Cisco Secure ACS: Network Access Restrictions with AAA Clients for Users and User Groups

Document ID: 91905

Contents

Introduction

This document describes how to configure the Network Access Restrictions (NAR) in Cisco Secure Access Control Server (ACS) 4.x version with AAA clients (includes routers, PIX, ASA, wireless controllers) for Users and User groups.

Prerequisites

Requirements

This document is created with the assumption that Cisco Secure ACS and AAA clients are configured and work properly.

Components Used

The information in this document is based on the Cisco Secure ACS 3.0 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Network Access Restrictions

This section describes NARs, and provides detailed instructions to configure and manage shared NARs.

This section contains these topics:

- About Network Access Restrictions
- Add a Shared NAR
- Edit a Shared NAR
- Delete a Shared NAR

About Network Access Restrictions

A 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 send. Although you can set up NARs in several ways, all are based on matching attribute information that a AAA client sends. Therefore, you must understand the format and content of the attributes that your AAA clients send if you want to employ effective NARs.

When you set 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. This table shows these 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. See the About IP–based NAR Filters section for more information.
- **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 can be the calling line identification (CLI) number, the Dialed Number Identification Service (DNIS) number, the MAC address, or another value that originates 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, which includes whatever format is used. For example, the telephone number (217) 555–4534 does not match 217–555–4534. See the About Non–IP–based NAR Filters section for more information.

You can define a NAR for, and apply it to, a specific user or user group. See the Set Network Access Restrictions for a User or Set Network Access Restrictions for a User Group sections for more information. 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. This is the order of NAR filtering:

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 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. However, if that user belongs to a group that is restricted by a shared or non−shared 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 as shown, which depends on 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 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.
- **If you are using RADIUS IETF** The `calling-station-id` (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.

Other attributes for **IP−based** restrictions, per protocol, include the NAR fields as shown:

- **If you are using TACACS+** The NAR fields in ACS use these values:

  - ♦ **AAA client** The NAS−IP−address is taken from the source address in the socket between ACS and the TACACS+ client.
  - ♦ **Port** The port 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 to restrict an 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 DNIS number.

However, when you enter 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® software 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.

Attributes for DNIS/CLI−based restrictions, per protocol, include the NAR fields as shown:

- **If you are using TACACS+** The NAR fields listed employ these values:

  - ♦ **AAA client** The `NAS-IP-address` is taken from the source address in the socket between 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 slash (/), the DNIS field contains the rem−addr data without the slash (/).

    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.

- **If you are using RADIUS** The NAR fields listed use these 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 you specify 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. This means the values contain a Boolean AND.

Add 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 these limits:
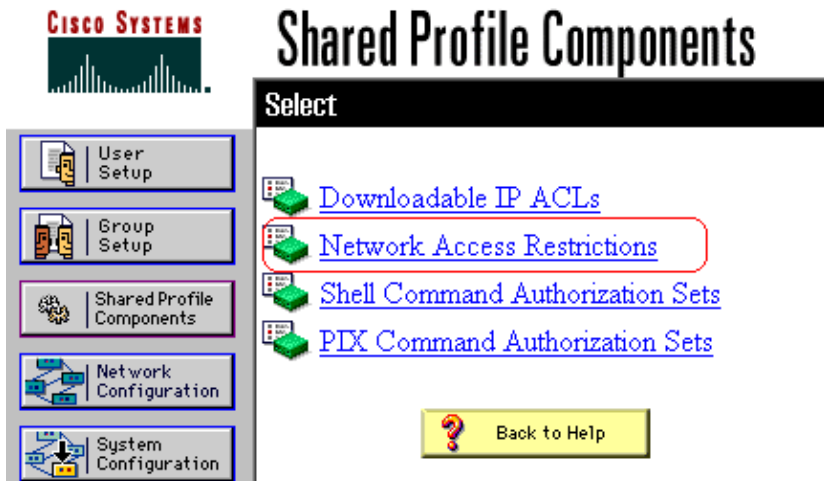
- The combination of fields for each line item cannot exceed 1024 characters.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS−based NAR where the AAA client names are 10 characters, 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 you reach the 16 KB limit.

