



## Posture Validation

---

This chapter contains the following topics:

- [What is Posture Validation?, page 14-1](#)
- [Network Access Control Overview, page 14-1](#)
- [Posture Validation in ACS, page 14-4](#)
- [Configuring Policies, page 14-17](#) (including internal, external, and audit server)
- [How Posture Validation Fits into Profile-Based Policies, page 14-27](#)

### What is Posture Validation?

The term *posture* is used to refer to the collection of attributes that play a role in the conduct and “health” of the endpoint device that is seeking access to the network. Some of these attributes relate to the endpoint device-type and operating system; other attributes belong to various security applications that might be present on the endpoint, such as antivirus (AV) scanning software.

Posture validation, or posture assessment, refers to the act of applying a set of rules to the posture data to provide an assessment (posture token) of the level of trust that you can place in that endpoint. The posture token is one of the conditions in the authorization rules for network access. Posture validation, together with the traditional user authentication, provides a complete security assessment of the endpoint device and the user.

Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, supports posture validation when ACS is deployed as part of a broad Cisco Network Access Control (NAC) solution.

### Network Access Control Overview

NAC is a set of technologies and solutions built on an industry initiative led by Cisco Systems. It uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources; thereby limiting damage from emerging security threats. Customers using NAC can allow network access only to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can restrict the access of noncompliant devices.

This section contains the following topics:

- [Benefits of NAC, page 14-2](#)
- [NAC Architecture Overview, page 14-2](#)

- [Posture Tokens](#), page 14-3

For more information about the NAC solution, see <http://www.cisco.com/go/nac>

## Benefits of NAC

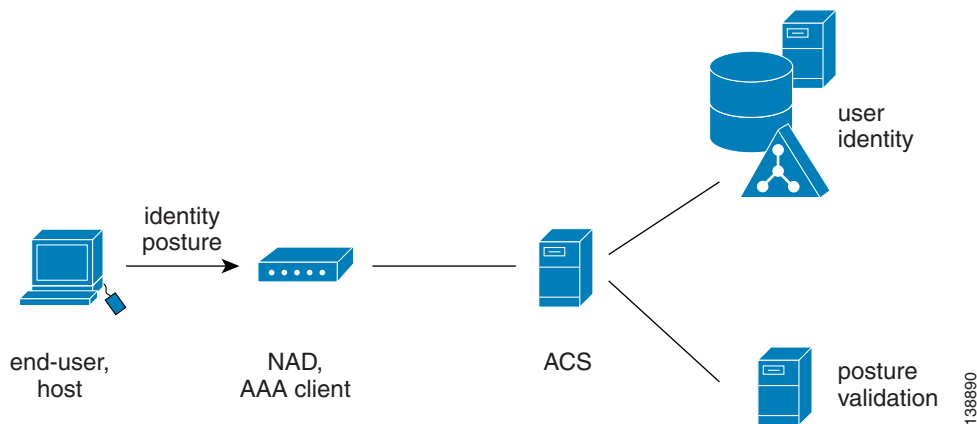
NAC:

- **Dramatically improves any network’s security**—NAC ensures that all endpoints conform to the latest security policy; regardless of the size or complexity of the network. With NAC in place, you can focus operations on prevention, rather than on reaction. As a result, you can proactively protect against worms, viruses, spyware, and malicious software before they are introduced into your network.
- **Extends the value of your existing investments**—Besides being integrated into the Cisco network infrastructure, NAC enjoys broad integration with antivirus, security, and management solutions from dozens of leading manufacturers.
- **NAC provides deployment scalability and comprehensive span of control**—NAC provides admission control across all access methods (LAN, WAN, wireless, and remote access).
- **Increases enterprise resilience**—NAC prevents noncompliant and rogue endpoints from affecting network availability.
- **Reduces operational expenses**—NAC reduces the expense of identifying and repairing noncompliant, rogue, and infected systems.

## NAC Architecture Overview

Figure 14-1 shows the components of a typical NAC deployment.

**Figure 14-1** Components of a Typical NAC Deployment



Typical NAC components are:

- **End-user or host**—Also known as the endpoint. The endpoint is a device such as a PC, workstation or server that is connected to a switch, access point, or router through a direct connection. In a NAC deployment, the host that is running the Cisco Trust Agent (CTA) application, collects posture data from the computer and from any NAC-compliant applications that are installed on the computer. For more information about posture credentials, see [Posture Validation Attribute Data Types](#), page 14-8.

Examples of NAC-compliant applications are the Cisco Security Agent and anti-virus programs from Network Associates, Symantec, or Trend Micro. These applications provide CTA with attributes about themselves, such as the version number of a virus definition file.

A NAC agentless host (NAH) is an endpoint that is not running the Cisco CTA application.

- **Network Access device (NAD)**—In a NAC deployment the AAA client is called a NAD. The NAD is a Cisco network access device, such as a router or switch, which acts as a NAC enforcement point.
- **ACS**—ACS performs the validation of the endpoint device by using internal policies, external policy servers, or both, to which the posture credentials are forwarded.
- **External posture validation servers**—These perform posture validation and return a posture token to ACS. In a NAC deployment with agentless hosts, you can configure ACS to invoke the services of a special type of posture validation server, called an audit server. An audit server uses out-of-bound methods, such as port scans, to validate the health of the endpoint device, and reports the result as a posture token to ACS.
- **Remediation servers**—Provide repair and upgrade services to hosts that do not comply with network admission requirements.

## Posture Tokens

Posture tokens represent the state of an endpoint device or a NAC-compliant application that is installed on the computer. A token that is associated with the state of the computer is a system posture token (SPT). A token that is associated with the state of a NAC-compliant application is an application posture token (APT).

APTs are the result of applying a policy to the credentials that are received in a posture-validation request. ACS determines the SPT of each request by comparing the APTs from all policies that are applied to the request. The most severe APT becomes the SPT.

[Table 14-1](#) describes the six predefined, non-configurable posture tokens, used for system and application posture tokens. They are listed in order from least to most severe.

**Table 14-1 ACS Posture Tokens**

Token	Description
Healthy	The endpoint device complies with the currently required credentials so you do not have to restrict this device.
Checkup	The endpoint device is within the policy but does not have the latest security software; update recommended. Use to proactively remediate a host to the <code>Healthy</code> state.
Transition	The endpoint device is in the process of having its posture checked and is given interim access pending a result from a full posture validation. Applicable during host boot where all services may not be running or while audit results are not yet available.
Quarantine	The endpoint device is out of policy and needs to be restricted to a remediation network. The device is not actively placing a threat on other hosts; but is susceptible to attack or infection and should be updated as soon as possible.
Infected	The endpoint device is an active threat to other hosts; network access should be severely restricted and placed into remediation or totally denied all network access.
Unknown	The posture credentials of the endpoint device cannot be determined. Quarantine the host and audit, or remediate until a definitive posture can be determined.

