



CHAPTER 14

Network Access Profiles

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports Network Access Profiles (NAP).

This chapter describes NAPs and contains:

- [Overview of NAPs, page 14-1](#)
- [Managing NAPs, page 14-4](#)
- [Using Profile Templates, page 14-7](#)
- [Configuring Policies for Profiles, page 14-22](#)
- [Policy Replication and Backup, page 14-38](#)
- [Network Access Profiles Pages Reference, page 14-39](#)

Overview of NAPs

Typical organizations have various kinds of users who access the network in different ways and for different purposes. Correspondingly, you must apply different security policies to the different use cases. For example, you might have to apply a tighter and more limiting security policy to the wireless access points of your building's lobby area, versus the physically secured production plant. Or, you might have to treat remote-access users who use a virtual private network (VPN) differently from users who log in from behind a firewall. Users who connect through certain subnetworks might be authenticated differently from other users. Wireless access is often treated more strictly than wired access, as is any form of remote access (for example, dial, VPN, home wireless).

A NAP, also known as a *profile*, is essentially a classification of network-access requests for applying a common policy. You can use NAPs to aggregate all policies that should be activated for a certain location in the network. Alternatively, you can aggregate all policies that handle the same device type, for example, VPNs or Access Points (APs).



Note

The Terminal Access Controller Access Control System (TACACS+) protocol for NAPs is not supported in ACS.

The following topics describe NAPs and their associated policies:

- [Classification of Access Requests, page 14-2](#)
- [Profile-based Policies, page 14-3](#)
- [Workflow for Configuring NAPs and Profile-based Policies, page 14-3](#)

- [Processing Unmatched User Requests, page 14-3](#)

Classification of Access Requests

You can classify access requests according to the AAA clients' IP addresses, membership in a network device group (NDG), protocol types, or other specific RADIUS attribute values sent by the network device through which the user connects.

You can use one or all of the following classification methods to classify access requests:

- [NAFs, page 14-2](#)
- [Protocol Types, page 14-2](#)
- [Advanced Filtering, page 14-2](#)

The profile is selected when all the selected conditions match. For each condition, the value **Any** always matches the condition. For example, if you create a network access filter (NAF) for wireless and then select the Aironet Protocol type, only devices with the protocol types in the wireless NAF will be selected for filtering.

NAFs

NAFs are groupings of AAA client configurations (which might represent multiple network devices), NDGs, or IP addresses of specific AAA client devices. You can use a NAF to group (and name) a disparate set of devices; for example: *these devices comprise the abc network service*.

You can also use NAFs to differentiate user requests on the same type of device. For example, while you undertake an IOS upgrade of Aironet wireless APs is undertaken (perhaps to enable some new encryption protocol) you might require a separate NAP for upgraded and nonupgraded APs.



Note

If you want to aggregate NDGs and use them as a filter to assign users to a profile, you must configure NAFs before you set up a profile.

Protocol Types

You use Protocol Types to classify a user request based on the type of protocol that is used to request access to the network.

Advanced Filtering

You can create rules based on specific RADIUS attributes and values (including Cisco AV pairs). Each rule contains one or more rule elements, and each rule element must be true for the whole rule to be true. In other words, all rule elements of a rule are joined with a Boolean AND. For more information about advanced filtering options, see [Profile Setup Page, page 14-40](#).

Profile-based Policies

After you set up a profile, you associate a set of rules or policies with it to reflect your organization's security policies. These *profile-based policies* include rules for authentication, authorization, and posture validation.

By defining profile-based policies, you can redirect authentication to different directories. For example, wireless users need to authenticate to AD while the same users who access the network through VPN might need to authenticate to an RSA One-Time Password (OTP) directory.

When a packet is received, ACS evaluates the profile filters to classify the packet. When a profile matches, ACS applies the configuration and policies that are associated with the profile during packet processing. ACS uses a first-match strategy on the first access request of the transaction. If no matching profile is found, ACS reverts to the global configuration settings.

Workflow for Configuring NAPs and Profile-based Policies

You can create a profile from scratch, or you can use one of the supplied templates to populate some default values. The templates that are provided are particularly useful for NAC-enabled networks. See [Using Profile Templates, page 14-7](#), for more information.

The following is the order of work for creating NAPs and their associated policies:

1. Identify the network services that you want to control with ACS (for example, VPN, Dial, WLAN, `ip_admission`).
2. Set up a profile for each network service. Setting up a profile defines how ACS will recognize or identify requests (for example, device IP, NDG, NAF, advanced filtering). For more information, see [Adding a Profile, page 14-4](#).
3. Define the password protocols and EAP configuration for the service. For more information, see [Protocol Configuration for NAPs, page 14-23](#).
4. Define the authentication methods that are required for the service. For more information, see [Authentication Policy Configuration for NAPs, page 14-27](#).
5. Define the posture-validation policies or rules (optional, if network admission control (NAC) is part of the deployment). See [Posture-Validation Policy Configuration for NAPs, page 14-29](#) for more information.
6. Define SoH rules. See [Setting a Posture-Validation Policy to Process Statements of Health, page 14-32](#) for more information.
7. Define the authorization mappings from group to RADIUS authorization components (RAC) and downloadable access control lists (DAACL). Also include the system posture token (SPT) if NAC is in use. For more information, see [Configuring an Authorization Rule, page 14-36](#).

If access is granted (`access-accept`) ACS merges between user, user-group RAC and ACLs, and provisions a result to the AAA client. For more information, see [Merging Attributes, page 14-35](#).

Processing Unmatched User Requests

In ACS you can configure global configuration settings as well as NAP-specific settings. The global configuration settings serve two purposes:

- Defining the fallback behavior for a request that does not match a profile.

- Defining the baseline for NAPs (if you want to enable a protocol in the NAP authentication page, you must first enable it in the Global Authentication Setup page).

Although legacy global settings and NAPs are supported and are interoperable, we do not recommend both of them, except for the case that is described in this section.

We recommend that you deny access when no profile matches and the access request cannot be classified.

The only case where ACS fallback behavior and NAPs should be used is with TACACS+. NAPs does not currently support TACACS+. Granting access using the global configuration is the only way to use TACACS+ and NAP configuration with RADIUS.

When you use both, you must ensure that the fallback behavior using global configuration will not create a security flaw in the network.

Managing NAPs

These topics describe how to set up and manage NAPs:

- [Adding a Profile, page 14-4](#)
- [Ordering Profiles, page 14-5](#)
- [Editing a Profile, page 14-5](#)
- [Cloning a Profile, page 14-6](#)
- [Deleting a Profile, page 14-6](#)
- [Using Profile Templates, page 14-7](#)

Adding a Profile

This topic describes how to set up a profile from scratch. For information about creating a profile from a profile template, see [Using Profile Templates, page 14-7](#).

To add a profile:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles Page appears.
- Step 2** Click **Add Profile**.
The Profile Setup page appears.
- Step 3** In the **Name** box, type the name of the new profile.
- Step 4** In the **Description** box, type a description of the new profile.
- Step 5** To enable the profile, check the **Active** check box.
- Step 6** Configure the access request classification settings for the profile. See [Profile Setup Page, page 14-40](#) for more information about profile configuration options.
- Step 7** Click **Submit**.
The Network Access Profile page reappears. The Network Access Profile's first match is implemented to authenticate or authorize a client request, or both.

- Step 8** Click the **Up** or **Down** buttons to move the profile to the correct position and submit the information to ACS.
 - Step 9** Configure how ACS should handle unmatched access requests. See [Processing Unmatched User Requests, page 14-3](#) for information.
 - Step 10** Click **Apply and Restart** for your changes to take effect.
-

Ordering Profiles

Since ACS applies a first-match principle when trying to match an access request with a profile, the order of the profiles in the list is significant.

To set the order of the profile:

- Step 1** In the [Network Access Profiles Page, page 14-39](#), click the radio buttons to select a profile.
 - Step 2** Click the **Up** or **Down** to move the profile to the position you want.
 - Step 3** Click **Apply and Restart** for your changes to take effect.
-

Editing a Profile

To edit the profile configuration:

- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
 - Step 2** To modify the filtering methods for a profile:
 - a. In the Network Access Profiles page, click the profile name.
The Profile Setup page appears.
 - b. Modify filtering methods, as required. For information about filtering options, see [Profile Setup Page, page 14-40](#).
 - Step 3** To modify configuration policies for a profile:
 - a. Select the relevant configuration policy for the profile.
The relevant policy configuration page appears.
 - b. Edit the policy. For more information, see [Configuring Policies for Profiles, page 14-22](#).
 - Step 4** To save your profile configuration settings, return to the Network Access Profiles page and click **Apply and Restart**.
-

Cloning a Profile

Cloning replicates all the following relevant components for a NAP:

- **Protocol references**—Password protocols.
- **Authentication references**—External databases.
- **Posture references**—Internal or external posture validation, and external audit server. For more information about posture references, see [Setting Up Posture Validation Policies, page 13-16](#).
- **Authorization references**—RACs and DACLs.

Cloning a NAP does not copy the shared-profile components, or the internal and external posture-validation policies, that the profile references. The newly cloned profile *references* the same shared-profile components as the original profile. For example, components that are referenced by name (RACs, DACLs, NAFs) remain the same.

When you clone a NAP, it is initially inactive by default. This inactive state avoids ambiguity when ACS tries to match an access request to a profile. After you modify the cloned profile, you can change the status to the active state.

The Profile description, Active Flag, Protocol Selection, Advanced Filter, Authentication, and Authorization policies are all cloned (copied). Posture-validation policies (Internal/External/Audit Servers) are not copied, but are referenced by the newly created Profile.

The naming pattern for cloning is **Copy-of-**. For multiple cloning (cloning the cloned element) the prefix **Copy-(2)-of-** is given.

If the new name length exceeds 32 characters, it is truncated to 32 characters.

To clone a profile:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
 - Step 2** Click the name of the profile you want to clone.
The Profile Setup page appears.
 - Step 3** Click **Clone**.
A copy of the cloned profile appears in the Network Access Profiles page.
 - Step 4** (Optional) Modify the cloned profile. For information about editing profiles, see [Editing a Profile, page 14-5](#).
 - Step 5** Click **Apply and Restart** for your changes to take effect.
-

Deleting a Profile

To delete a profile:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
 - Step 2** Click the **Name**.

- The Profile Setup page appears.
- Step 3** Click **Delete**.
- A warning message appears.
- Step 4** Click **OK** to delete the profile configuration.
- Step 5** Click **Apply and Restart** for your changes to take effect.
-

Using Profile Templates

You use a *profile template* to construct a new profile. Instead of setting up a new profile from scratch, you can select a profile from a predefined set of profile templates. For a list of templates, see [Profile Templates, page 14-8](#). The templates include a preconfigured set of NAC samples that you can use as the basis for building NAC policies. After you have set up a new profile based on a template, you can customize the profile settings to the specific needs of your security policy.