Note: Before you define a NAR, make certain that you have established the elements you intend to use in that NAR. Therefore, you must have specified all NAFs and NDGs, and defined all relevant AAA clients, before you make them part of the NAR definition. See the About Network Access Restrictions section for more information.
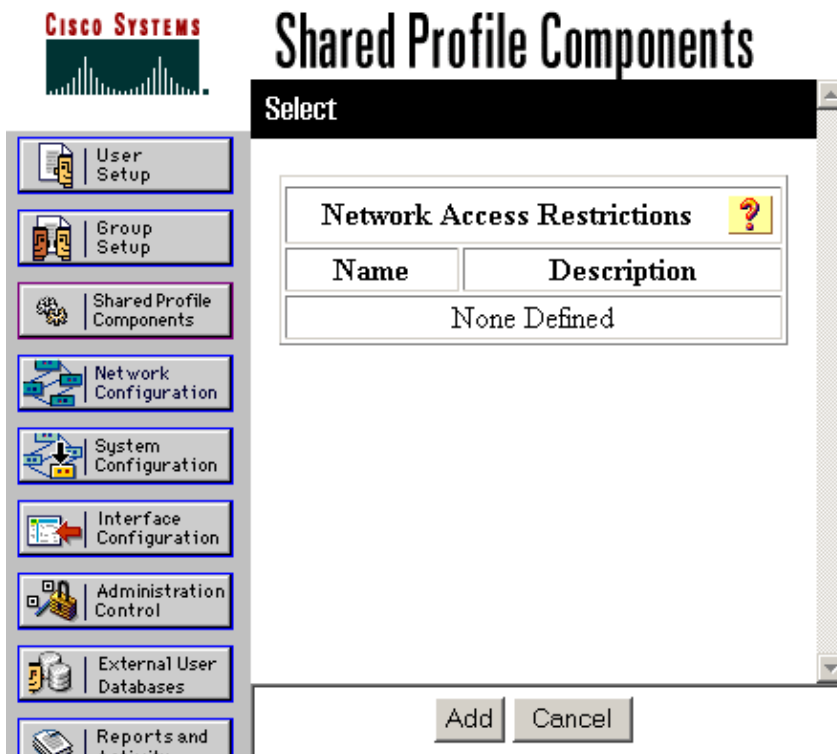
Complete these steps in order to add a shared NAR:

1. In the Navigation bar, click **Shared Profile Components**.

   The Shared Profile Components window appears.

2. Click **Network Access Restrictions**.

3. Click **Add**.

The Network Access Restriction window appears.

Shared Profile Components

Network Access Restriction

Name: _____

Description: _____

☐ Define IP-based access restrictions

Table Defines | Permitted Calling/Point of Access Locations ▾ |

AAA Client   Port   Src IP Address

_____

[remove]

AAA Client | All AAA Clients ▾ |
Port | _____ |
Src IP Address | _____ |

[enter]

☐ Define CLI/DNIS-based access restrictions

Table Defines | Permitted Calling/Point of Access Locations ▾ |

AAA Client   Port   CLI   DNIS

_____

4. In the Name box, enter 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 these characters: left bracket ([), right bracket (]), comma (,), or slash (/).
5. In the Description box, enter a description of the new shared NAR. The description can be up to 30,000 characters.
6. If you want to permit or deny access based on IP addressing:

   a. Check the **Define IP−based access descriptions** check box.
   b. In order to specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.
   c. Select or enter the applicable information in each of these 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** Enter 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** Enter 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. Repeat steps c and d in order to enter additional IP−based line items.