From the perspective of ACS, the actions that you set in your authorization rule determine the meaning of an SPTe. These actions associate a token with RADIUS authorization components (RACs), DACLs, or both. The authorization rule may also specify a user group as part of the condition. For details on configuring RACs, see [Adding RADIUS Authorization Components, page 5-9](#). For details on setting up your authorization rules as part of network access profiles, see [Setting Up a Profile, page 15-3](#).

Posture validation requests resulting in an SPT for which access is not strictly denied are logged in the Passed Authentications log. Posture validation requests resulting in an SPT for which access is denied are logged in the Failed Attempts log. For more information on logging and reports, see [Posture-Validation Attributes in Logs, page 11-3](#).

ACS only uses APTs to determine the SPT; but the endpoint device receiving the results of the posture validation can use them based on their meanings to the relevant NAC-compliant application.

## Posture Validation in ACS

This section provides overview information on posture validation and NAC support in ACS.

- [Configuring NAC in ACS, page 14-4](#)
- [Posture Validation Process, page 14-6](#)
- [Policy Overview, page 14-7](#)
- [Internal Policies, page 14-9](#)
- [External Policies, page 14-11](#)
- [NAH Policies, page 14-14](#)

## Configuring NAC in ACS

This section provides an overview of the steps to configure posture validation in ACS, with references to more detailed procedures for each step.



### Note

---

Design your posture policies by using the Posture Validation tab and then assign those policies to profiles by using the Posture Validation link inside the Network Access Profiles tab.

---

### Before You Begin

Before ACS can perform posture validation, you must complete several configuration steps. An overview of the steps follows. For information on finding detailed instructions on Cisco.com, see [Network Access Control Overview, page 14-1](#).

To implement posture validation:

- 
- Step 1** Install a server certificate. ACS requires a server certificate for NAC because an EAP tunnel protects NAC communication with an end-user client. You can use a certificate that is acquired from a third-party certificate authority (CA) or you can use a self-signed certificate.

For detailed steps about installing a server certificate, see [Installing an ACS Server Certificate, page 10-26](#). For detailed steps about generating and installing a self-signed certificate, see [Generating a Self-Signed Certificate, page 10-35](#).

**Note**

If you use a self-signed certificate, you may need to export the certificate from ACS and import it as a trusted root CA certificate into local storage on the endpoint computers.

**Step 2** For posture credentials from a third-party vendor, you must import the corresponding NAC attribute definition file (ADF). For detailed steps on importing and ADF, see [Import Vendor Attribute-Value Pairs \(AVPs\), page 15-36](#).

**Step 3** To set up external policies or use external policy audit servers, you should plan on configuring ACS to communicate with the external server over HTTPS; although ACS also supports HTTP communication. ACS authenticates the audit servers and posture validation servers by using certificates. You must choose the certificate from ACS or configure the Certificate Trust List (CTL). If the external servers use a different CA than the CA that issued the ACS server certificate, then you must configure the CTL. For detailed steps, see [Editing the Certificate Trust List, page 10-28](#).

If your external server uses a self-signed certificate, you do not need to alter the CTL.

**Tip**

You must add your audit vendor to the ACS internal dictionary by using the `CSUtil.exe` command before you can configure an external posture validation audit server. For detailed instructions, see [Importing External Audit Posture-Validation Servers, page D-33](#).

**Step 4** Enable the Passed Authentications log. ACS uses this log to log all posture validation credentials whenever access is not strictly denied. If the requests were denied, then ACS logs the results in the Failed Attempts log. When you enable the Passed Authentications log, be sure to move NAC-related attributes to the Logged Attributes column on the Passed Authentications File Configuration page.

For detailed steps about configuring this type of log, see [Configuring a CSV Log, page 11-14](#).

**Step 5** Configure the Failed Attempts log to include NAC attributes. Posture validation requests that were denied are logged to the Failed Attempts log. Including NAC attributes in this log can help you debug errors in your NAC implementation. For example, if none of the posture validation rules is matched, the request is logged here. Using the Failed Attempts log, you can see the contents of the attributes that are received in the request from the endpoint and sent in the reply to the endpoint.

For detailed steps about configuring this type of log, see [Configuring a CSV Log, page 11-14](#).

**Step 6** On the Global Authentication Setup page, enable posture validation by selecting **Allow Posture Validation** under EAP. Complete the steps for layer 2 or layer 3 support.

For detailed steps, see [Configuring Authentication Options, page 10-19](#).

**Step 7** If you have not already configured the AAA clients supporting NAC in the Network Configuration section, do so now.

For detailed steps, see [Adding AAA Clients, page 4-11](#).

**Step 8** From **Network Access Profiles**, set up the user groups that you want to use for posture validation. You are likely to want a separate user group for each possible SPT; therefore, select six user groups. If possible, choose groups that have not been configured to authorize users. Additionally, consider using groups that are widely separated from groups that authorize users. For example, assuming that the lowest numbered groups have been used for user authorization, consider using groups 494 through 499.

**Step 9** For detailed steps on setting up profiles, see [Setting Up a Profile, page 15-3](#).

**Tip**

To avoid confusion between groups that are intended to authorize users and groups that are intended to authorize endpoints, consider renaming the groups with an easily understood name. For example, if you selected group 499 to contain authorizations that are related to the Unknown SPT, you could rename the group **NAC Unknown**. For detailed steps, see [Renaming a User Group, page 6-40](#).

- Step 10** For each posture validation rule, assign a posture token and an SPT, which you can later associate with a profile that contains downloadable IP ACL sets and/or RACs that limit network access appropriately. For detailed steps on creating rules, see [Creating an Internal Policy, page 14-18](#). For detailed steps, see [Adding a Downloadable IP ACL, page 5-15](#) (and [Adding RADIUS Authorization Components, page 5-9](#).) To associate posture rules to profiles, see [Setting Up a Profile, page 15-3](#).
- Step 11** For each profile, you can create several different posture validation policies that contain any number of rules to validate your endpoint device. You can:
- a. Create a policy and its associated rules, including configuring mandatory credential types and policies.  
For detailed steps, see [Configuring Policies, page 14-17](#).
  - b. Use **Network Access Profiles** to assign posture validation policies to profiles to validate your endpoint devices.  
For detailed steps, see [Setting Up a Profile, page 15-3](#).

## Posture Validation Process

ACS evaluates the posture attributes received from an endpoint computer. The following overview describes the steps and systems involved in posture validation. Details about various concepts, such as posture tokens and policies, are provided in topics that follow.

1. Following a network event (for example, **EoLAN Hello=802.1** or traffic captured by the EoU ACL on the NAD), the NAD initiates an EAP conversation with the endpoint and forwards EAP messages from the endpoint to ACS.
2. ACS establishes a secure conversation with the host by using PEAP or EAP-FAST (depending on the ACS configuration and endpoint support).
3. (EAP-FAST only and optional) ACS authenticates the end user.
4. ACS queries the endpoint for posture attributes. In response, the endpoint sends posture attributes to ACS.
5. ACS performs the evaluation of the posture attributes internally and/or uses external posture validation servers. The evaluation results in a set of application posture tokens (APTs). ACS then evaluates the system posture token (SPT) by using the most severe APT.
6. Based on authorization rules that you set in Network Access Profiles, ACS sends the endpoint computer the system posture token and the results of each policy that is applied to the posture validation request, and then ends the EAP session. Based on the evaluation that ACS grants the client network access based on access limitations; or the noncompliant device can be denied access, placed in a quarantined network segment, or given restricted access to computing resources.