Note

Each template references a set of shared-profile components. Before creating a template, ACS verifies that the appropriate shared-profile components exist. If the shared-profile components were not configured, ACS uses a set of shared-profile components that were created especially for the selected template.

When you select a predefined template, ACS creates a full-scale NAP, including profile authentication, posture validation, and authorization policies.

The following topics describe profile templates and how to use them:

- [Prerequisites for Using Profile Templates, page 14-7](#)
- [Creating a Profile with a Profile Template, page 14-8](#)
- [Profile Templates, page 14-8](#)

Prerequisites for Using Profile Templates

Before you can use a profile template, you must configure:

- At least one AAA client by using the RADIUS Internet Engineering Task Force (IETF) protocol.
- Certificate setup.
- Administrator accounts (if needed).
- Logging settings.
- Global Authentication Setup for templates, depending on the template.
- User-Level or Group-Level Downloadable ACLs in the Interface Configuration > Advanced Options, depending on the template.

ACS rules are constructed from attributes that reside in the ACS dictionaries. During installation, the ACS posture dictionary is initialized to include attributes that belong to the `cisco:pa`. (It is mandatory that this default set of attributes be supported by every Cisco Trust Agent implementation.)

The internal posture-validation policies that the templates create are based on these sets of attributes.

In ACS, each template that is created references a set of reusable objects. Before creating the template, ACS verifies that the relevant reusable objects already exist. If they do not, ACS automatically creates the required objects for the template. Creation of profiles from templates will not fail if these objects do not exist beforehand. If the reusable objects exist for the selected template, ACS uses the relevant reusable objects.

**Note**

You cannot delete an attribute if it is being used in a posture-validation policy.

Creating a Profile with a Profile Template

To select a profile template:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
- Step 2** Click **Add Template Profile**.
The [Create Profile from Template Page, page 14-43](#), appears.
- Step 3** Enter an **Name** and **Description** for the Profile.
- Step 4** Select a template from the drop-down list.
- Step 5** Check the **Active** check box to activate the profile.
- Step 6** Click **Submit**.
A window appears showing the new objects that have been created for the profile.
- Step 7** Click **Close**.
The Network Access Profiles page reappears showing the new profile.
- Step 8** To save your profile configuration settings, click **Apply and Restart**.
-

Profile Templates

These topics describe the profile templates that ACS provides:

- [NAC L3 IP, page 14-9](#)
- [NAC L2 IP, page 14-11](#)
- [NAC Layer 2 802.1x, page 14-14](#)
- [Microsoft IEEE 802.1x, page 14-16](#)
- [Wireless \(NAC L2 802.1x\), page 14-17](#)
- [Agentless Host for L2 \(802.1x Fallback\), page 14-17](#) (802.1x fallback)
- [Agentless Host for L3, page 14-18](#) (EAP over User Datagram Protocol (UDP) fallback)
- [Agentless Host for L2 and L3, page 14-20](#)

NAC L3 IP

This template is used for access requests from a LAN Port IP by using Layer 3 posture validation.

Before you use this template, ensure that you have checked the following options in the Global Authentication Setup page:

- Allow Posture Validation.
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) authenticated in-band PAC provisioning.
- EAP-FAST MS-CHAPv2.
- EAP-FAST Generic Token Card (GTC).

Downloadable ACLs

Downloadable per-user ACL support is available for Layer 3 network devices that support downloadable ACLs. These include Cisco PIX security appliances, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that you can apply per user or per group. This feature complements NAC support by enabling the enforcement of the correct ACL policy. When you use this feature in conjunction with NAFs, you can apply downloadable ACLs differently per device, allowing you to tailor ACLs uniquely per user or per access device.

Table 14-1 describes the Profile Sample in the NAC Layer 3 IP Sample Profile Template.

Table 14-1 NAC Layer 3 IP Profile Sample

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(([[26/9/1]Cisco av-pair]aaa:service = ip_admission) AND ([006]Service-Type != 10)
Authentication	Protected Extensible Authentication Protocol (PEAP)	Allow Posture Only is checked
	Credential Validation Database	N/A

Table 14-1 NAC Layer 3 IP Profile Sample (continued)

Section	Property		Value		
Posture Validation	Posture Validation Rule	Name	NAC-EXAMPLE-POSTURE-EXAMPLE		
		Required credential types	Cisco:PA		
		Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
		Selected external posture policies	N/A		
	System Posture Token configuration	System Posture Token	PA message	URL Redirect	
		Healthy	Healthy	N/A	
		Checkup	Checkup	N/A	
		Transition	Transition	N/A	
		Quarantine	Quarantine	N/A	
		Infected	Infected	N/A	
	Unknown	Unknown	N/A		

Table 14-2 Authorization Rules for NAC Layer 3 IP Profile Template

Authorization Rules	User Group	System Posture Token	Shared RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC-SAMPLE-HEALTHY-ACL
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC-SAMPLE-QUARANTINE-ACL
Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 14-3 describes the posture-validation policies in the NAC Layer 3 IP Sample Profile Template.

Table 14-3 Posture Validation for NAC Layer 3 IP Sample

Section	Object	Value	System Posture Token	Notification String	
Internal posture policy	NAC-SAMPLE-CTA-POLICY	Condition			
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

Table 14-4 describes the Shared Profile Components in the NAC Layer 3 IP Sample Profile Template.

Table 14-4 Shared Profile Components for NAC Layer 3 IP Sample

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [26/9/1]cisc-av-pair status-query-timeout=300 [029] Termination-Action RADIUS-Request (1)
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [26/9/1]cisc-av-pair status-query-timeout=30 [029] Termination-Action RADIUS-Request (1)
Downloadable IP ACLs	NAC-SAMPLE-HEALTHY-ACL	ACL Content Name
	NAC-SAMPLE-QUARANTINE-ACL	L3-EXAMPLE
		Content
		permit ip any any
		NAF
		(All-AAA-Clients)

NAC L2 IP

Before you use this template, ensure that you have checked the Enable EAP Configuration > Allow Posture Validation option in the Global Authentication Setup page.

You can use NAC Layer 2 IP on an access port on an edge switch to which an endpoint system or client is connected. The device (host or client) can be a PC, a workstation, or a server that is connected to the switch access port through a direct connection, an IP phone, a hub, or a wireless access point.

When NAC Layer 2 IP is enabled, UDP only works with IPv4 traffic. The switch checks the antivirus condition of the endpoint devices or clients and enforces access-control policies.

This template sets Advanced Filtering and Authentication properties with NAC-L2-IP Configuration automatically.

ACS and AV Pairs

When you enable NAC Layer 2 IP validation, ACS provides NAC AAA services by using RADIUS. ACS gets information about the antivirus credentials of the endpoint system and validates the antivirus condition of the endpoint.

You can set these Attribute-Value (AV) pairs on ACS by using the RADIUS cisco-av-pair vendor-specific attributes (VSAs).

- **Cisco Secure-Defined-ACL**—Specifies the names of the downloadable ACLs on the ACS. The switch gets the ACL name through the Cisco Secure-Defined-ACL AV pair in this format:

#ACL#-IP-name-number

where *name* is the ACL name and *number* is the version number, such as 3f783768.

The Auth-Proxy posture code checks if the access-control entries (ACEs) of the specified downloadable ACL were previously downloaded. If it was not, the Auth-Proxy posture code sends an AAA request with the downloadable ACL name as the username so that the ACEs are downloaded. The downloadable ACL is then created as a named ACL on the switch. This ACL has ACEs with a source address of **Any** and does not have an implicit **Deny** statement at the end. When the downloadable ACL is applied to an interface after posture validation is complete, the source address is changed from any to the host source IP address. The ACEs are prepended to the downloadable ACL that is applied to the switch interface to which the endpoint device is connected.

If traffic matches the Cisco Secure-Defined-ACL ACEs, the appropriate NAC actions are taken.

- **url redirect and url-redirect-acl**—Specifies the local URL policy on the switch. The switches use these cisco-av-pair VSAs:

— *url-redirect = <HTTP or HTTPS URL>*

— *url-redirect-acl = switch ACL name*

These AV pairs enable the switch to intercept an HyperText Transfer Protocol (HTTP) or Secure HyperText Transfer Protocol (HTTPS) request from the endpoint device and forward the client web browser to the specified redirect address from which the latest antivirus files can be downloaded. The url-redirect AV pair on the ACS contains the URL to which the web browser will be redirected. The url-redirect-acl AV pair contains the name of an ACL which specifies the HTTP or HTTPS traffic to be redirected. The ACL must be defined on the switch. Traffic which matches a permit entry in the redirect ACL will be redirected.

These AV pairs might be sent if the host's posture is not healthy.

For more information about AV pairs that Cisco IOS software supports, see the documentation about the software releases that run on the AAA clients.

Default ACLs

If you configure NAC Layer 2 IP validation on a switch port, you must also configure a default port ACL on a switch port. You should also apply the default ACL to IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the switch and the ACS sends a host access policy to the switch, the switch applies the policy to traffic from the host that is connected to a switch port. If the policy applies to the traffic, the switch forwards the traffic. If the policy does not apply, the switch applies the default ACL. However, if the switch gets a host access policy from the ACS, but the default ACL is not configured, the NAC Layer 2 IP configuration does not take effect.

When ACS sends the switch a downloadable ACL that specifies a redirect URL as a policy-map action, this ACL takes precedence over the default ACL that is already configured on the switch port. The default ACL also takes precedence over the policy that is already configured on the host. If the default port ACL is not configured on the switch, the switch can still apply the downloadable ACL from ACS.

You use this template for access requests from Layer 2 devices that do not have the 802.1x client installed. The Authentication Bypass (802.1x fallback) template is used for access requests to bypass the nonclient authentication process. Users are mapped to a User Group based on their identity.

**Note**

Do not use the Populate from Global button; otherwise, this authentication field will be inherited from the settings in the Global Authentication Setup in System Configuration.

Table 14-5 describes the content of the Profile in the NAC Layer 2 IP Sample Profile Template.

Table 14-5 NAC Layer 2 IP Profile Sample

Section	Property	Value			
NAP	Name	User configurable			
	Description	User configurable			
Profile	NAF	N/A			
	Protocol	N/A			
	Advance filter	<code>([[26/9/1]Cisco av-pair]aaa:service = ip_admission) AND ([006]Service-Type != 10)</code>			
Authentication	PEAP	Allow Posture Only is checked			
	Credential Validation Database	N/A			
Posture Validation	Posture Validation Rule	Name	NAC-EXAMPLE-POSTURE-EXAMPLE		
		Required credential types	Cisco:PA		
		Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
		Selected external posture policies	N/A		
		System Posture Token configuration	System Posture Token	PA message	URL Redirect
	Healthy	Healthy	N/A		
	Checkup	Checkup	N/A		
	Transition	Transition	N/A		
	Quarantine	Quarantine	N/A		
Infected	Infected	N/A			
Unknown	Unknown	N/A			

Table 14-6 describes the content of the Authorization Rules in the NAC Layer 2 IP Sample Profile Template.

