictions, per protocol, include the following NAR fields:

- **If you are using TACACS+**—The NAR fields listed in Cisco Secure ACS use the following values:
 - **AAA client**—The `NAS-IP-address` is taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client.
 - **Port**—The `port` field is taken from the TACACS+ start packet body.
- **If you are using RADIUS**—The NAR fields listed in Cisco Secure ACS use the following values:
 - **AAA client**—The `NAS-IP-address` (attribute 4) or, if `NAS-IP-address` does not exist, `NAS-identifier` (attribute 32) is used.
 - **Port**—The `NAS-port` (attribute 5) or, if `NAS-port` does not exist, `NAS-port-ID` (attribute 87) is used.

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”/“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 calling line ID (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; 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.

Attributes for **DNIS/CLI-based** restrictions, per protocol, include the following NAR fields:

- **If you are using TACACS+**—The NAR fields listed employ the following values:
 - **AAA client**—The `NAS-IP-address` is taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client.
 - **Port**—The `port` field in the TACACS+ start packet body is used.
 - **CLI**—The `rem-addr` field in the TACACS+ start packet body is used.
 - **DNIS**—The `rem-addr` field taken from the TACACS+ start packet body is used. In cases in which the `rem-addr` data begins with “/” the DNIS field contains the `rem-addr` data without the “/” character.



Note

When an authentication request is forwarded by proxy to a Cisco Secure 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.

- **If you are using RADIUS**—The NAR fields listed use the following values:
 - **AAA client**—The `NAS-IP-address` (attribute 4) or, if `NAS-IP-address` does not exist, `NAS-identifier` (RADIUS attribute 32) is used.
 - **Port**—The `NAS-port` (attribute 5) or, if `NAS-port` does not exist, `NAS-port-ID` (attribute 87) is used.
 - **CLI**—The `calling-station-ID` (attribute 31) is used.
 - **DNIS**—The `called-station-ID` (attribute 30) is used.

When specifying a NAR you can use asterisks (*) as wildcards for any value, or as part of any value to establish a range. All the values/conditions in a NAR description must be met for the NAR to restrict access; that is, the values are “ANDed”.

Adding a Shared Network Access Restriction

You can create a shared NAR that contains many access restrictions. Although the Cisco Secure ACS HTML interface does not enforce limits to the number of access restrictions in a shared NAR or to the length of each access restriction, there are limits that you must adhere to, as follows:

- 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 sure that you have established the elements you intend to use in that NAR. This means that 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 5-15](#).

To add a shared NAR, follow these steps:

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 four characters:
[], /

Step 5 In the **Description** box, type a description of the new shared NAR.

Step 6 If you want to permit or deny access based on IP addressing, follow these steps:

- a. Select 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 that you want to permit or deny access to. You can use the wildcard asterisk (*) 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 wildcard asterisk (*) 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 Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

d. Click **enter**.

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

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

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

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 that this NAR applies to, select one of the following values from the AAA Client list:

- The name of the NDG
- The name of the NAF
- 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 that this NAR should filter on, 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 to filter on.
- **CLI**—Type the CLI number to filter on. 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 5-15](#).
- **DNIS**—Type the number being dialed into to filter on.



Note

The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure 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 **c.** through **e.**

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

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

Editing a Shared Network Access Restriction

To edit a shared NAR, follow these steps:

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 you want to edit.

The Network Access Restriction page appears with information displayed for the selected NAR.

Step 4 Edit the Name or Description of the NAR, as applicable.

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

- 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 Cisco Secure ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and Cisco Secure 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, follow these steps:

- 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, follow these steps:

- 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 Cisco Secure ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and Cisco Secure 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, follow these steps:

- 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**.

Cisco Secure ACS re-enters the filter with the new information, which takes effect immediately.

Deleting a Shared Network Access Restriction

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, follow these steps:

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 you want to delete.

The Network Access Restriction page appears with information displayed 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 5-25](#)
 - [Command Authorization Sets Description, page 5-26](#)
 - [Command Authorization Sets Assignment, page 5-28](#)
 - [Case Sensitivity and Command Authorization, page 5-28](#)
 - [Arguments and Command Authorization, page 5-29](#)
 - [About Pattern Matching, page 5-30](#)
- [Adding a Command Authorization Set, page 5-31](#)
- [Editing a Command Authorization Set, page 5-33](#)
- [Deleting a Command Authorization Set, page 5-34](#)

About Command Authorization Sets

This section contains the following topics:

- [Command Authorization Sets Description, page 5-26](#)
- [Command Authorization Sets Assignment, page 5-28](#)
- [Case Sensitivity and Command Authorization, page 5-28](#)

- [Arguments and Command Authorization, page 5-29](#)
- [About Pattern Matching, page 5-30](#)

Command Authorization Sets Description

Command authorization sets provide a central mechanism to control the authorization of each command issued on any given network device. This greatly enhances the scalability and manageability of setting authorization restrictions. In Cisco Secure 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 Cisco Secure 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 your firewalls use; if not, use Shell Command Authorization Sets to perform command authorization for PIXes.