You can set up many types of restrictions in authorization rules by using various RADIUS attributes in the RAC (which might be combined with the user's group), downloadable ACL, and url-redirect or status-query-timeout.

7. ACS sends the AAA client the RADIUS attributes as configured in the shared RAC, including ACLs and attribute-value pairs that are configured in the Cisco IOS/PIX 6.0 RADIUS attribute `cisco-av-pair`.
8. ACS logs the results of the posture validation request. If the request was not denied, ACS logs the results in the Passed Authentications log (if enabled). If the request was denied (for instance by the authorization policy or if no posture validation rule with matched required credential types was present), then ACS logs the results in the Failed Attempts log.

The endpoint handles the results of the posture validation request according to its configuration. The AAA client enforces network access as dictated by ACS in its RADIUS response. By configuring profiles, you define authorizations and, therefore, network access control, based on the system posture token that is determined as a result of posture validation.

## Policy Overview

You can use ACS to set up internal or external posture validation policies that return a posture token and an action after checking the rules that you (or the external server) set for the policy.

Policies are reusable; that is, you can associate a single policy with more than one network access profile. For example, if your NAC implementation requires two profiles, one for endpoints using NAI software and one for endpoints using Symantec software, you may need to apply the same rules about the operating system of the endpoint; regardless of which anti-virus application is installed. You can create a single policy that enforces rules about the operating system and associate it with the Symantec and the NAI server information.

The results of applying a policy are:

- **Posture Assessment**—The credential type and, therefore, the NAC-compliant application to which the policy evaluation result applies.
- **Token**—One of six predefined tokens that represents the posture of the endpoint and, specifically, the application that the result credential type defines.
- **Notification String**—An optional text string that is sent in the posture validation response to the application that the posture assessment defines.

## About Posture Credentials and Attributes

For posture validation, credentials are the sets of attributes sent from the endpoint to ACS. Also known as inbound attributes, these attributes contain data that is used during posture validation to determine the posture of the computer. ACS considers attributes from each NAC-compliant application and from CTA to be different types of credentials.

With policies that ACS creates for validation, the rules that you create use the content of inbound attributes to determine the APT returned by applying the policy. With policies that are created for validation by an external server, ACS forwards the credential types that you specify to the external NAC server. In either case, the contents of inbound attributes provide the information that is used to determine posture and, thus, to control network admission for the computer.

ACS uses NAC attributes in its response to the endpoint. These attributes are called outbound attributes. For example, APTs and the SPT are sent to the endpoint in attributes.

Credential types are uniquely identified by two identifiers: vendor ID and application ID. The vendor ID is the number that is assigned to the vendor in the [IANA Assigned Numbers RFC](#). For example, vendor ID 9 corresponds to Cisco Systems, Inc. Vendors assign numbers to the NAC applications that they provide. For example, with Cisco Systems, Inc., applications, application ID 1 corresponds to CTA. In the HTML interface, when you specify result credential types for a policy, credential types are identified by the names that are assigned to the vendor and application. For example, the credential type for CTA is Cisco:PA (where PA refers to posture agent, another term for CTA). In a posture validation response, ACS would use the numeric identifiers 9 and 1, which are the identifiers for Cisco and CTA, respectively.

Attributes are uniquely identified by three identifiers: vendor ID, application ID, and attribute ID. For each unique combination of vendor and application, there are set of attributes that each have numbers as well. When ACS communicates with an endpoint, the identifiers are numerical. In the HTML interface, when you define rules for internal policies, attributes are identified by the names that are assigned to vendor, application, and attribute. For example, the CTA attribute for the version of the operating system is Cisco:PA:OS-Version. The data that ACS receives identifies the attribute with the numeric identifiers 9, 1, and 6, which are the identifiers for Cisco, CTA, and the sixth attribute of CTA, respectively.

For more information about attributes, including data types and operators that are used in rules for internal policies, see [Posture Validation Attribute Data Types, page 14-8](#). We recommend that you use RDBMS Synchronization to add and configure custom RADIUS vendors; however, you can use `CSUtil.exe` to accomplish the same custom RADIUS vendor and VSA configurations that you can accomplish by using RDBMS Synchronization. For information about using `CSUtil.exe` to export, add, or delete posture validation attributes, see [Posture-Validation Attributes, page D-28](#).

## Extended Attributes

You use extended attributes to configure conditions that support Linux clients, and are specific for different Linux packages. For example, you can configure a condition for the version of the **openssl** package.

You input values for these Linux packages in the Entity field. When you input an extended attribute from the attribute drop-down list, the entity field is enabled. You can then select an entity from the drop-down list.

For example, if you select the `Cisco:Host:Package:Version` attribute, which is an extended attribute, the Entity drop-down list displays all the Linux packages that are configured in the system (ACS).

You can add or delete extended attributes by using `CSUtil.exe`. For more details, see [Posture-Validation Attributes, page D-28](#).

## Posture Validation Attribute Data Types

Posture validation attributes can be one of the following data types:

- **boolean**—The attribute can contain a value of 1 or 0 (zero). In the HTML interface, when you define a rule element with a boolean attribute, the words `false` and `true` are valid input. Valid operators are `=` (equal to) and `!=` (not equal to). When a rule element using a Boolean attribute is evaluated, `false` corresponds to a value of 0 (zero) and `true` corresponds to 1.

For example, if a rule element for a Boolean attribute requires that the attribute is not equal to `false` and the attribute in a specific posture validation request was 1, ACS would evaluate the rule element to be true; however, to avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **string**—The attribute can contain a string. Valid operators are `=` (equal to), `!=` (not equal to), `contains`, `starts-with`, and `regular-expression`.

- **integer**—The attribute can contain an integer, including a signed integer. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to). Valid input in rule elements is an integer between -65535 and 65535.
- **unsigned integer**—The attribute can contain only an integer without a sign. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid input in rule elements is a whole number between 0 and 4294967295.
- **ipaddr**—The attribute can contain an IPv4 address. Valid operators are = (equal to), != (not equal to), and `mask`. Valid format in rule elements is dotted decimal format. If the operator is `mask`, the format is the `mask/IP`. For more information, see [Internal Policy Configuration Options, page 14-10](#).
- **date**—The attribute can contain a date. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to), and `days-since-last-update`. Valid format in rule elements:  

```
mm/dd/yyyy
hh:mm:ss
```
- **version**—The attribute can contain an application or data file version. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid format in rule elements:  

```
n.n.n.n
```

where each *n* can be an integer from 0 to 65535.
- **octet-array**—The attribute can contain data of arbitrary type and variable length. Valid operators are = (equal to) and != (not equal to). Valid input in rule elements is any hexadecimal number, such as 7E (the hexadecimal equivalent of 126).