Table 14-6 Authorization Rules for NAC Layer 2 IP Profile Template

Authorization Rules	User-Group	System Posture Token	RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC-SAMPLE-HEALTHY-ACL
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC-SAMPLE-QUARANTINE-ACL

Table 14-6 Authorization Rules for NAC Layer 2 IP Profile Template (continued)

Authorization Rules	User-Group	System Posture Token	RAC	DACL
Default			NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 14-7 describes the content of the posture-validation policies in the NAC Layer 2 IP Sample Profile Template.

Table 14-7 Posture Validation for NAC Layer 2 IP Sample

Section	Object	Value
Internal posture policy	NAC-SAMPLE-POSTURE-RULE	Condition
	Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0
	Default	N/A
		System Posture Token
		Notification String
		Cisco:PA:Healthy
		N/A
		Cisco:PA:Quarantine
		N/A

NAC Layer 2 802.1x

Before you use this template, ensure that you have checked the following options in the Global Authentication Setup page:

- EAP-FAST
- EAP-FAST Authenticated in-band PAC Provisioning
- EAP-FAST MS-CHAPv2
- EAP-FAST GTC

Table 14-8 describes the content of the NAC L2 802.1x Sample Profile Template.

Table 14-8 NAC L2 802.1x Profile Sample

Section	Property	Value
NAP	Name	User configured
	Description	User configured
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	([006]Service-Type != 10) and (not exist [26/9/1]cisco-av-pair aaa:service)

Table 14-8 NAC L2 802.1x Profile Sample (continued)

Section	Property	Value			
Authentication	EAP-FAST	Allow EAP-FAST is checked. Allow authenticated in-band PAC provisioning is checked. Allow inner methods EAP-GTC is checked. Allow inner methods EAP-MS-CHAPv2 is checked. Allow Stateless Session Resume is checked. Accept client on authenticated provisioning is checked. Posture Validation required is checked.			
	Credential Validation Database	ACS Internal user database			
Posture Validation					
Posture validation Rule	Name	NAC-SAMPLE-POSTURE-RULE			
	Required credential types	Cisco:PA			
	Selected internal posture policies	NAC-SAMPLE-CTA-POLICY			
	Selected external posture policies	N/A			
	System Posture Token configuration	System Posture Token	PA message	URL	
		Healthy	Healthy	N/A	
		Checkup	Checkup	N/A	
		Transition	Transition	N/A	
Quarantine		Quarantine	N/A		
Infected		Infected	N/A		
	Unknown	Unknown	N/A		

Table 14-9 describes the content of the Authorization Rules in the NAC Layer 802.1x Sample Profile Template.

Table 14-9 Authorization Rules for NAC Layer 2 801.x Profile Sample

Authorization Rules	User group	System Posture Token	RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L2-RAC	N/A
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L2-RAC	N/A
Default			NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL

Table 14-9 Authorization Rules for NAC Layer 2 801.x Profile Sample (continued)

Authorization Rules	User group	System Posture Token	RAC	DAACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 14-10 describes the content of the posture-validation policies in the NAC Layer 802.1x Sample Profile Template.

Table 14-10 Posture Validation for NAC Layer 2 802.1x Profile Sample

Section	Object	Value			
Internal posture policy	NAC-SAMPLE-CTA-POLICY		Condition	System Posture Token	Notification String
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

Table 14-11 describes the content of the Shared Profile Components in the NAC Layer 802.1x Sample Profile Template.

Table 14-11 Shared Profile Components for NAC Layer 2 802.1x Profile Template

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-HEALTHY-L2-RAC	[027] Session-Timeout = 36,000 [26/9/1] cisco-av-pair sec:pg=healthy_hosts [029] Termination-Action RADIUS-Request (1) [064] Tunnel-Type [T1] VLAN (13) [065] Tunnel-Medium-Type [T1] 802 (6) [081] Tunnel-Private-Group-ID = healthy
	NAC-SAMPLE-QUARANTINE-L2-RAC	[027] Session-Timeout = 3,600 [26/9/1]cisco-av-pair sec:pg=quarantine_hosts [029] Termination-Action RADIUS-Request (1) [064] Tunnel-Type [T1] VLAN (13) [065] Tunnel-Medium-Type [T1] 802 (6) [081] Tunnel-Private-Group-ID = quarantine

Microsoft IEEE 802.1x

Before you use this template, ensure that you have checked the Allow EAP-MS-CHAPv2 option in the Global Authentication Setup page.

Table 14-12 describes the Profile Sample in the Microsoft IEEE 802.1x Sample Profile Template.

Table 14-12 Microsoft IEEE 802.1x Profile Sample

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(([006]Service-Type != 10) and (not exist [26/9/1]cisco-av-pair aaa:service))
Authentication	PEAP	Allow EAP MS-CHAPv2 is checked
	Credential Validation Database	ACS Internal Users Database
Posture Validation	N/A	

Table 14-13 describes the Authorization Rules in the Microsoft IEEE 802.1x Sample Profile Template.

Table 14-13 Authorization Rules for Microsoft IEEE 802.1x Profile Sample

Authorization Rules	User Group	System Posture Token	RAC	DACL
Default	Deny = unchecked			
Include RADIUS attributes from user's group	Checked			
Include RADIUS attributes from user record	Checked			

Wireless (NAC L2 802.1x)

The templates for wireless (NAC L2 802.1x) are the same as the NAC L2 802.1x templates. See [NAC Layer 2 802.1x, page 14-14](#) for more information.

Agentless Host for L2 (802.1x Fallback)

You can use the Agentless Host for L2 (802.1x Fallback) profile template to create a profile that matches a RADIUS request that will come from a switch. Once the profile is created an analysis of the RADIUS packet that comes from the Catalyst 6500 must be done to create an accurate match for the profile. The RADIUS request from the switch has a Service Type value of 10, just like NAC-L2-IP; but does not have a Cisco Attribute Value Pair (AVP) that contains the keywords service. Therefore, two entries are created in the Advanced Filtering box.

Table 14-14 describes the content of the Profile Sample in the Agentless Host for L2 (802.1x Fallback) Sample Profile Template.

Table 14-14 Agentless Host for L2 (802.1x Fallback) Sample Profile

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(not exist [26/9/1]cisco-av-pair aaa:service) AND ([006]Service-Type = 10)
	Credential Validation Database	N/A
Authentication	Protocols	Allow Agentless Request Processing will be checked Default user-group will be set to default group
Posture Validation	N/A	

Table 14-15 describes the content of the Authorization Rules in the Authentication Bypass Sample Profile Template.

Table 14-15 Authorization Rules for Agentless Host for L2 (802.1x Fallback) Sample Profile

Authorization Rules	User Group	System Posture Token	RAC	DAACL
Rule 1	Default-group	N/A	NAC-SAMPLE-QUARANTINE-L2-RAC	N/A
Default	Deny = checked			
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Agentless Host for L3

This template is used for access requests for NAC Agentless Hosts (NAH), also known as agentless hosts. These requests use EAP over UDP (EoU).

Table 14-16 describes the Profile Sample in the Agentless Host for L3 Sample Profile Template.

Table 14-16 Agentless Host for L3 Sample Profile Template

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable

Table 14-16 Agentless Host for L3 Sample Profile Template (continued)

Section	Property	Value			
Profile	NAF	N/A			
	Protocol	N/A			
	Advance filter	([[26/9/1]Cisco av-pair]aaa:service = ip_admission) AND ([006]Service-Type = 10)			
	Credential Validation Database	N/A			
Posture Validation	N/A				
Authorization	Rules	User-group	System Posture Token	RAC	DACL
		N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL
		N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
		N/A	Transition	NAC-SAMPLE-TRANSITION-L3-RAC	NAC_SAMPLE_TRANSITION_ACL
	Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
	Include RADIUS attributes from user's group	Unchecked			
	Include RADIUS attributes from user record	Unchecked			

Table 14-17 describes the Shared Profile Components in the Agentless Host for L3 Sample Profile Template.

Table 14-17 Shared Profile Components for Agentless Host for L3 Sample

Type	Object	Value		
RADIUS Authorization Components	NAC-SAMPLE-TRANSITION-L3-RAC	[027] Session-Timeout = 60 [029] Termination-Action RADIUS-Request (1) A Session-Timeout can be overwritten if hinted by an audit server		
	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [029] Termination-Action RADIUS-Request (1)		
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [029] Termination-Action RADIUS-Request (1)		
Downloadable IP ACLs		ACL Content Name	Content	NAF
	NAC-_SAMPLE-_TRANSITION-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_HEALTHY-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_QUARANTINE-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

Agentless Host for L2 and L3

This template is used for access requests from agentless hosts connected to an L2 Network Access Device (NAD). ACS first admits the device to a quarantine network where it can receive an IP address. Audit begins when the device has received an IP address. At this point, the audit is the same as an audit for an L3 host. The NAD must be configured to learn the host's IP address ahead of time. ACS responds to an initial Access-Request with a notification to the device to issue another request when it learns the IP address. If the NAD does not learn the host's IP address, ACS invokes a failure condition and policy flow falls over to Audit Fail-Open policy. The administrator can then choose to reject the user, or assign a posture token and an optional user group.

[Table 14-18](#) describes the Profile Sample in the Agentless Host for L2 and L3 Sample Profile Template.

Table 14-18 Agentless Host for L2 and L3 Sample Profile Template

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable

Table 14-18 Agentless Host for L2 and L3 Sample Profile Template (continued)

Section	Property	Value			
Profile	NAF	N/A			
	Protocol	N/A			
	Advance filter	([006]Service-Type = 10) AND (not exist [26/9/1]cisco-av-pair aaa:service) AND (audit-session-id=^)			
	Credential Validation Database	N/A			
Posture Validation	N/A				
Authorization	Rules	User-group	System Posture Token	RAC	DACL
		N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL
		N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
		N/A	Transition	NAC-SAMPLE-TRANSITION-L3-RAC	NAC_SAMPLE_TRANSITION_ACL
	Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
	Include RADIUS attributes from user's group	Unchecked			
	Include RADIUS attributes from user record	Unchecked			

Table 14-19 describes the Shared Profile Components in the Agentless Host for L2 and L3 Sample Profile Template.

Table 14-19 Shared Profile Components for Agentless Host for L3 and L3 Sample

Type	Object	Value		
RADIUS Authorization Components	NAC-SAMPLE-TRANSITION-L3-RAC	[027] Session-Timeout = 60 [029] Termination-Action RADIUS-Request (1) A Session-Timeout can be overwritten if hinted by an audit server		
	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [029] Termination-Action RADIUS-Request (1)		
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [029] Termination-Action RADIUS-Request (1)		
Downloadable IP ACLs		ACL Content Name	Content	NAF
	NAC-_SAMPLE-_TRANSITION-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_HEALTHY-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_QUARANTINE-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

Configuring Policies for Profiles

After you set up a profile, you associate a set of rules or policies with it, to reflect your organization's security policies. You can configure policies for:

- **Protocols** — Define the password protocols and EAP configuration.
- **Authentication**—A set of configuration policies that are related to authentication mechanisms.
- **Posture validation**—Define the manner in which posture validation will be performed (only if you plan to deploy NAC in your network).
- **Authorization**—Configure a set of authorization rules (optional).