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

a. Check the **Define CLI/DNIS based access restrictions** check box.

b. In order to specify whether you are listing locations that are permitted or denied from the Table Defines list, select the applicable value.

c. In order to specify the clients to which this NAR applies, select one of these 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. In order to specify the information on which this NAR should filter, enter values in these boxes, as applicable:

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

a. **Port** Enter the number of the port on which to filter.

b. **CLI** Enter 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. See the About Network Access Restrictions section for more information.

c. **DNIS** Enter 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 that specifies the NAR line item appears in the table.

f. Repeat steps c through e in order to enter additional non−IP−based NAR line items.

g. Click **Submit** in order to save the shared NAR definition.

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

Edit a Shared NAR

Complete these steps in order to edit a shared NAR:

1. In the Navigation bar, click **Shared Profile Components**.

The Shared Profile Components window appears.

2. Click **Network Access Restrictions**.

The Network Access Restrictions table appears.

3. In the Name column, click the shared NAR that you want to edit.

   The Network Access Restriction window appears and displays information for the selected NAR.

4. Edit the Name or Description of the NAR, as applicable. The description can be up to 30,000 characters.

5. In order 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 under 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 can accept 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.

6. In order to remove a line item from the IP–based access–restrictions table:

   a. Select the line item.

   b. Under the table, click **Remove**.

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

7. In order 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 under 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 can accept 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.

8. In order to remove a line item from the CLI/DNIS access–restrictions table:

   a. Select the line item.

   b. Under the table, click **Remove**.

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

9. Click **Submit** in order to save the changes you have made.

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

Delete a Shared NAR

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

Complete these steps in order to delete a shared NAR:

1. In the Navigation bar, click **Shared Profile Components**.

   The Shared Profile Components window appears.
2. Click **Network Access Restrictions**.
3. Click the name of the shared NAR that you want to delete.

   The Network Access Restriction window appears and displays information for the selected NAR.
4. At the bottom of the window, click **Delete**.

   A dialog box warns you that you are about to delete a shared NAR.
5. Click **OK** in order to confirm that you want to delete the shared NAR.

   The selected shared NAR is deleted.

Set Network Access Restrictions for a User

You use the Network Access Restrictions table in the Advanced Settings area of User Setup to set NARs in three ways:

- Apply existing shared NARs by name.
- Define IP−based access restrictions to permit or deny user access to a specified AAA client or to specified ports on an AAA client when an IP connection has been established.
- Define CLI/DNIS−based access restrictions to permit or deny user access based on the CLI/DNIS that is used.

   Note: You can also use the CLI/DNIS−based access restrictions area to specify other values. See the Network Access Restrictions section for more information.

Typically, you define (shared) NARs from within the Shared Components section so that you can apply these restrictions to more than one group or user. See the Add a Shared NAR section for more information. You must have selected the **User−Level Network Access Restrictions** check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the web interface.

However, you can also use ACS to define and apply a NAR for a single user from within the User Setup section. You must have enabled the **User−Level Network Access Restrictions** setting on the Advanced Options page of the Interface Configuration section for single user IP−based filter options and single user CLI/DNIS−based filter options to appear in the web interface.

Note: When an authentication request is forwarded by proxy to an ACS, any NARs for Terminal Access Controller Access Control System (TACACS+) requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

When you create access restrictions on a per−user basis, ACS does not enforce limits to the number of access restrictions and does not enforce a limit to the length of each access restriction. However, there are strict limits:

- The combination of fields for each line item cannot exceed 1024 characters in length.
- 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 you reach the 16

KB limit.

Complete these steps in order to set NARs for a user:

1. Perform steps 1 through 3 of Adding a Basic User Account.

   The User Setup Edit window opens. The username that you add or edit appears at the top of the window.