## Internal Policies

This section contains the following topics:

- [About Internal Policies, page 14-9](#)
- [About Rules, Rule Elements, and Attributes, page 14-10](#)
- [Internal Policy Configuration Options, page 14-10](#)

## About Internal Policies

Internal policies comprise one or more rules that you define in ACS. When ACS applies an internal policy, it uses the policy rules to evaluate credentials that are received with the posture validation request. Each rule is associated with an APT, a credential type, and an action. The credential type determines which NAC-compliant application with which the APT and action are associated.

ACS applies each rule in the order they appear on the Posture Validation Policies page (from top to bottom), resulting in one of the following two possibilities:

- **A configurable rule matches**—When all elements of a rule are satisfied by the credentials that are received in a posture validation request, the result of applying the policy is the condition, posture assessment, and notification string that are associated with the rule. ACS does not evaluate the credentials with any additional rules.
- **No configurable rule matches**—When the attributes that are included in the posture validation request satisfy no policy rules, ACS uses the condition, posture assessment, and notification string that are associated with the default rule as the result of the policy.

**Note**

Applying a policy to a posture validation request always results in a match, to one of the configurable rules or to the default rule.

When you specify the order of rules in a policy, determine the likelihood of each rule to be true and then order the rules so that the rule most likely to be true is first and the rule least likely to be true is last. Doing so makes rule processing more efficient; however, determining how likely a rule is to be true can be challenging. For example, one rule may be true for the posture of twice as many endpoints as a second rule, but posture validation may occur more than twice as often for endpoints whose posture matches the second rule; therefore, the second rule should be listed first.

## About Rules, Rule Elements, and Attributes

A rule is a set of one or more rule elements. A rule element is a logical statement which comprises:

- A posture validation attribute
- An operator or posture token
- A value or notification string

ACS uses the operator to compare the contents of an attribute to the value. Each rule element of a rule 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 detailed descriptions of rules, see [Setting Up a Profile, page 15-3](#).

## Internal Policy Configuration Options

You can specify the rules that a policy comprises, including their order from the Internal Posture Validation Setup pages. The options for configuring a internal policy are as follows:

- **Name**—Specifies the name by which to identify the policy. When selecting a policy, you select it by name, and the description is not viewable on the policy selection page; therefore, you should make the name as useful as possible.

**Note**

The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), and the slash (/).

- **Description**—Specifies a text description of the policy, up to 255 characters. In the **Description** box you enter details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules. Because you can apply the same policy to more than one profile, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which servers use it.
- **Posture Validation Rules**—Lists rules that you define in the order in which ACS uses them to evaluate the posture validation request. Each rule appears as a separate row in the table and is identified by its rule elements, which appear as a blue link in the Posture Validation Rules page. You can order the rules in this table by selecting the option directly to the left of a rule and clicking **Up** and **Down** to position it as needed. For more information about the order of rules, see [About Internal Policies, page 14-9](#).

The Posture Validation Rules table contains:

- **Condition**—Specifies a vendor and application; the credential type. If the rule is true, the credential type determines the application to which the token in the corresponding Token list is associated. For example, CTA appears on the list as `Cisco:PA`. For more information about credential types, see [About Posture Credentials and Attributes, page 14-7](#).
- **Posture Assessment**—Specifies the vendor and application, and a token (an APT). If the rule is true, the Token list determines the APT that is associated with the vendor and application that is selected in the corresponding Posture Assessment list. For more information about tokens, see [Posture Tokens, page 14-3](#).
- **Notification String**—Specifies a text message that is sent to the application that the Result Credential Type list indicates. The vendor determines use of the text message. Some NAC-compliant applications do not implement the use of the Notification String box.
- **Default Rule**—If no configurable rule is true, the Default Rule specifies the posture assessment, token, and notification string (if specified) that ACS uses as the result of applying the policy.



---

**Note** Under Default Rule, the meanings of the Posture Assessment list, Token list, and Notification String box are identical to the options of the same name in the Posture Validation Rules table; except that the default rule is automatically true, provided that no rule in the Posture Validation Rules table is true.

---

## External Policies

This section contains the following topics:

- [About External Policies, page 14-11](#)
- [External Policy Configuration Options, page 14-12](#)

### About External Policies

External policies are policies that are defined by an external NAC server, usually from an anti-virus vendor and a set of credential types to be forwarded to the external database. You also have the option of defining a secondary external NAC server. The presence of a secondary server allows the secondary or failover to evaluate any policies from the primary server.

ACS does not determine the result of applying an external policy; instead, it forwards the selected credentials to the external NAC server and expects to receive the results of the policy evaluation: an APT, a result credential type, and an action.

Each external policy that is associated with an external server must return a result; otherwise, ACS rejects policy validation requests that are evaluated with a profile whose external policies do not return a result. For example, if ACS evaluates a posture validation request by using a profile that has 10 internal policies and one external policy, but the external NAC servers associated with the external policy are not online, it is irrelevant that the 10 internal policies all return SPTs. The failure of the single external policy causes ACS to reject the posture validation request.

## External Policy Configuration Options

On the External Posture Validation Setup page you can specify a NAC server (and an optional second NAC server) that ACS relies upon to apply the policy and configure the set of credential types that ACS forwards. The options for configuring an external policy are as follows:

- **Name**—Specifies the name by which to identify the policy.




---

**Note** The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), and the slash (/).

---

- **Description**—Specifies a text description of the policy, up to 255 characters. For each profile using the policy, the text you type in the **Description** box appears beside the policy. Use the Description box to provide details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules.

Because you can apply the same policy to more than one profile, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which profiles use it.

- **Server Configuration**—You must specify a primary server. You can specify a secondary server for failover operation. For each posture validation request to which an external policy is applied, ACS attempts to use the first enabled server configuration in the policy that is enabled. If the first enabled server is the primary server and ACS cannot reach the primary server or the primary server fails to respond to the request, ACS will use the secondary server, if it is configured and enabled.

For the primary and secondary server configurations, each have:

- **URL**—Specifies the HTTP or HTTPS URL for the server. The format for URLs is:

```
[http[s]://]host[:port]/resource
```

where *host* is the hostname or IP address of the NAC server, *port* is the port number used, and *resource* is the rest of the URL, as required by the NAC server itself. The URL varies depending upon the server vendor and configuration. For the URL that your NAC server requires, refer to your NAC server documentation.

The default protocol is HTTP. URLs beginning with the hostname are assumed to be using HTTP. To use HTTPS, you must specify the URL beginning with `https://` and you must import a self-generated CA certificate into ACS for this policy server. See [ACS Certificate Setup, page 10-26](#).

If the port is omitted, the default port is used. The default port for HTTP is port 80. The default port for HTTPS is port 443.