ACS associates attributes according to the profile that was requested. The attributes that are returned in an `Access-Accept` message are a consolidation of attributes that are associated with a profile (such as `Tunnel-Type` for a VPN profile request) and session-specific attributes that are bound to the end-user (such as `Idle-Timeout` for example). The profile mapping is independent of the user identity; therefore, each user can use multiple profiles, and has only one entry in the validating database.

These topics describe how to configure and manage policies for NAPs:

- [Protocol Configuration for NAPs, page 14-23](#)
- [Authentication Policy Configuration for NAPs, page 14-27](#)
- [Posture-Validation Policy Configuration for NAPs, page 14-29](#)
- [Authorization Policy Configuration for NAPs, page 14-34](#)

Protocol Configuration for NAPs

These topics describe how to configure authentication protocols for NAPs:

- [Authentication Protocols](#), page 14-23
- [Agentless Request Processing](#), page 14-24
- [EAP Configuration for NAPs](#), page 14-25
- [EAP-FAST with Posture Validation](#), page 14-25
- [EAP Authentication with RADIUS Key Wrap](#), page 14-25
- [Configuring Protocols](#), page 14-26

Authentication Protocols

You can configure all relevant parameters for authentication protocols for your NAPs. These parameters are applied during access request processing.

Populating Protocol Setting with ACS Global Settings

You can populate the protocol settings with the ACS global settings, and then customize them. This method facilitates configuring the protocol settings each time you set up a new profile.

Global Authentication Setup serves as a central location for all of the EAP configuration settings in the active or inactive profiles. You cannot enable EAP types in an ACS profile, which are disabled in the Global Authentication Page. Every EAP type that is unchecked in the Global Authentication Page will automatically be unchecked in all ACS (active and inactive) profiles. Options that are not available in the Global Authentication Setup page, are unchecked in the Protocol Settings page after populating from the Global Authentication Setup page.

To apply global settings: Click **Populate from Global** to apply authentication settings that were set in the **System Configuration > Global Authentication Setup** window. For more information, see [Configuring Authentication Options](#), page 9-21.

We recommend that you check all authentication protocols in the Global Authentication Setup for NAC. The following authentication protocols, listed from weakest to most secure, can be configured:

- RADIUS Authentication protocols allow or disallow authentication by using:
 - Password Authentication Protocol (PAP) protocol.
 - CHAP password protocol.
 - MS-CHAPv1 password protocol.
 - MS-CHAPv2 password protocol.
 - Agentless Request Processing. For more information, see [Agentless Request Processing](#), page 14-24.
 - An option to allow or disallow a set of EAP types (outer and inner) to be used for EAP authentication, including the relevant setting for each EAP-type. See [EAP Configuration for NAPs](#), page 14-25, for more information.
- You can configure the following EAP protocols:
 - PEAP
 - EAP-FAST

- EAP-Transport Layer Security (TLS) with or without RADIUS Key Wrap. See [EAP Authentication with RADIUS Key Wrap, page 14-25](#), for more information.
- EAP-Message Digest 5 (MD5)

The protocols that you select determine the flexibility of negotiation. The final result is to determine which protocol to use to authenticate. For more information about protocols, see [About Certification and EAP Protocols, page 9-1](#).

**Note**

LEAP (EAP-Cisco Wireless) is not supported when working with Network Access Profiles.

Agentless Request Processing

Agentless Request Processing, is an identity-based network security feature that is configured on a port basis. A switch makes a RADIUS request to ACS with the MAC (Media Access Control) address of the endhost connecting to the switch. Agentless authentication happens on the switch or device as a fallback that results from a 802.1x failure or an EAPoUDP failure, and hence bypasses these mechanisms. This feature is useful for allowing network access for hosts without 802.1x or EAPoUDP support. For example, devices such as printers or terminals that do not have an 802.1x client can use this feature to access to the network.

You can use this feature to map MAC addresses to user groups. You can use a configured LDAP server or the internal ACS Database to authenticate MAC address user requests. ACS uses the LDAP server to look up MAC addresses and to retrieve LDAP group attributes for MAC addresses. If the MAC addresses exist in the LDAP Server, ACS maps the LDAP Group to the ACS Groups configured in the configured ACS External LDAP Database. ACS accepts any of the MAC address standard formats. If the list of defined addresses does not contain a MAC address, you can associate a fallback user group with the access request. Groups can be included in the profile's authorization policy and then be evaluated for network admission based on authorization rules.

For information about configuring the LDAP external database for agentless requests see *Configuration Guide for Cisco Secure ACS Release 4.2*.

The MAC address is sent in the Calling-Station-ID RADIUS attribute. ACS identifies an Agentless Request in this manner:

Service-Type = 10 (Call Check)

If the **Allow Agentless Request Processing** option is not enabled, MAC address authentication is not applied and the access request is rejected.

ACS supports the following three standard formats for representing MAC-48 addresses in human-readable form:

- Six groups of two hexadecimal digits, separated by hyphens (-) in transmission order, for example, *01-23-45-67-89-ab*.
- Six groups of two separated by colons (:), for example, *01:23:45:67:89:ab*.
- Three groups of four hexadecimal digits separated by dots (.), for example, *0123.4567.89ab*.

An Error alert appears for invalid MAC addresses. MAC addresses are presented in one format regardless of the format in which they were entered into ACS.

To process agentless requests, **Allow Agentless Request Processing** must be enabled in the [Protocols Settings for profile_name Page, page 14-43](#). You must also define settings in the [Authentication for profile_name Page, page 14-46](#). You choose which configured database to use to authenticate a MAC address user request, and define the default mapping for MAC addresses that do not match.

EAP Configuration for NAPs

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x, or RADIUS and supports multiple authentication types:

- PEAP (Protected EAP)
- EAP-FAST
- EAP-TLS (based on X.509 certificates)
- EAP-MD5: Plain Password Hash (CHAP over EAP)
- EAP-GTC: OTP Tokens

**Note**

You can enable RADIUS Key Wrap attributes for PEAP, EAP-FAST and EAP-TLS authentication.

The following extended EAP methods are available for NAC:

- EAP-TLV: Carry posture credentials, adding posture AVPs, posture notifications.
- Status Query: You can use this new EAP method for securely querying the status of a peer without a full credential validation.
- EAPoUDP: use of EAP over UDP for Layer 3 transport.

EAP-FAST with Posture Validation

Several organizations might be in the process of supplying their hosts with the Cisco Trust Agent and some hosts might or might not have the Cisco Trust Agent installed. Cases might arise where you might want to enforce posture validation on machines with the Cisco Trust Agent; however, you do not want to fail authentication on those machines that are temporarily without the Cisco Trust Agent. When EAP-FAST is enabled with Required Posture Validation, you can select the Optional selection and supply a resulting SPT. You can use the SPT that is set here for setting Authorization settings. For a description of the tokens that are used in ACS, see [Posture Tokens, page 13-3](#).

**Note**

If posture-validation rules are not defined, the posture token returned is **Unknown**.

EAP Authentication with RADIUS Key Wrap

You can configure ACS to use PEAP, EAP-FAST and EAP-TLS authentication with RADIUS Key Wrap. ACS can then authenticate RADIUS messages and distribute the session key to the network access server (NAS). The EAP session key is encrypted by using Advanced Encryption Standard (AES), and the RADIUS message is authenticated by using HMAC-SHA-1.

Because RADIUS is used to transport EAP messages (in the EAP-Message attribute), securely authenticating RADIUS messages ensures securely authenticated EAP message exchanges. You can use RADIUS Key Wrap when PEAP, EAP-FAST and EAP-TLS authentication is enabled as an external authentication method. Key Wrap is not supported for EAP-TLS as an inner method (for example, for EAP-FAST or PEAP).

RADIUS Key Wrap support in ACS uses three new AVPs for the cisco-av-pair RADIUS Vendor-Specific-Attribute (VSA); the TLV value of Cisco VSA is [26/9/1]:

- **Random-Nonce**—Generated by the NAS, it adds randomness to the key data encryption and authentication, and links requests and response packets to prevent replay attacks.
- **Key**—Used for session key distribution.
- **Message-Authenticator-Code**—Ensures the authenticity of the RADIUS message, including the EAP-Message and Key attributes.

When using RADIUS Key Wrap, ACS enforces the use of these three RADIUS Key Wrap AVPs for message exchanges and key delivery. ACS will reject all RADIUS (EAP) requests that contain RADIUS Key Wrap AVPs and the standard RADIUS Message-Authenticator attribute.

To use RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications, you must enable the EAP authentication with RADIUS Key Wrap in the Protocol Settings page for the NAP. You must also define two shared secret keys for each AAA Client, or for an NDG. Each key must be unique, and must also be distinct from the RADIUS shared key. RADIUS Key Wrap does not support proxy functionality, and should not be used with a proxy configuration.

Configuring Protocols

To configure protocols for NAPs:

Step 1 Choose **Network Access Profiles**.

The Network Access Profiles page appears.

Step 2 Click **Protocol** for the relevant NAP.

The Protocols and EAP Configuration page appears.

Step 3 To populate the page with ACS global protocol settings, select **Populate from Global**. For more information about global protocol settings, see [Configuring Authentication Options, page 9-21](#).



Note If LEAP was configured in the Global Authentication Setup page, it will not be supported with NAPs.

Step 4 To process agentless requests, choose one of the available options in **Allow Agent Request Processing** to authenticate MAC address user requests.

Step 5 Change other settings as required. For information about options, see [Protocols Settings for profile_name Page, page 14-43](#).

Step 6 Click **Submit**.

The Network Access Profiles page reappears.

Step 7 Click **Apply and Restart** for your changes to take effect.

Authentication Policy Configuration for NAPs

Authentication settings define which databases are used to validate the credentials of the user for authentication. Before you configure authentication policies configure the External User Databases that you mapped to ACS user groups by the mapping rules that are defined in Database Group Mapping.



Note The ACS internal database is the default selected database.

You can also configure Agentless Request Processing for MAC addresses as part of your authentication policy. For more information, see [Agentless Request Processing, page 14-24](#).

These topics describe how to configure authentication settings:

- [Credential Validation Databases, page 14-27](#)
- [Group Filtering at NAP Level, page 14-27](#)
- [Object Identifier Check for EAP-TLS Authentication, page 14-28](#)
- [Configuring Authentication Policies, page 14-28](#)

Credential Validation Databases

The Credential Validation Databases are databases that you use to validate users. The Available Databases are the configured External User Databases that are mapped to ACS user groups by the mapping rules defined in Databases Group Mapping. The ACS internal database appears, by default, as a selected database.