User Setup

Advanced Settings

Network Access Restrictions (NAR)

Shared Network Access Restrictions

☐   Only Allow network access when

     ⦿ All selected NARs result in permit

     ○ Any one selected NAR results in permit

NARs		Selected NARs
testnar	>> -> <- <<	

View IP NAR   View CLI/DNIS NAR

Per User Defined Network Access Restrictions

☐   Define IP-based access restrictions

Table Defines :   Permitted Calling/Point of Access Locations ▾

AAA Client   Port   Address

remove

AAA Client   All AAA Clients ▾

Port

Submit   Delete   Cancel

2. In order to apply a previously configured shared NAR to this user:

   Note: In order to apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. See the Add a Shared NAR section for more information.

a. Check the **Only Allow network access when** check box.

b. In order to specify whether one or all shared NARs must apply for the user to be permitted access, select one, as applicable:

◊ All selected NARS result in permit.

◊ Any one selected NAR results in permit.

c. Select a shared NAR name in the NARs list, and then click −−> (right arrow button) to move the name into the Selected NARs list.

Tip: In order to view the server details of the shared NARs you have selected to apply, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

3. In order to define and apply a NAR, for this particular user, that permits or denies this user access based on IP address, or IP address and port:

Note: You should define most NARs from within the Shared Components section so that you can apply them to more than one group or user. See the Add a Shared NAR section for more information.

a. In the Network Access Restrictions table, under Per User Defined Network Access Restrictions, check the **Define IP−based access restrictions** check box.

b. In order to specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, choose one:

◊ **Permitted Calling/Point of Access Locations**
◊ **Denied Calling/Point of Access Locations**

c. Select or enter the information in these boxes:

a. **AAA Client** Select **All AAA Clients**, or the name of a network device group (NDG), or the name of the individual AAA client, to which to permit or deny access.

b. **Port** Enter the number of the port to which 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.

c. **Address** Enter the IP address or addresses to use when performing access restrictions. You can use the asterisk (*) as a wildcard.

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 specified AAA client, port, and address information appears in the table above the AAA Client list.

4. In order to permit or deny this user access based on calling location or values other than an established IP address:

a. Check the **Define CLI/DNIS based access restrictions** check box.

b. In order to specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, choose one:

◊ **Permitted Calling/Point of Access Locations**
◊ **Denied Calling/Point of Access Locations**

c. Complete the boxes as shown:

Note: You must make an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string that you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

    a. **AAA Client** Select **All AAA Clients**, or the name of the NDG, or the name of the individual AAA client, to which to permit or deny access.
    b. **PORT** Enter the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.
    c. **CLI** Enter the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.

       Tip: Use the CLI entry if you want to restrict access based on other values such as a Cisco Aironet Client MAC address. See the About Network Access Restrictions section for more information.
    d. **DNIS** Enter the DNIS number to which to permit or deny access. Use this entry to restrict access based on the number into which the user will dial. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.

       Tip: Use the DNIS selection if you want to restrict access based on other values such as a Cisco Aironet AP MAC address. See the About Network Access Restrictions section for more information.

       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.

   d. Click **Enter**.

    The information that specifies the AAA client, port, CLI, and DNIS appears in the table above the AAA Client list.

5. If you are finished configuring the user account options, click **Submit** in order to record the options.

Set Network Access Restrictions for a User Group

You use the Network Access Restrictions table in the Group Setup to apply NARs in three distinct ways:

- Apply existing shared NARs by name.
- Define IP−based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS−based group NARs to permit or deny access to either, or both, the CLI number or the DNIS number used.

    Note: You can also use the CLI/DNIS−based access restrictions area to specify other values. See the About Network Access Restrictions section for more information.

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can apply to more than one group or user. See the Add a Shared NAR section for more information. You must check the **Group−Level Shared Network Access Restriction** check box on the **Advanced Options** page of the Interface Configuration section for these options to appear in the ACS web interface.

However, you can also use ACS to define and apply a NAR for a single group from within the **Group Setup** section. You must check the **Group−Level Network Access Restriction** setting under the Advanced Options

page of the Interface Configuration section for single group IP–based filter options and single group CLI/DNIS–based filter options to appear in the ACS web interface.