If the NAC server hostname is *antivirus1*, which uses port 8080 to respond to HTTP requests for the service provided *policy.asp*, a script kept in a web directory called *cnac*, valid URLs would be:

```
http://antivirus1:8080/cnac/policy.asp
antivirus1:8080/cnac/policy.asp
```

If the same server used the default HTTP port, valid URLs would be:

```
http://antivirus1/cnac/policy.asp
http://antivirus1:80/cnac/policy.asp
antivirus1/cnac/policy.asp
antivirus1:80/cnac/policy.asp
```

If the same server used HTTPS on the default port, valid URLs would be:

```
https://antivirus1/cnac/policy.asp
https://antivirus1:443/cnac/policy.asp
```

- **Username**—Specifies the username by which ACS submits forwarded credentials to the server. If the server is not password protected, the values in the Username and Password boxes are ignored.
- **Password**—Specifies the password for the username in the Username box.
- **Timeout (Sec)**—The number of seconds that ACS waits for a reply from a server after it forwards the credentials.

If a secondary server is configured, requests to the primary server that time out are forwarded to the secondary server.

If no secondary server is configured or if a request to the secondary server also times out, ACS cannot apply the external policy and the posture validation request is rejected.

For each posture validation request, ACS always tries the primary server first, regardless of whether previous requests timed out.

- **Trusted Root CA**—The certificate authority (CA) that issued the server certificate that the uses server. If the protocol is HTTPS, ACS forwards credentials to a server only if the CA that is specified on this list issued the certificate that it presents. If ACS cannot forward the request to the primary or secondary NAC server because the trusted root CAs did not issue the server certificates, the external policy cannot be applied and, therefore, the posture validation request is rejected.

If the Trusted Root CA list does not contain the CA that issued a NAC server certificate, you must add the CA certificate to ACS. For more information, see [Adding a Certificate Authority Certificate, page 10-28](#).



**Note**

ACS does not check NAC server certificates against certificate revocation lists, regardless of whether you have configured a CRL issuer for the CA of the NAC server certificate.



**Tip**

You must select the correct certificate type for the CA, not just the name of the CA. For example, if the server presents a VeriSign Class 1 Primary CA certificate and VeriSign Class 1 Public Primary CA is selected on the Trusted Root CA list, ACS does not forward the credentials to the server when HTTPS is in use.

- **Forwarding Credential Types**—Contains two lists for use in specifying which credential types are forwarded to the external server. The credentials are:
  - **Available Credentials**—Specifies the credential types that *are not* sent to the external server.
  - **Selected Credentials**—Specifies the credential types that *are* sent to the external server.



**Tip**

You can add credential types by using the **CSUtil** command. For detailed instructions, see [Importing External Audit Posture-Validation Servers, page D-33](#).

## NAH Policies

This section contains the following topics:

- [About External Audit Servers, page 14-14](#)
- [External Audit Server Configuration Options, page 14-16](#)

### About External Audit Servers

Audit servers are Cisco and third-party servers that determine posture information about a host without relying on the presence of a Posture Agent (PA). The Cisco PA is also known as the Cisco Trust Agent (CTA). Audit servers are used to assess posture validation with an organization's security policy. You can also define a secondary external audit server. The presence of a secondary audit server allows the second or failover server to evaluate any policies from the primary server when the primary server rejects a policy.

An audit policy is a set of processing rules for evaluating the posture of a NAH through an audit server. Audit policies are used to retrieve posture decisions for hosts that do not have an EAP supplicant. When a host accesses the network through a NAD that is acting as a NAC enforcement point, the NAD sends information to ACS so that ACS can trigger auditing. If ACS is configured correctly, it queries the audit server for the result (posture token) of the audit and then determines the authorization based on the audit result.

Your network-management security strategy may include external audit servers that work with ACS to control access to your network.

ACS will use the **GAME** protocol to communicate with audit servers. In each audit request, ACS forwards the following information to the audit server:

- `host id`
- `ip-address`
- `mac-address` (optional)

The name of the System-Posture-Token is dynamically sent (without requiring any configuration) to the device.

[Table 14-2](#) defines the details required in applying the results of an audit.

**Table 14-2**      **Audit Policy Requirements**

Audit Policy	Description
<code>auditServerConfiguration</code>	A pointer to the audit server configuration that defines how to communicate with the audit server.
<code>exemptionList</code>	A list of MAC and/or IP addresses that are exempt from audit.
<code>inverseExemptionFlag</code>	If this flag is set, the meaning of the exemption list will be inverted. That is, only the hosts specified in the list will be audited; all others will be exempt.
<code>exemptionToken</code>	The token to assign to hosts who are exempt.
<code>defaultInProgressToken</code>	The token to use when the audit is in progress and we have no cached token.

Table 14-2 Audit Policy Requirements (continued)

Audit Policy	Description
<b>staticAttributes</b>	These name value pairs will be sent to the audit server when this policy is invoked. For this release, this list of attributes will be used to pass the policy name.
<b>tokenMappings</b>	The token to user group mapping. Note that this scheme assumes that there is only one audit policy per service.

### How an External Audit Gets Triggered

An endpoint failure triggers an external audit. This failure occurs when the enforcement point detects that the endpoint is not responding as required. The enforcement point sends the `aaa:event` failure message to indicate that a device failure has occurred.

The current release of ACS supports this event type and provides configuration in the out-of-band posture policy about which event should activate the policy (may be more than one).

ACS must be able to recognize the following events that may or may not trigger an audit, depending on policy configuration:

- NAS detects lack of functioning CTA and sends NRH notification in the `aaa:event` attribute
- Endpoint device (or supplicant) is unable to respond to a posture request
- An explicit audit request from the device

Once ACS recognizes that an audit will occur, the audit server is queried. The audit server responds with results or an audit-in-progress message, which may contain a polling timeout hint to pass on to the NAD. At this point, ACS evaluates the enforcement policy for the given host based on the default APT that is associated with the posture validation policies. Part of the enforcement policy must be a session-timeout value that is used to trigger the NAD to reauthenticate the host. ACS receives the request and queries the audit server. This process repeats itself until the audit server responds with an APT. Once the audit response is received, enforcement policies are reevaluated and returned to the NAD.

The NAD caches the posture token that will be sent along with any subsequent access requests occurring during the host's session; for instance, as a result of session timeout (reauthentication). ACS uses this token for default policy evaluation during the audit for these subsequent authentications, thereby avoiding session downgrade for the connected host.

### Exemption List Support

ACS supports an exemption list for audit activation. The exemption list contains a list of IP or MAC addresses to include or exclude from the audit. When a host is exempted, it is assigned an exemption token that determines its posture status. The exemption list is defined in the out-of-band audit policy. The IP list may contain single IP addresses or IP mask ranges. The MAC lists may be MAC ranges in the form of partial MAC strings that are matched with the hosts MAC address by using the *begins with* operator.

## External Audit Server Configuration Options

Table 14-3 describes the external audit server settings.