Note

If you specify multiple databases for authentication, ACS will query each directory server in the order specified until it receives an authoritative response. You should put the most likely directory servers higher in the list to improve response times and user experience.

Group Filtering at NAP Level

You can use ACS to perform group filtering at the NAP level. Depending on the user's external database group membership, ACS can reject or accept access to the network based on the group filtering settings.

Group filtering indicates the expected group membership in an external LDAP database. For example, if the group filter for the NAP is configured as *LDAP_GRP1*, *LDAP_GRP2*, the user must belong to any one of these groups in LDAP to authenticate successfully.

Group filtering is checked while performing group mapping during external database authentication.



Note

Group filtering occurs at the NAP level and cannot be used as a NAP selection criteria, since a user's external database membership is still unknown during the NAP selection processing.



Note

This feature is based at the NAP level only for RADIUS authentications, since NAPs are applicable only for RADIUS packet processing.

Object Identifier Check for EAP-TLS Authentication

ACS can compare the OID against the Enhanced Key Usage (EKU) field in the user's certificate. ACS denies access if the OID and EKU do not match. For more information about options, see [Authentication for profile_name Page, page 14-46](#).

When OID comparison is enabled and a valid OID string is entered, all the certificates that the users present for EAP-TLS authentication are checked against the OIDs entered. Authentication will be successful only if the OIDs match. If OID comparison is enabled but the user certificate presented does not contain any OID in the EKU field, authentication will fail.

To enable OID comparison you must:

- Enable EAP-TLS from the NAP page.
- Enter only contain numbers, dots, commas and spaces in the OID strings, for example: 1.3.6.1.5.5.7.3.2 is a valid OID string.
- Enter multiple OIDs as comma-separated values. For example: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2 is a valid string.

Configuring Authentication Policies

To configure authentication policies for NAPs:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Click **Authentication** for the relevant policy.
The Authentication Settings page appears.
- Step 3** Select **Populate from Global** to populate authentication settings from the ACS Global Authentication Setup page. For more information, see [Global Authentication Setup Page, page 9-41](#).
- Step 4** Select the **Credential Validation Databases**. For information about options, see [Authentication for profile_name Page, page 14-46](#).
- Step 5** Configure **Group Filtering**. For more information about options, see [Authentication for profile_name Page, page 14-46](#).
- Step 6** To configure MAC authentication settings:
- a. Choose which configured database to use to authenticate MAC address user request. You can use a configured LDAP server or the internal ACS Database to authenticate MAC address user requests.
 - b. Define the default mapping for MAC addresses that do not match by selecting a group from the drop-down list.
- For information about options, see [Authentication for profile_name Page, page 14-46](#).
- Step 7** Compare the OID (optional). For information about options, see [Authentication for profile_name Page, page 14-46](#).
- Step 8** Click **Submit**.
The Network Access Profiles page reappears.
- Step 9** Click **Apply and Restart** for your changes to take effect.
-

Posture-Validation Policy Configuration for NAPs

These topics contain information about configuring posture-validation policies:

- [About Posture Validation Rules, page 14-29](#)
- [Setting a Posture-Validation Policy, page 14-30](#)
- [Deleting a Posture Validation Rule, page 14-31](#)
- [Configuring Posture Validation for Agentless Hosts, page 14-33](#)

About Posture Validation Rules

Posture validation rules are used to select the posture validation components. A posture validation rule is comprised of a condition and actions. The condition is a set of required credential types. The actions are to determine which internal policies or external servers should be used for posture validation. Posture validation rules return a posture token and action for a posture request. See [Chapter 13, “Posture Validation in Network Access Control,”](#) for more information.

ACS interprets a posture-validation rule as:

If posture credentials contain data that was sent from the following plug-ins <required credential types>, then perform posture validation by using the following internal, external, or both internal and external posture validation methods <list of internal policies and external servers>.

ACS applies all the policies that associated with the selected posture-validation rule to derive application posture tokens (APT), which represent the state of the client (also known as the endpoint). ACS compares all derived APTs and uses the worst case posture token as the SPT, which symbolizes the overall posture of the client.

You can also set up policies and associated rules to process SoH from external AAA servers used in these networks.

Audit servers are Cisco and third-party servers that determine posture information about a client without relying on the presence of a NAC-compliant Posture Agent (PA). These types of clients are referred to as NAC Agentless Hosts (NAH). Audit servers are used to assess posture validation with an organization’s security policy. For more information, see [Setting a Posture-Validation Policy, page 14-30](#).

The Cisco PA is also known as the Cisco Trust Agent.

Each rule contains:

- Name (posture-validation policy) for identification.
- Required credential types that define the credential types that activate this rule.
- Internal policies and external servers that execute to calculate the posture token. You should configure these policies before creating Posture Validation rules. See [Configuring Policies, page 13-15](#).
- Posture Agent (PA) messages that return to the client for each SPT.
- URL redirect that is sent to the AAA client for each SPT.

**Note**

ACS supports up to 100 rules per policy.

The posture rules are evaluated in a first-match strategy. A posture-validation policy can have zero or more ordered posture-validation rules and is selected by using the first rule that matches.

Audit Server Functionality

The audit server scans the host and returns the token to ACS. The audit server may use asynchronous port scans, HTTP redirection, a proprietary client, and table lookups to provide posture-validation information. ACS polls for the audit result, so the audit server must hold its results until the next poll.

For more information about setting up audit servers, see [Setting Up an External Audit Posture Validation Server, page 13-25](#).

System Posture Token Configuration

A system posture token is associated with the state of the computer and a posture token is associated with the state of a NAC-compliant application.

Actions are the result of applying a policy to the credentials received in a posture-validation request. ACS determines the posture token of each request by comparing the actions from all policies applied to the request. The worst posture token becomes the system posture token.

URL Redirect Policy

The URL Redirect policy provides a mechanism to redirect all HTTP or HTTPS traffic to a remediation server that allows a noncompliant host to perform the necessary upgrade actions to become compliant. The policy comprises:

- A URL that points to the remediation server.
- An ACL on the switch that causes all HTTP or HTTPS packets from the host other than those destined to the remediation server address to be captured and redirected to the switch software for the necessary HTTP redirection.

The ACL name for the host policy, the redirect URL, and the URL redirect ACL are conveyed by using RADIUS Attribute-Value objects.

Fail Open for Errors

You can configure fail open for errors that can prevent the retrieval of posture token from an upstream NAC server. If fail open is not configured, the user request is rejected.

When fail open is configured, and an error occurs when communicating with an upstream posture-validation server, the policy results will be as if posture validation was successful. The SPT for the given policy will be a static, preconfigured value.

You can select whether to enable fail open for profiles that are associated with an:

- External Posture Validation Server— If more than one server is configured for a profile, each server that fails contributes an APT to the final SPT. The worst case token is used as the SPT, which symbolizes the overall posture of the NAC-client computer. See [Setting a Posture-Validation Policy, page 14-30](#).
- Audit Server— Configuring fail open results in the SPT being set to the statically configured posture token. See [Configuring Posture Validation for Agentless Hosts, page 14-33](#).

Setting a Posture-Validation Policy

A posture-validation policy can have one or more posture-validation rules. When ACS uses a posture-validation policy to evaluate a posture-validation request, the first match is implemented. The selected rules determine which internal and external policies will be activated for the request.

You can configure posture-validation policies that might be associated with a rule in Internal or External Posture Validation Setup, as applicable.

Before you begin:

- Ensure that you have checked the Allow Posture Validation option in Network Access Profiles > Authentication Settings page (see [Authentication for profile_name Page, page 14-46](#)).
- Ensure that you have set posture validation settings (see [Configuring NAC in ACS, page 13-13](#) for details).

To add an internal posture-validation policy, external posture-validation server, or both, to a profile:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the selected profile.
The Posture Validation page appears.
- Step 3** Click **Add Rule**.
The Posture Validation Rule Page appears. For details of options on this page, see [Posture Validation Rule for profile_name Page, page 14-48](#).
- Step 4** Enter a Name for the rule.
- Step 5** Configure the **Required Credential Types**.
- Step 6** Choose the Internal Posture Validation Policies and External Posture Validation Servers to be activated.
- Step 7** To configure fail open for a selected external posture validation server do one:
- Check **Reject User** to deny access for fail open.
 - In the Failure Posture Assessment field, select:
 - **Credential Type**—The namespace for the APT which replaces the APT that should have been returned from the failed server.
 - **Posture Token**—The posture token to be used in the event of a failure.
- Step 8** (Optional) Use the **System Posture Token Configuration** Table to set PA Messages and URL Redirects for the System Posture Token.
- Step 9** Click **Submit**. The Posture Validation page reappears.
- Step 10** In the Posture Validation page, click **Done**.
The Network Access Profiles page reappears.
- Step 11** Select **Apply and Restart** for your changes to take effect.
- Step 12** Click **Cancel** to return to the posture-validation policy.
-

Deleting a Posture Validation Rule

To delete an internal posture-validation policy rule:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the selected profile.
The Posture Validation page appears.
- Step 3** Click the rule name that you want to delete. The [Posture Validation Rule for profile_name Page](#) appears.
- Step 4** Click **Delete**.

A warning message appears.

Step 5 Click **OK**.

Setting a Posture-Validation Policy to Process Statements of Health

A posture-validation policy can have one or more posture-validation rules. When ACS uses a posture-validation policy to evaluate a posture-validation request, the first match is implemented. The chosen rules determine which internal and external policies will be activated for the request.

You can configure posture-validation policies that might be associated with a rule in Internal or External Posture Validation Setup, as applicable.

You can also set up a SoH posture validation rule.

Before you begin:

Ensure that you have:

- Checked the **Allow Posture Validation** option on the Authentication Settings page (see [Authentication for profile_name Page, page 14-46](#)).
- Set posture validation settings (see [Configuring NAC in ACS, page 13-13](#) for details).
- Checked the **Microsoft Network Access Protection Settings** check box on the Advanced Options page.

To add an SoH posture validation rule to a profile:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose **Posture Validation** for the selected profile.

The Posture Validation page appears.

Step 3 Click **Add Rule** under the Statement of Health Posture Validation Rules table.

The Statement of Health Posture Validation Rule page appears.

Step 4 Enter a Name for the rule.

Step 5 Configure the **Endpoint Location**.

Step 6 Choose which External Posture Validation Servers are to be activated.

Step 7 To configure ACS to reject a user if the Network Policy Server (NPS) is unable to finalize the Statement of Health for the client, check the **Reject User** check box.



Note The Reject User option works only if the NPS Server is unable to finalize the Statement of Health for the client.

Step 8 If you want to specify a token that will be used if the NPS Server is unable to finalize the Statement of Health for the client:

- Uncheck the **Reject User** check box.
- From the drop-down list in the Failure Posture Token field, choose a token type to assign.



Note Even if the user is not rejected, the NPS Server validates the Statement of Health and returns an appropriate token to ACS.