Tip

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

To offer fine-grained 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 either permitted or denied for execution by a particular user on a given device. Cisco Secure ACS has further enhanced this capability as follows:

- **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. Cisco Secure ACS enforces data integrity. Named command authorization sets are kept in the CiscoSecure user database. You can use the Cisco Secure ACS Backup and Restore features to back up and restore them. You can also replicate command authorization sets to secondary Cisco Secure ACSes 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 Cisco Secure ACS groups that contain users of the device-management application. The Cisco Secure 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.

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

1. **Command Match:** Cisco Secure 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, which is either permit or deny. Otherwise, if the command is matched, evaluation continues.
2. **Argument Match:** Cisco Secure 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, Cisco Secure ACS determines whether each command argument is explicitly

permitted. If all arguments are explicitly permitted, Cisco Secure ACS grants command authorization. If any arguments is not permitted, Cisco Secure ACS denies command authorization.

Command Authorization Sets Assignment

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

- **Shell Command Authorization Sets**—See either of the following:
 - [Configuring a Shell Command Authorization Set for a User Group, page 6-33](#)
 - [Configuring a Shell Command Authorization Set for a User, page 7-25](#)
- **PIX Command Authorization Sets**—See either of the following:
 - [Configuring a PIX Command Authorization Set for a User Group, page 6-35](#)
 - [Configuring a PIX Command Authorization Set for a User, page 7-28](#)
- **Device Management Command Authorization Sets**—See either of the following:
 - [Configuring Device-Management Command Authorization for a User Group, page 6-37](#)
 - [Configuring Device-Management Command Authorization for a User, page 7-30](#)

Case Sensitivity and Command Authorization

When performing command authorization, Cisco Secure 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 may send commands and arguments 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 may submit the command and arguments to Cisco Secure ACS as:

```
interface FastEthernet 0 1
```

If, for the **interface** command, the command authorization set explicitly permits the FastEthernet argument using the spelling “fastethernet”, Cisco Secure ACS fails the command authorization request. If the command authorization rule instead permits the argument “FastEthernet”, Cisco Secure ACS grants the command authorization request. The case used in command authorization sets must match what the device sends, which may or may 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 Cisco Secure ACS to permit unmatched arguments, you must make certain that you know how devices send arguments to Cisco Secure ACS. A device requesting command authorization may send different arguments than the user typed to issue the command.

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

```
interface FastEthernet0/1
```

the router may send the command and arguments Cisco Secure ACS as follows:

```
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 character 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 using the spelling “FastEthernet0/1”, Cisco Secure ACS fails the command authorization request because it does not match what the router submitted to Cisco Secure ACS. If the command authorization rule instead permits the argument “FastEthernet 0 1”, Cisco Secure ACS grants the command authorization request. The case of arguments specified in command authorization sets must match what the device sends, which may or may not match the case you use when you type the arguments.

About Pattern Matching

For permit/deny command arguments, Cisco Secure 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/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. Either of these methods can be used, with the **Permit Unmatched Args** option unselected, to match and therefore permit or deny commands that have no argument.

Adding a Command Authorization Set

To add a command authorization set, follow these steps:

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

The Shared Profile Components page lists the command authorization set types 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 upon the type of command authorization set you are adding, the contents of the page vary. Below the Name and Description boxes, Cisco Secure ACS displays either 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:

? " * > <

Leading and trailing spaces are not allowed.

Step 5 In the Description box, type a description of the command authorization set.

Step 6 If Cisco Secure 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. To do so, follow these steps:

- a. To expand a checklist node, click the plus (+) symbol 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 Cisco Secure 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. To do so, follow these steps:

- a. To specify how Cisco Secure ACS should handle unmatched commands, select either 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 word; if you use command abbreviations, authorization control may 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**.

Cisco Secure 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, follow these steps:

-
- 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, 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.

- To disable an action, clear its check box. For example, to disable a Device View action, clear 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.
 - 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, follow these steps:

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