**Table 14-3 External Audit Server Options**

Options	Description
<b>Which Hosts Are Audited</b>	
<b>Audit all hosts</b>	Audit all hosts that do not contain a posture agent.
<b>Audit these hosts</b>	Audit only the hosts for which you have provided host IP addresses and ranges (IP/Mask) or MAC addresses.
<b>Do not audit these hosts</b>	Exclude the hosts for which you have provided host IP addresses and ranges (IP/Mask) or MAC addresses and audit all other hosts.
<b>Select a token for the hosts that will not be audited</b>	Select a token from the drop-down list for hosts that are not audited.
<b>Use These Audit Servers</b>	
<b>Audit server vendor</b>	Vendor name in ADF file. See <a href="#">Importing External Audit Posture-Validation Servers, page D-33</a> if no audit servers appear in the drop-down box.
<b>Primary &amp; Secondary Server Configuration</b>	
<b>URL</b>	URL of the audit server. Refer to your audit server documentation for format guidelines.
<b>Username</b>	Credential ACS needs to access the audit server.
<b>Password</b>	Credential ACS needs to access the audit server.
<b>Timeout (sec)</b>	Number of seconds ACS waits for a result from the audit server, including domain name resolution.
<b>Trusted Root CA</b>	If the URL you provide specifies the HTTPS protocol, select the certification authority that issued the audit server certificate installed on the primary server from the Trusted Root CA list.
<b>Validate Certificate Common Name</b>	Enable this option to compare the host name within the URL to the common name in the certificate. If they do not match, the SSL connection is closed, posture validation fails, and user access will be denied. Leave this check box unchecked to disable this feature.
<b>Audit Host Settings</b>	
<b>Use this token while Audit Server does not yet have a posture validation result</b>	Interim posture token sent from ACS to the NAD while waiting for a result.
<b>Polling Intervals and Session-Timeout:</b>	Select whether ACS should use timeout values that are sent by the audit server or use settings in the authorization policy.  If you select <b>Use Settings in Authorization Policy for Session-Timeout</b> , you must specify a polling interval in the Polling Interval (seconds) field. You must also configure any RACs in the authorization policy to assign specific timeout values for the final resulting tokens. See <a href="#">Configuring an Authorization Rule, page 15-44</a> .

Table 14-3 External Audit Server Options (continued)

Options	Description
<b>Which Hosts Are Audited</b>	
<b>Maximum amount of times the Audit Server should be polled</b>	Select the maximum amount of times ACS should query the audit server for a result (posture token). Maximum of 10 times.
<b>Policy string to be sent to the Audit Server</b>	If the audit server supports named policy invocation, enter the name of policy here.

## Configuring Policies

If you plan to use NAC in your network, you will need to define the manner in which posture validation will be performed. Policies are sets of rules that are used to determine a posture token for a posture validation request.

You can configure posture validation, also known as posture compliance, as:

- Internally within ACS. See [Setting Up Posture Validation Policies, page 14-18](#).
- Externally by using the Host Credential Authorization Protocol (HCAP) protocol to one or more Posture Validation Servers (PVSs). See [Setting Up an External Policy Server, page 14-24](#).
- Externally by using the GAME protocol to an audit server for NAC agentless host (NAH) support. See [Setting Up an External Audit Posture Validation Server, page 14-25](#).

Table 14-4 describes the setup options for posture validation.

Table 14-4 Posture Validation Options

Component	Description	Notes
<b>Internal Posture Validation</b>	Policy requirements for the network are internally (or locally) validated within ACS.	NAC policies for the CTA, Windows, CSA, and anti-virus software applications are among recommended internal policies. See <a href="#">Creating an Internal Policy, page 14-18</a>
<b>External Posture Validation</b>	Policies are validated by an outside posture validation server.	Externalizing the posture validation to an AV server allows you to handle proprietary AV posture credentials and anti-virus policy administration by an AV administrator separate from the ACS administrator.
<b>External Audit Posture Validation</b>	Cisco and third-party servers that determine posture information about a host without relying on the presence of a PA. These types of hosts are also referred to as <i>agentless</i> . Audit servers are used to assess posture validation with an organization's security policy.	The Cisco PA is also known as the CTA. If no CTA is on the host, then an audit server can be used.



### Note

You can perform internal and external posture validation at the same time; but not for the same NAC credential types (vendor-application combinations).

To configure a policy for internal or external posture validation:

- 
- Step 1** In the navigation bar, click **Posture Validation**.
- Step 2** Select one of the components to set up your posture validation servers:
- **Internal Posture Validation Setup**—See [Internal Policies, page 14-9](#) or [Creating an Internal Policy, page 14-18](#)
  - **External Posture Validation Setup**—See [External Policies, page 14-11](#) or [Setting Up an External Policy Server, page 14-24](#)
  - **External Posture Validation Audit Setup**—See [NAH Policies, page 14-14](#) or [Setting Up an External Audit Posture Validation Server, page 14-25](#)
- Step 3** Complete the required steps to set up internal or external posture validation.
- 

## Setting Up Posture Validation Policies

This section contains the following topics:

- [Creating an Internal Policy, page 14-18](#)
- [Cloning a Policy or Policy Rule, page 14-21](#)
- [NAH Policies, page 14-14](#)
- [Editing a Policy, page 14-20](#)
- [Deleting a Policy or Rule, page 14-23](#)

### Creating an Internal Policy

Use internal posture validation to write your own policies for access in your network. After you have created policies, you can then profile rules to use these policies.

You can select internal policies for more than one profile. To add the policy to a profile, use the Network Access Profiles page.

For descriptions of the options available on the Internal Posture Validation Setup page, see [Internal Policy Configuration Options, page 14-10](#).

For details on how to set up your third-party component policies, see the related documentation on the Go NAC website on Cisco.com. For information on adding internal policies to your profiles, see [Configuring Posture-Validation Policies, page 15-35](#).

Once you have set up at least one policy, you can use the clone rule option to save time by copying a policy and customizing it. For details on how to use cloning, see [Cloning a Policy or Policy Rule, page 14-21](#).

To create your internal posture validation policy:

- 
- Step 1** Access the Internal Policy Validation Setup page:
- a. In the navigation bar, click **Posture Validation**.
  - b. Click **Internal Posture Validation Setup**.  
ACS displays a list of posture validation policies, if available.

c. Click **Add Policy**.

**Step 2** In the **Name** box, type a descriptive name for the policy.

**Step 3** In the **Description** box, type a useful description of the policy.

**Step 4** Click **Submit**.

**Step 5** Click **Add Rule**.

**Step 6** Set conditions to define.

a. For each condition set that you want to add:

- i. Select an attribute. For more information about attribute types, see [Posture Validation Attribute Data Types, page 14-8](#).
- ii. Select an entity (only available for extended attributes).
- iii. Select an operator.
- iv. Type a value.
- v. Click **Enter** and then **Submit**.

For example, if you create a policy for the Cisco Security Agent (CSA) you might create the following condition sets:

- *Cisco:PA:PA-Version >= 2.0.0.0 AND Cisco:PA:Machine-Posture-State = 1 with a Posture token=Healthy.*
- *Cisco:PA:PA-Version >= 2.0.0.0 AND Cisco:PA:Machine-Posture-State = 2 with a Posture Token=Transition.*
- Match OR inside Condition and AND between Condition Sets to allow ACS to choose between tokens.