ACS uses the token that you specify for the Statement of Health Posture rule *only* if the NPS Server is unable to finalize the Statement of Health for the client. Therefore, the token that you choose here is a “fail-safe” token that is used only when the NPS Server cannot process the Statement of Health, and it is not mandatory that you choose one.

-
- Step 9** In the URL Redirect table, for each of the System Posture Token types, enter a URL for a server to which to redirect users.
- Step 10** Click **Submit**.
The Posture Validation page reappears.
- Step 11** In the Posture Validation page, click **Done**.
The Network Access Profiles page reappears.
- Step 12** Click **Apply and Restart** for your changes to take effect.
- Step 13** Click **Cancel** to return to the posture-validation policy.
-

Deleting a Statement of Health Posture Validation Rule

To delete an SoH posture validation rule:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the chosen profile.
The Posture Validation page appears.
- Step 3** Click the rule name that you want to delete. The Statement of Health Posture Validation Rule for profile_name page appears.
- Step 4** Click **Delete**.
A warning message appears.
- Step 5** Click **OK**.
-

Configuring Posture Validation for Agentless Hosts

Posture-validation rules define what the returned posture token for posture validation will be. The posture-validation table includes posture-validation rules and audit configuration settings.

Posture-validation rules contain:

- A required credential that defines the mandatory credential types that activate the rule.
- The local policies and external servers that will execute to calculate the posture token.
- PA (posture agent) Messages that will return to the client for each posture token.
- A URL redirect that will be sent to the AAA client for each posture token.

A posture-validation policy can have 0-*n* ordered posture rules.

The posture validation selected is the first that match of the mandatory credential types.

The posture token that will return is the worst assessment that returned from the selected local policies and external posture servers.

If the client is an agentless host, the selected Audit server will audit the client.

To configure a posture validation policy for a NAH:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the selected profile.
The Posture Validation Page appears.
- Step 3** Choose **Select Audit**.
The [Select External Posture Validation Audit for profile_name Page](#) appears.
- Step 4** Choose the relevant audit server. Select **Do Not Use Audit Server** if you do not want to use an audit server for posture validation.
- Step 5** To enable fail open:
- Check the **Do Not reject when Audit failed** check box.
 - Choose the **posture token** to be used in the event of a failure.
 - Enter a value for **session-timeout** for the audit server.
 - To assign a user group, check the **Assign a User Group** check box and choose a group from the drop-down list.
- Step 6** Click **Submit**.
- Step 7** Click **Apply and Restart** for your changes to take effect.
-

Authorization Policy Configuration for NAPs

These topics provide information on configuring authorization rules:

- [About Authorization Rules, page 14-34](#)
- [Configuring an Authorization Rule, page 14-36](#)
- [Configuring a Default Authorization Rule, page 14-37](#)
- [Ordering the Authorization Rules, page 14-37](#)
- [Deleting an Authorization Rule, page 14-38](#)
- [Troubleshooting Profiles, page 14-38](#)

About Authorization Rules

Authorization policies comprise rules that are applied to a NAP. Authorization policies are used for authorizing an authenticated user. Authorization rules can be based on group membership, posture validation, or both. Authorization actions are built from RACs and ACLs.

For more information about configuring RACs, see [RADIUS Authorization Components, page 4-6](#). For more information about downloadable ACLs, see [Downloadable IP ACLs, page 4-13](#).

Credentials are used in identity and posture authorization. Each application's posture credentials are evaluated separately. Credentials are compared against the posture-validation policies.

When you configure authorization policies consider the result if:

- User authentication is assignment to a User Group.
- Posture validation is a System Posture Token.
- EAP-FAST authentication and posture validation in the same session results in assignment to a user group and a posture token.

Authorization policies are a conversion of an ACS user group and a posture token to a set of RADIUS attributes that will be sent to the device. You may deny access for a specific user group, or deny access based on a returned token.

An authorization rule can be defined as:

If the user-group = selected-user-group or the posture-assessment = selected-posture-assessment, then provision the profile with the selected-RAC or the selected DACL.

Authorization rules allow for variation of device provisioning within the NAP based on group membership and posture token. The set of possible mappings is theoretically quite high for each NAP, for each group, and for each posture. However, in practice most users will be caught by a default case; for example, normal healthy users. Exceptions might be groups that require specialized access rights (for example, administrators) or users with Infected or Quarantined postures. Therefore, when you design the authorization rules, it is useful to define the normal condition first; then the set of exception cases that require more specific mappings.

You can also use authorization rules to explicitly deny (send an access-reject) as an action.

After you have configured your authorization rules, check that the Network Access Restriction (NAR) policies for the selected user group do not override the NAP policies. Accept or reject will be applied, depending on the result of the NAR evaluation. For more information, see [Network Access Restrictions, page 4-18](#).

Shared RACs

You can use NAPs to provision the same RADIUS attribute to have different values for different users, groups and NAPs. The one-user-one-group-one-profile is now more flexible by using profile based policies. For each NAP, you can configure what policies will authenticate and authorize based on RADIUS attribute values.

For a particular group (for example, Admins) who require distinct authorization profiles for the Corporate LAN, VPN, and WLAN NAPs, you can assign them a specific set of RADIUS attributes to allow them special access. If your user is in a group named contractors, they may get the same set of attributes with different values that may specify more stringent security measures. For more information about configuring RACs for NAPs, see [Understanding RACs and NAPs, page 4-7](#)

Merging Attributes

You can use RADIUS attribute overrides for group or user attributes. When you choose these options, ACS merges RADIUS attributes, downloadable ACLs, and other attributes that are created dynamically. RADIUS attributes can be at a user record level, group level and shared RAC level.

Attribute merging is performed by a process of repeated overriding whatever is listed in priority order, highest first. The order is:

- User overrides

- Dynamic session (for example, posture token)
- Authentication protocol (for example, session timeout, wireless session keys)
- Downloadable ACL (assignment)
- Shared RACs
- Static group

When you merge between group, RAC, and user attributes, remember that attributes set at a group level are not guaranteed to make the final profile. Depending on your selections, RAC might override them.

The attributes in the assigned Shared RAC override those that are defined in a static ACS group. That attribute set is then overridden with attributes from downloadable ACL and so on. Be cautious when you use NAP authorization policies.

Configuring an Authorization Rule

Before You Begin

Define per-service provisioning components (Shared RACs and DACLs). If required for a given service, create custom RACs and DACLS for those groups of users that require specific settings.

To configure an authorization rule:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the selected profile **Authorization** policy.

The Authorization Rule page appears.

Step 3 Click **Add Rule**.

A new rule row appears.

Step 4 Define the authorization rule conditions:

- Choose a **User Group** from the drop-down list.
- In a NAC network, choose the **System Posture Token**. (In a non-NAC network, leave the System Posture Token as **Any**.)

For more information about condition options, see [Authorization Rules for profile_name, page 14-50](#).

Step 5 Define the authorization rule actions:

You can deny access or you can choose one or both authorization actions to implement when the authorization rules match:

- **Deny Access**—Check this option to deny access for users that have matching conditions. When you choose this option the other action options are grayed out.
- **Shared RAC**—Choose a Shared RAC from the drop-down list.
- **Downloadable ACL**—Choose a downloadable ACL from the drop-down list.

For more information about action options, see [Authorization Rules for profile_name, page 14-50](#).

Step 6 Set RADIUS attribute overrides.

The following options are enabled by default. Uncheck them if you do not want to use RADIUS attributes per user record or per user's group:

- Include RADIUS attributes from user's group
- Include RADIUS attributes from user record

Step 7 Click **Submit**.

Related Topics

- [RADIUS Authorization Components, page 4-6](#)
- [Downloadable IP ACLs, page 4-13](#)

Configuring a Default Authorization Rule

You can set a default authorization rule if a condition is not defined or no matched condition is found. You can deny or grant access based on Shared RACs and DACLs selections.

To configure a default authorization rule:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the selected profile **Authorization** policy.
The [Authorization Rules for profile_name](#) appears.

Step 3 Click **Add Rule**.

Step 4 Select Authentication Action for the line that contains the text **If a condition is not defined or there is no matched condition**.

Step 5 Choose Authentication Actions.

You may choose an authorization action to implement for the default rule:

- **Deny Access**—Choose this option to deny access for users that have matching conditions. You do not have to select any shared RACs or DACLs for this option.
- **Shared RAC**—Choose a Shared RAC from the drop-down list. For more information, see [Troubleshooting Profiles, page 14-38](#).
- **Downloadable ACL**—Choose a downloadable ACL from the drop-down list. See [Downloadable IP ACLs, page 4-13](#) for more information.

Step 6 Set RADIUS attribute overrides.

The following options are enabled by default. Uncheck them if you do not want to use RADIUS attributes per user record or per user's group:

- Include RADIUS attributes from user's group
- Include RADIUS attributes from user record

Step 7 Click **Submit**.

Ordering the Authorization Rules

The authorization policy first match is implemented to authorize a client request.



Note

You must place your highest priority authorization policies at the top of the list. If you select Any Group for the User Group or Any Assessment for the posture token first match, the underlying policies will not be effective because authorization accepts the first match.

When you specify the order of conditions in a policy, determine the likelihood of each condition to be true and then order the policies so that the condition most likely to be true is first and the least likely to be true is last.

To order authorization rules:

-
- Step 1** In the Authorization Rules page, click the radio button to select the authorization rule that you want to reorder.
- Step 2** Click **Up** or **Down** to set the order.
-

Deleting an Authorization Rule

To delete an authorization rule:

-
- Step 1** In the Authorization Rules page, click the radio button to select the authorization rule that you want to delete.
- Step 2** Click **Delete** to remove the selected rule.
- By default, RADIUS attribute rules from user or group records are enabled.
-

Troubleshooting Profiles

If the profile that is sent to the device is not what you expected, the authorization policy has probably been changed to disable group or user attributes. These attributes are being merged with the RAC that the policy assigns. Other possibilities are that ACS automatically adds certain attributes as part of the authentication protocol or an external audit server might sometimes dictate a specific Session-Timeout.

Ensure that attribute merging is not selected.



Note

The Session-Timeout values for NAC deployments can have a significant impact on ACS performance. You should adjust it for the scale of your network and ACS transaction capacity.

Policy Replication and Backup

All NAP policies are entirely replicated when you select NAPs for replication. Profiles contain a collaboration of configuration settings. The profile replication components include:

- Network Access Profiles
- Posture-validation settings
- AAA clients and hosts
- External database configuration
- Global authentication configuration
- NDGs
- Dictionaries

- Shared-profile components (RAC, NAF, and downloadable ACLs)
- Additional logging attributes.

EAP-FAST uses a different mechanism for replication and, therefore, should also be checked.

**Note**

Replication of profiles contradicts with replication of Network Configuration Device tables, therefore do not check both of these components at the same time. Replication in ACS only works between the same versions of ACS. Replication does not include external databases and all other global ACS configuration parameters.