Note: When an authentication request is forwarded by proxy to an ACS server, any NARs for RADIUS requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

Complete these steps in order to set NARs for a user group:

1. In the Navigation bar, click **Group Setup**.

   The Group Setup Select window opens.
2. From the Group list, select a group, and then click **Edit Settings**.

   The name of the group appears at the top of the Group Settings window.

Group Setup

Network Access Restrictions (NAR) ❓

Shared Network Access Restrictions

☐ Only Allow network access when

◉ All selected NARs result in permit

○ Any one selected NAR results in permit

NARs		Selected NARs
testnar		

[>>] [->]

[<-] [<<]

[View IP NAR] [View CLI/DNIS NAR]

Per Group Defined Network Access Restrictions

☐ Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations ▼

AAA Client	Port	Address

[remove]

AAA Client: All AAA Clients ▼

Port:

Address:

[enter]

☐ Define CLI/DNIS-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations ▼

AAA Client	Port	CLI	DNIS

[remove]

AAA Client: All AAA Clients ▼

Port:

CLI:

DNIS:

[enter]

[Submit] [Submit + Restart] [Cancel]

3. In order to apply a previously configured shared NAR to this group:

Note: In order to apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. See the Add a Shared NAR section for more information.

    a. Check the **Only Allow network access when** check box.
    b. In order to specify whether one or all shared NARs must apply for a member of the group to be permitted access, check one of these options:

        ◊ All selected shared NARS result in permit.
        ◊ Any one selected shared NAR results in permit.
    c. Select a shared NAR name in the Shared NAR list, and then click −−> (right arrow button) to move the name into the Selected Shared NARs list.

        Tip: In order to view the server details of the shared NARs that you have applied, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

4. In order to define and apply a NAR for this particular user group, that permits or denies access to this group based on IP address, or IP address and port:

Note: You should define most NARs from within the Shared Components section so that the restrictions can apply to more than one group or user. See the Add a Shared NAR section for more information.

    a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, check the **Define IP−based access restrictions** check box.
    b. In order to specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, choose **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.
    c. Select or enter the information in these boxes:

        a. **AAA Client** Select All AAA clients or the name of the NDG or the name of the individual AAA client to which you want to permit or deny access.
        b. **Port** Enter the number of the port to which 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.
        c. **Address** Enter the IP address or addresses to filter on when performing access restrictions. You can use the asterisk (*) as a wildcard.

        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 specified the AAA client, port, and address information appears in the **NAR Access Control** list.

5. In order to permit or deny access to this user group based on calling location or values other than an established IP address:

    a. Check the **Define CLI/DNIS−based access restrictions** check box.
    b. In order to specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, choose one:

       ◊ **Permitted Calling/Point of Access Locations**

       ◊ **Denied Calling/Point of Access Locations**

  c. From the AAA Client list, choose **All AAA Clients**, or the name of the NDG or the name of the particular AAA client to which to permit or deny access.

  d. Complete these boxes:

Note: You must enter an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

     a. **PORT** Enter the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.

     b. **CLI** Enter the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number or all numbers.

Tip: CLI is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet Client MAC address. See the About Network Access Restrictions section for more information.

     c. **DNIS** Enter the DNIS number to restrict access based on the number into which the user will be dialing. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number or all numbers.

Tip: DNIS is also the selection if you want to restrict access based on other values, such as a Cisco Aironet AP MAC address. See the About Network Access Restrictions section for more information.

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 that specifies the AAA client, port, CLI, and DNIS appears in the list.

6. Click **Submit** in order to save the group settings that you have just made.

    Refer to Saving Changes to User Group Settings for more information.

Related Information

- **Cisco Secure Access Control Server Support Page**
- **Technical Support & Documentation – Cisco Systems**