For more information about operators, see [Internal Policy Configuration Options, page 14-10](#).

For information on CTA posture plugin attributes and values, see the Cisco Trust Agent documentation.

The condition set appears in the Conditions Sets table.

b. Select which Boolean condition to add to this condition set:

- **Match OR inside Condition and AND between Condition Set**—Select if you want to be less stringent with your conditions.
- **Match AND inside Condition and OR between Condition Sets**—Select if you want to be more secure with your posture validation.

c. Verify that the condition sets are configured as intended.



**Tip**

If you want to change a condition set that you have already added, select the condition element, click **Remove**, and update its attribute, entity, operator, or value, then click **Enter**.

d. For the new rule, do each of the following:

- i. Select a credential type.
- ii. Select a token.
- iii. Type an action (in the form of an notification string).

For more information about tokens, see [Posture Tokens, page 14-3](#).

If the rule matches the posture validation request, ACS associates with the policy the result credential type, token, and action that you specify.



**Tip** If you want to create another condition set that is identical to one that is already created, click **Clone**. Then change the condition set as needed.

**Step 7** Click **Submit**.

The Policy Validation Rules page appears again. The new condition set appears at the bottom of the Condition Sets table.



**Tip** You can return to the Posture Validation Rules page by clicking the rule.

**Step 8** After you create the rules that define the policy, order the rules as needed. ACS applies a policy by attempting to match rules in the order that they appear on the Policy Validation Rules page, from top to bottom. Policy processing stops at the first successful rule match; so order is important. To move a rule:

- a. Select the rule. To do so, click the radio button to the left of the rule.
- b. Click the **Up** or **Down** button as needed until the rule is positioned properly.

**Step 9** Configure the Default Rule at the bottom of the Posture Validation Rules page by clicking **Default**:

- i. Select a credential type.
- ii. Select a token.
- iii. Type an action (in the form of a notification string).

When ACS applies this policy to a posture-validation request and none of the configurable rules matches the request, ACS associates the default credential type, token, and action that you specify with the policy.

**Step 10** Click **Submit**.

The Posture Validation Rules page displays the new rule.

**Step 11** Click **Done**.

The current configuration has been changed.

**Step 12** Click **Apply and Restart** for your changes to take effect.

## Editing a Policy

You can only edit a policy by accessing it through the Posture Validation pages.

To edit a policy or posture validation rule:

**Step 1** In the navigation bar, click **Posture Validation**.

**Step 2** Click **Internal Posture Validation Setup**.

**Step 3** Click on the policy name of the rule that you want to edit.

The applicable policy rules page appears.

**Step 4** To edit a policy:

- a. Click **Add Rule** to add more condition sets.

- b. To change a condition set that you have already added:
    - i. Select the condition element.
    - ii. Click **Remove**.
    - iii. Update its attribute, entity, operator, or value; then click **Enter**.
  - c. To add a new condition:
    - i. Select the attribute, entity, and operator from the drop-down lists.
    - b. Enter a value.
    - c. Click **Enter**.
  - d. Click **Clone** to copy an existing condition set or policy rule.
  - e. Click **Delete** to remove policy rule. You can also remove a condition set or an element from a condition set. See [Deleting a Condition Component or Condition Set, page 14-23](#).
  - f. To move a rule:
    - i. Select the rule by clicking the button to the left of the rule.
    - ii. Click the **Up** or **Down** button as needed until the rule is positioned properly.
  - g. If you want to add or change a Boolean condition to this condition set, select one of the options:
    - **Match OR inside Condition and AND between Condition Set**—Select if you want to be less stringent with your conditions.
    - **Match AND inside Condition and OR between Condition Sets**—Select if you want to be more secure with your posture validation.
  - h. Click **Rename** to change the existing name.
 

ACS creates a new policy. ACS stores the new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.
- Step 5** When finished with editing, click **Submit**. Then click **Done**.
- Step 6** Click **Apply and Restart** for your changes to take effect.

## Cloning a Policy or Policy Rule

This option creates a policy or rule that is identical to the selected one. You can then easily modify the settings.

To clone an internal posture validation policy or policy rule:

- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To do so:
- a. In the navigation bar, click **Posture Validation**.
  - b. Click **Internal Posture Validation Setup**.
 

ACS displays a list of posture validation policies.
  - c. Select a policy name from the list.



**Tip** If no policies are configured, click **Add Policy** and follow the instructions in [Creating an Internal Policy, page 14-18](#).

- Step 2** To make a copy of the current policy, click **Clone**.  
For example, if you selected *VPNmgmt1* as the policy, the copy would be *Copy-of-VPNmgmt1*.
- Step 3** To make a copy of one of the policy rules inside the current policy, click the condition name. Then click **Clone**.  
The Policy Validation Rule page appears again. The new condition set appears in the Condition Sets table.
- Step 4** Click **Rename** to change the existing name to a more meaningful name or description.  
ACS creates a new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.
- Step 5** When you finish with editing, click **Submit**.
- Step 6** Click **Done** if you are finished adding clones.
- Step 7** Click **Apply and Restart** for your changes to take effect.
- 

## Renaming a Policy

Use the renaming feature to change the name or description of an existing or cloned policy to something more meaningful.

To rename a policy:

- 
- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To do so:
- In the navigation bar, click **Posture Validation**.
  - Click **Internal Posture Validation Setup**.  
ACS displays a list of posture validation policies.
  - Select a policy name from the list.
- Step 2** Click **Rename** to change the existing policy name or make the description more meaningful.
- Step 3** Enter the changes to the policy name or description. When you finish editing, click **Submit**.  
ACS creates a new policy. ACS stores the new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.
- Step 4** Click **Done**.  
The renamed policy appears at the bottom of the Posture Validation Policies page.
- Step 5** Click **Apply and Restart** for your changes to take effect.
-

## Deleting a Policy or Rule

To delete a policy or rule:

- 
- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To Access the Internal Policy Validation Setup page:
- In the navigation bar, click **Posture Validation**.
  - Click **Internal Posture Validation Setup**.
- ACS displays a list of posture validation policies.
- Step 2** To delete a rule or policy, select a policy name from the list of posture validation policies.
- The Posture Validation Rules page appears.
- Step 3** To delete an entire policy and all its rules, click **Delete**.
- This deletes the policy from the policy validation list; but does not remove the policy from any profiles with which it may be associated. A warning message prompts you to cancel or click **OK**.
- Step 4** To delete an element or condition set, see [Deleting a Condition Component or Condition Set, page 14-23](#).
- ACS deletes the policy rule. The policies page reappears and the policies table no longer lists the deleted policy. All profiles that were configured to use the policy no longer include the deleted policy.
- 

## Deleting a Condition Component or Condition Set

A condition component is the list of elements that a condition set comprises. To delete a condition component from a condition set or an entire condition set:

- 
- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To Access the Internal Policy Validation Setup page:
- In the navigation bar, click **Posture Validation**.
  - Click **Internal Posture Validation Setup**.
- ACS displays a list of posture validation policies.
- Step 2** Select a policy name from the list of posture validation policies.
- The Posture Validation Rules page appears.
- Step 3** Select a blue link in the Condition list on the Posture Validation Rules page.
- Step 4** To delete the entire condition set, click **Delete**. Then click **Done**.
- Step 5** To delete a selected condition component from the set, select a blue link in the Condition Sets list, then click **Delete**. Click **Submit** when you have deleted all condition components desired.
- ACS deletes the condition set or condition component.
- Step 6** Click **Done**.
-

## Setting Up an External Policy Server

This procedure describes how you can create an external policy.