For more information about replication, see [ACS Internal Database Replication, page 8-1](#).

Network Access Profiles Pages Reference

These topics describe the pages in the Network Access Profile section of the ACS web interface:

- [Network Access Profiles Page, page 14-39](#)
- [Profile Setup Page, page 14-40](#)
- [Create Profile from Template Page, page 14-43](#)
- [Protocols Settings for profile_name Page, page 14-43](#)
- [Authentication for profile_name Page, page 14-46](#)
- [Posture Validation Page, page 14-48](#)
- [Posture Validation Rule for profile_name Page, page 14-48](#)
- [Authorization Rules for profile_name, page 14-50](#)
- [Select External Posture Validation Audit for profile_name Page, page 14-49](#)

Network Access Profiles Page

The Network Access Profiles page is the starting point for configuring profile-based policies.

To open this page, click **Network Access Profiles on the navigation bar**.

Table 14-20 Network Access Profiles Page

Option	Description
Name	Activates the configuration for the profile. Opens the Profile Setup Page .
Policies	Contains links to protocols, authentication, posture validation, and authorization policies. <ul style="list-style-type: none"> • Protocols—Configures the password protocols and EAP configuration. Opens the Protocols Settings for profile_name Page page. • Authentication—Controls the profile's authentication policy. Opens the Authentication for profile_name Page where you can select the database that is used to validate user credentials. • Posture Validation—Configures posture-validation policies. Opens the Deleting a Posture Validation Rule. • Authorization—Maps between a user-group and system posture token result, to a radius-profile tag and Access Control List (ACL) name. Opens the Configuring a Default Authorization Rule.
Add Profile	Opens the Profile Setup Page to configure NAPs.
Add Template Profile	Creates a profile from a selection of templates including NAC L3 IP, NAC L2 IP, and Agentless Host. Use the templates to facilitate the construction of a profile. Opens the Create Profile from Template Page .
Up and Down buttons	Changes the order of the profiles. Click the Up or Down buttons to change the sort order.
Deny access when no profile matches	When enabled, and the access request does not match any profile, authentication fails and ACS denies the access request. This is the recommended option for handling unmatched access requests.
Grant access using global configuration, when no profile matches	When enabled, and the access request does not match any profile, authentication fails and ACS grants the access request based on the default configuration. The Unknown User policy then determines packet processing. Use this option for TACACS+ with NAPs.
Apply and Restart	Restarts ACS and applies the modifications.

Related Topics

- [Managing NAPs, page 14-4](#)
- [Using Profile Templates, page 14-7](#)

Profile Setup Page

Use this page to add, edit, clone, or delete a Network Access Profile.

To open this page, choose **Network Access Profiles > Add Profile** or **highlight the profile Name**.

Table 14-21 Profile Setup Page

Option	Description
Name	The profile name.
Description	The profile description.
Active	Activates or deactivates the profile.
Network Access Filter	The list of available NAFS for use with this profile (Default = Any).
Protocol Types	The list of client vendor types from which ACS allows access requests. <ul style="list-style-type: none"> • Allow Any Protocol Type—Allows any protocol type in the Protocol type list. • Allow Selected Protocol Types—Use only the protocol type(s) in the Selected list. The arrows to move the Protocol Types between lists.
Advanced Filtering	
Attribute	<p>A list of all RADIUS attributes. A number uniquely identifies each RADIUS attribute; for example, 001 is the number for <code>User-Name</code>, except for vendor-specific attributes. Vendor Specific Attributes (VSAs) use the number 026 as an identifier. The format is:</p> <p><i>Cisco AV-pair 026 / <vendor type> / <vendor attribute></i></p> <p>For example, 026/009/001 is a Cisco AV-pair attribute.</p> <p>Note ACS supports Cisco IOS RADIUS AV pairs. Before you select an AV pair, confirm that your AAA client supports it. The condition always fails for an AV pair that the AAA client does not support.</p>

Table 14-21 Profile Setup Page (continued)

Option	Description
Operator	<p>The list of operators appropriate to each attribute. Defines the comparison method by which ACS evaluates whether the rule element is true.</p> <ul style="list-style-type: none"> • = (equal to)—The rule element is true if the value in the attribute is exactly equal to the value that you specify. • != (not equal to)—The rule element is true if the value in the attribute does not equal the value that you specify. • > (greater than)—The rule element is true if the value in the attribute is greater than the value that you specify. • < (less than)—The rule element is true if the value in the attribute is less than the value that you specify. • <= (less than or equal to)—The rule element is true if the value in the attribute is less than or equal to the value that you specify. • >= (greater than or equal to)—The rule element is true if the value in the attribute is greater than or equal to the value that you specify. • contains—The rule element is true if the attribute contains a string and if any part of that string matches the string that you specify. • starts with—The rule element is true if the attribute contains a string and if the beginning of that string matches the string that you specify. • regular expression—The rule element is true if the attribute contains a string that matches the regular expression that you specify. ACS supports the following regular expression operators: <ul style="list-style-type: none"> – ^ (caret)—The ^ operator matches the start of a string. – \$ (dollar)—The \$ operator matches the end of a string. – * (asterisk)—The * operator matches zero or more of the preceding expression. – + (plus)—The + operator matches one or more of the preceding expression. – ? (question mark)—The ? operator matches either zero or one of the preceding expression. – a-z (dash)—The - operator matches a range of characters or numbers from a to z. – . (period)—The . operator matches any character. – \ (backslash)—The \ operator matches characters that would otherwise be interrupted as a regular expression operator. – (pipe)—The operator signifies a logical or that is often used in character sets. – [] (square brackets)—The [] operator denotes a set of allowed characters to use in matching such as [a-zA-Z0-9] for alphanumeric characters. – () (dollar)—The () matches a subexpression group. <p>Note Operators contains, start with, and regular expression only apply to string-type attribute values.</p>

Table 14-21 Profile Setup Page (continued)

Option	Description
Value	A value appropriate to the attribute.
cisco-av-pair	For the {026/009/001} cisco-av-pair attribute, the operator and values for the av-pair-key and av-pair-value.
Submit	Submits modifications. Returns to the Profile Setup Page .
Clone	Creates a copy of the NAP.
Delete	Deletes a profile, after warning.
Cancel	Returns to the Profile Setup Page without implementing changes.

Related Topics

- [Network Access Filters, page 4-2](#).
- [Managing NAPs, page 14-4](#)
- [Cloning a Profile, page 14-6](#)

Create Profile from Template Page

Use to this page to create a new profile from a template.

To open this page, choose **Network Access Profiles > Add Profile from Template**.

Table 14-22 Create Profile from Template Page

Option	Description
Name	A name for the profile.
Description	A description for the profile.
Template	The list of available templates. Note The NAC L3 IP template requires the Allow Posture Validation setting on the Protocols Settings for profile_name Page .
Active	Activates or deactivates the profile.
Submit	Submits modifications. Returns to the Profile Setup Page .
Cancel	Returns to the Profile Setup Page without implementing changes.

Related Topics

[Using Profile Templates, page 14-7](#)

Protocols Settings for *profile_name* Page

Use this page to set password protocols and EAP configuration.

To open this page, choose **Network Access Profiles > Protocols** (appears for each profile).

Table 14-23 Protocols and EAP Configuration Page

Option	Description
Populate from Global	Populates the Protocol Settings with the ACS Global Authentication settings. This method facilitates configuration of the authentication settings for new profiles.
Authentication Protocols	
Allow PAP	Enables PAP. PAP uses clear-text passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	Enables CHAP. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with the Windows user database.
Allow MS-CHAPv1	Enables MS-CHAPv1.
Allow MS-CHAPv2	Enables MS-CHAPv2.
Allow Agentless Request Processing	Enable to configure the authentication process for a profile that receives a MAC address request.
EAP Configuration	
Allow RADIUS Key Wrap	Enables RADIUS Key Wrap attributes in PEAP, EAP-FAST and EAP-TLS authentication.
PEAP	<p>The PEAP types. Check at least one box to enable authentication with PEAP. In most cases, check all boxes.</p> <p>Note PEAP is a certificate-based authentication protocol. Authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.</p> <ul style="list-style-type: none"> • Allow EAP-MSCHAPv2—Enables EAP-MS-CHAPv2 within PEAP authentication. Use for AD authentication. • Allow EAP-GTC—Enables EAP-GTC within PEAP authentication. Use for RSA Secure ID authentication. • Allow Posture validation—Enables the collection of posture data when using PEAP. This option uses EAP over UDP. Allow Posture Validation must be checked to use the NAC L3 IP Profile Template on the Create Profile from Template Page. • Allow EAP TLS—Enables EAP-TLS within PEAP authentication.
EAP FAST	
Allow EAP-FAST	Enables EAP-FAST authentication. All other EAP-FAST-related options are irrelevant if unchecked. Some of the following settings must have corresponding settings on the PC based authentication agent (the EAP-FAST client).
Use PACS	Check if you want ACS to provision authorization PACs for EAP-FAST clients. All the relevant PAC options are disabled if this option is not checked.
Allow anonymous in-band PAC provisioning	If this check box is checked, ACS establishes a secure anonymous TLS handshake with the client to provision it with a so-called PAC by using phase zero of EAP-FAST, and using EAP-MS-CHAP as the inner method.
Allow full TLS renegotiation in case of Invalid PAC	Check if you want ACS to allow a full TLS renegotiation when the client is attempting to authenticate by using an invalid PAC.

Table 14-23 Protocols and EAP Configuration Page

Option	Description
Allow anonymous in-band PAC provisioning	Check if you want ACS to establish a secure anonymous TLS handshake with the client, to provision it with a so-called PAC, by using phase zero of EAP-FAST, and by using EAP-MSCHAP as the inner method.
Enable anonymous TLS renegotiation	This option allows an anonymous TLS handshake between the end-user client and ACS. EAP-MS-CHAP will be used as the only inner method in phase zero.
Allow authenticated in-band PAC provisioning	<p>ACS uses secure sockets layer (SSL) server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning; but requires that a server certificate and a trusted root CA are installed on ACS.</p> <ul style="list-style-type: none"> • Accept client on authenticated provisioning—Enable to slightly shorten the protocol. • Require client certificate for provisioning—Enable if the clients are configured with public key infrastructure (PKI) certificates.
Allow Stateless session resume	<p>When enabled, ACS provisions authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled).</p> <ul style="list-style-type: none"> • Authorization PAC TTL <number> <timeframe>—Determines the expiration time of the user authorization PAC. When ACS receives an expired authorization PAC, it performs phase two EAP-FAST authentication.
When receiving client certificate, select one of the following lookup methods	<p>Certificate SAN Lookup—Choose to lookup the certificate based on the Subject Alternative Name field in the client certificate.</p> <p>Certificate CN Lookup—Choose to look up the certificate base on the Common Name field in the client certificate.</p>
Do not use PACs	<p>When enabled, determines whether ACS runs EAP-FAST but does not issue or accept any tunnel or machine PACs. All requests for PACs are ignored and ACS responds with a Success-TLV without a PAC. All the relevant PAC options are disabled if this option is not checked.</p> <ul style="list-style-type: none"> • Requires Client Certificate—Select to support EAP-FAST tunnel establishment with a client certificate. • Disable Client Certificate Lookup and Comparisons —Select to disable the client certificate lookup and whether the clients are configured with public key infrastructure (PKI) certificates. When this option is enabled, EAP-FAST PKI Authorization Bypass is invoked. Authorization is generally performed by retrieving the user’s group data and certificate from an external database. ACS then compares at least one of the certificate, CN, or SAN to the values received from the client supplied certificate. If the comparison succeeds the group is mapped to an ACS user-group, otherwise the authentication fails. When PKI Authorization Bypass is enabled this stage is passed over and the session is mapped to a pre-configured user-group. See PAC Free EAP-FAST, page 9-16 for more information. • Assign Group — Select a group to map these requests to an ACS user-group.

Table 14-23 Protocols and EAP Configuration Page

Option	Description
Allowed inner methods	<p>When enabled, determines which inner EAP methods run inside the EAP-FAST tunnel. For anonymous in-band provisioning, EAP-GTC and EAP-MS-CHAPv2 must be enabled for backward compatibility. In most cases, all the inner methods should be checked.</p> <p>Note ACS always starts the authentication process by using the first enabled EAP method. For example, if you select EAP-GTC and EAP-MS-CHAPv2, then the first enabled EAP method is EAP-GTC.</p> <ul style="list-style-type: none"> • EAP-GTC—Uses a two-factor authentication; for example, OTP. • EAP-MSCHAPv2—Used for AD authentication. • EAP-TLS—Uses certificates for authentication.
Posture Validation	<p>Determines the EAP-FAST posture-validation mode. Select one of the following posture-validation modes:</p> <ul style="list-style-type: none"> • None—Authentication is performed; however, no posture-validation data is requested from the client and no SPT is returned. • Required—Authentication and posture validation are performed in the same authentication session. As a result, an SPT is returned. If this option is selected and posture credentials that are requested from the client are not received, authentication fails. If you are implementing NAC, this option should be enabled. • Optional—Client may not supply posture data. Sets a default SPT when a client cannot supply posture data to ACS. • Use Token—Select an SPT from the drop-down list to use as the default posture token. • Posture Only—Perform posture validation without running authentication inner methods within the authentication session. This option returns an SPT for posture validation.
EAP-TLS	<p>Enables EAP-TLS authentication.</p> <p>EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.</p> <ul style="list-style-type: none"> • Allow EAP-TLS—Check to enable EAP-TLS authentication.
EAP-MD5	Enables EAP-based Message Digest 5 hashed authentication.

Related Topics

[Protocol Configuration for NAPs, page 14-23](#)

Authentication for *profile_name* Page

Use this page to specify the databases that the profile uses for authentication rules, and to set up the Agentless Request Processing for MAC addresses configuration.

To display this page, choose **Network Access Profiles > Authentication** (appears for each profile).

Table 14-24 Authentication Settings Page

Option	Description
Credential Validation Databases	The lists of Available Databases and Selected Databases that can validate users. The lists of databases include the ACS Internal Database and all databases configured in External User Databases > Unknown User Policy . If the Unknown User Policy configures a database to fail, the database cannot become a validation database and fails with an error message.
Populate from Global	Populates the Authentication Settings from the System Configuration > Global Authentication Setup page. Facilitates configuration of the authentication settings.
Group Filtering	Use this option to configure group filtering based on groups defined in the LDAP external database.
Available Groups/Selected Groups	The list of Available Groups and Selected Groups that can validate users. The lists of groups include the groups configured in LDAP External User Databases configuration. Use the arrows to move the Available Groups into the Selected Groups list.
Authenticate MAC With	<p>ACS can authenticate MAC addresses with an LDAP server or the ACS Internal Database.</p> <p>ACS supports the following three standard formats for representing MAC-48 addresses in human-readable form:</p> <ul style="list-style-type: none"> • Six groups of two hexadecimal digits, separated by hyphens (-) in transmission order, for example, <i>01-23-45-67-89-ab</i>. • Six groups of two separated by colons (:), for example, <i>01:23:45:67:89:ab</i>. • Three groups of four hexadecimal digits separated by dots (.), for example, <i>0123.4567.89ab</i>.
LDAP Server	<p>If chosen, configures an LDAP server from the available servers on the External User Databases > External User Database Configuration page.</p> <p>ACS uses the LDAP server to look up MAC addresses and to retrieve LDAP group attributes for MAC addresses. If the MAC addresses exist in the LDAP Server, ACS maps the LDAP Group to the ACS Groups configured in the configured ACS External LDAP Database.</p>
Internal ACS Database	<p>If chosen, provides fields for MAC Addresses, each with an associated User Group.</p> <p>Each NAP can hold up to 10,000 MAC addresses in the Authentication page. Each NAP can hold up to 100 mappings (a map between list of one or more MAC addresses to a group), meaning you can have up to 100 lines of mappings from lists of MACs to user-groups. You can map up to 10,000 MAC Addresses to the same user-group in one NAP.</p>
Default Action (If Agentless request was not assigned to a user group)	If the MAC addresses were not found in the LDAP Server or the ACS Internal Database, or if the LDAP Server is not reachable, provides a group to which to assign the MAC addresses.
OID Comparison	Compare Object ID with the Enhanced Key Usage (EKU) field in the user's certificate.
Enter OIDs separated by comma	OID strings can only contain numbers, dots (.), commas(,) and spaces. Multiple OIDs can be entered as comma-separated values.

Table 14-24 Authentication Settings Page

Option	Description
Submit	Submits changes to the ACS internal database.
Cancel	Returns to the Network Access Profiles Page without submitting new changes.

Related Topics

- [Authentication Policy Configuration for NAPs, page 14-27](#)

Posture Validation Page

Use this page to order and associate Posture Validation rules.

To display this page, click **Posture Validation** in the [Network Access Profiles Page, page 14-39](#).

Table 14-25 Posture Validation Page for profile_name Page

Field	Description
Posture Validation Rules	
Rule Name	The name of the posture-validation rule.
Required Credential Types	The Available Credentials list displays the credential types that ACS does not require. The Selected Credentials list displays the credential types that ACS requires in a posture-validation request in order to use this posture-validation rule to evaluate the posture-validation request.
Associate With	The policies that are associated with a rule.
Up/Down	Sets the order of evaluation.
Add Rule	Opens the Posture Validation Rule for profile_name Page on which you create a new posture-validation rule.
Select Audit	Opens the Select External Posture Validation Audit for profile_name Page to configure an audit server for NAC. NAC-compliant AAA clients can handle NAC for computers that do not respond to attempts to start a posture-validation session with the Cisco Trust Agent by querying an audit server. If the Cisco Trust Agent is not installed on the computer or is unreachable for other reasons, NAC-compliant AAA clients will attempt to perform posture validation on an audit server. The result that an audit server returns is a posture token.

Related Topics

- [Chapter 13, “Posture Validation”](#)
- [Setting a Posture-Validation Policy, page 14-30](#)

Posture Validation Rule for profile_name Page

Use this page to define a Posture Validation rule.

To display this page, click **Add Rule** in the [Posture Validation Page, page 14-48](#).

Table 14-26 Posture Validation Rule for *profile_name* Page

Field	Description
Rule Name	Displays the rule name for identification.
Add Rule	Click to add a posture-validation rule. The Posture Validation Rule configuration page appears.
Edit Rule	Highlight the Rule Name. The Posture Validation Rule configuration page for the specific profile appears for editing.
Action	
Select Internal Posture Validation Policies	Select the internal posture validation policies that ACS will apply to the attributes received in the request for this rule.
Select External Posture Validation Server	Select the external posture validation server policies that ACS will apply to the attributes received in the request for this rule.
Failure Action	Check to configure the Fail Open feature.
Failure Posture Token	Select the credential type (AV pair) that is returned to the supplicant. Select the Posture Token for the credential type.
System Posture Token Configuration	Use this table to configure the SPT to return to the AAA client. There are six predefined, nonconfigurable SPTs. The SPT results are listed in order from best to worst: <ul style="list-style-type: none"> • System Posture Token—A Posture Agent Message and URL Redirect for each posture token. • System Posture Token—A message that will appear for each posture agent. • URL Redirect—The URL redirect that will be sent to the AAA client for each posture token.

Related Topics

- [Setting Up Posture Validation Policies, page 13-16](#)
- [Setting Up an External Policy Server, page 13-22](#)
- [Setting a Posture-Validation Policy, page 14-30](#)

Select External Posture Validation Audit for *profile_name* Page

Use this page to select an external posture validation audit server for posture validation.

To display this page, click **Select Audit** in the [Posture Validation Page, page 14-48](#).

Field	Description
Select	Select the external posture-validation audit server or select Do Not Use Audit Server .
Fail Open Configuration	Determines treatment of errors that might occur, thereby preventing the retrieval of a posture token from an upstream NAC server. If fail open is not configured, ACS rejects the user request.
Do not reject when Audit failed	Enables or disables fail open (default = enabled). <ul style="list-style-type: none"> • Use this token when unable to retrieve posture data—An appropriate token. • Timeout—The timeout value for the session. • Assign a User Group—The destination user group.

Related Topics

- [Setting Up an External Audit Posture Validation Server, page 13-25](#)
- [Configuring Posture Validation for Agentless Hosts, page 14-33](#)

Authorization Rules for *profile_name*

Use this page to list the set of authorization rules for a Network Access Profile.

To display this page, click **Authorization** in the [Network Access Profiles Page, page 14-39](#).

Table 14-27 *Authorization Rules for profile_name*

Field	Description
Condition	
User Group	The ACS group to which the user was mapped. This field defines the group of users for this rule. If you are not basing authorization rules on authentication, select Any .
System Posture Token	The posture token that was returned as a result of posture validation. ACS checks the token status before proceeding to follow the configured actions. You can use posture tokens to validate user groups. If you are not using posture validation, select Any .
Action	
Deny Access	Denies access for requests that do not match any configured policy.
Shared RAC	The list of RACs defined in the Shared Profile Components > RADIUS Authorization Components option. Note If you configure an external posture validation audit server to use session-timeout settings in the Authorization policy, you must select a shared RAC. See Configuring Policies, page 13-15 and External Posture Validation Audit Setup Pages, page 13-36 .
Downloadable ACL	The list of downloadable ACLs defined in Shared Profile Components > Downloadable IP ACLs.
If a condition is not defined or there is no matched condition:	A default action when a matched condition is not found.
Include RADIUS attributes from user's group	Enable to use RADIUS attributes per user's group.
Include RADIUS attributes from user record	Enable to use RADIUS attributes per user record.

Related Topics

- [Configuring an Authorization Rule, page 14-36](#)
- [Configuring a Default Authorization Rule, page 14-37](#)