### Before You Begin

You can select external policies for more than one profile. To create external policies, use the External Posture Validation Setup pages. To add the policy to a profile, use the Network Access Profiles page. See [Setting Up a Profile, page 15-3](#).

The external server that you use to access the External Policy Validation page does not limit which profiles can select the new external policy.

For descriptions of the options available on the External Policy Configuration page, see [External Policy Configuration Options, page 14-12](#).

---

**Step 1** After selecting **External Posture Validation Setup**, the External Posture Validation Servers page displays.

**Step 2** Click **Add Server**.

The Add/Edit External Posture Validation Server page appears.

**Step 3** Name the server and provide a description if necessary.

**Step 4** Provide addressing information for the primary and secondary servers.

- a. Select the **Primary Server configuration** check box.




---

**Note** If you do not select the **Primary Server Configuration** check box, ACS uses the secondary server configuration. If no secondary server configuration exists or if the secondary server is unreachable, the posture validation request is rejected.

---

- b. Provide configuration details about the primary NAC server. For more information about the boxes and list in this area, see [External Policy Configuration Options, page 14-12](#).

**Step 5** (Optional) In the **Secondary Server configuration** pane:

- a. Select the **Secondary Server configuration** check box
- b. Enter configuration details about the secondary NAC server. For more information about the boxes and list in this area, see [External Policy Configuration Options, page 14-12](#).

**Step 6** Determine credentials to forward to the primary or secondary external server by moving the available credentials to the selected credentials column.

**Step 7** Click **Submit** to save your changes.

**Step 8** Click **Apply and Restart** to submit your changes to ACS.

---

## Editing an External Posture Validation Server

You can edit an external posture validation server by accessing it through the Posture Validation pages. To edit an external posture validation server:

- 
- Step 1** In the navigation bar, click **Posture Validation**.
  - Step 2** Click **External Posture Validation Setup**.
  - Step 3** Click the server name that you want to edit.  
The Add/Edit External Posture Validation Server page appears.
  - Step 4** Edit the fields and click **Submit**.
- 

## Deleting an External Posture Validation Server

You can remove an external posture validation server by accessing it through the Posture Validation pages.

To delete an external posture validation server:

- 
- Step 1** In the navigation bar, click **Posture Validation**.
  - Step 2** Click **External Posture Validation Setup**.
  - Step 3** Click the server name that you want to delete.  
The Add/Edit External Posture Validation Server page appears.
  - Step 4** Click **Delete**.
- 

## Setting Up an External Audit Posture Validation Server


Use this page to create, modify, and delete external posture validation audit servers. Policies are reusable; you can associate an audit policy with more than one network access profiles.

### Before You Begin

You must add your audit vendor to the ACS internal dictionary by using the **CSUtil** command before you can configure an external posture validation audit server. For detailed instructions, see [Importing External Audit Posture-Validation Servers, page D-33](#).

To configure an audit server for external posture validation:

- 
- Step 1** After selecting **External Posture Validation Audit Setup**, the External Posture Validation Audit Server page appears.
  - Step 2** Click **Add Servers**.  
The Edit External Posture Validation Audit Setup page appears.
  - Step 3** Enter a name for the audit policy.

- Step 4** Select which hosts to audit. Select one of the following options from the drop-down list:
- **Audit all hosts**—Audit all hosts that do not contain a posture agent.
    - **Audit these hosts**—Audit only the hosts for which you have provided Host IP addresses and ranges (IP/Mask) or MAC addresses.
    - **Do not audit these hosts**—Exclude the hosts for which you have provided Host IP addresses and ranges (IP/Mask) or MAC addresses and audit all other hosts.
  - **Select a Posture Token for the hosts that will not be audited**—Select a token from the drop-down list for hosts that are not audited.
- Step 5** Select your audit server vendor, and provide addressing information and credentials for accessing a primary and if you require a failover, a secondary audit server.
-  **Tip** If your audit vendor does not appear, it does not have an audit APT defined in the internal ACS dictionary. To add an audit vendor, see [Importing External Audit Posture-Validation Servers, page D-33](#)
- Step 6** Set directives for interpreting the various results and states that the audit server returns. The directives include:
- **Use this Posture Token while the Audit Server does not yet have a posture validation result**—Select a token from the drop-down list. The in progress token is used before the audit server determines the actual posture of the NAC agentless host.
  - **Polling Intervals and Session-Timeout**—This option specifies polling intervals sent by the audit server and is enabled by default.
  - **Maximum amount of times the Audit Server should be polled**—Select the maximum amount of times that ACS should query the audit server for a result (posture token).
  - **Policy string sent to be sent to the Audit Server**—If the audit server supports named policy invocation, enter the name of policy.
- Step 7** Click **Submit** to save your external posture validation audit server setup.
- 

## Editing an External Posture Validation Audit Server

You can edit an external posture validation audit server by accessing it through the Posture Validation pages.

To edit an external posture validation server:

- Step 1** In the navigation bar, click **Posture Validation**.
- Step 2** Click **External Posture Validation Audit Setup**.
- Step 3** Click the server name that you want to edit.  
The External Posture Validation Audit Server page appears.
- Step 4** Edit the fields and click **Submit**.
-

## Deleting an External Posture Validation Server

You can remove an external posture validation audit server by accessing it through the Posture Validation pages.

To delete an external posture validation audit server:

- 
- Step 1** In the navigation bar, click **Posture Validation**.
  - Step 2** Click **External Posture Validation Audit Setup**.
  - Step 3** Click the server name that you want to delete.  
The External Posture Validation Audit Server page appears.
  - Step 4** Click **Delete**.
- 

## How Posture Validation Fits into Profile-Based Policies

In order to understand the profile-based policy paradigm, you should understand network access profiles. A profile is essentially a classification of network access requests for applying a common policy. Profile-based policies include rules for authentication, authorization, and posture validation.

Authorization rules are no longer set in Posture Validation but in the Network Access Profiles tab. Using authorization in NAP, you can provision the same RADIUS attribute to have different values for different users, groups and profiles. The one-user-one-group-one-profile is now more flexible, by using profile-based policies instead.

After configuring posture validation rules, you must associate those rules to a network access profile. For detailed instructions, see [Setting a Posture-Validation Policy, page 15-37](#).

For more detailed information on policy-based profiles, see [Overview of NAPs, page 15-1](#).

