



## CHAPTER 13

# Posture Validation

---

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports posture validation when ACS is deployed as part of a broader Cisco Network Access Control (NAC) solution.

This chapter contains:

- [What is Posture Validation?, page 13-1](#)
- [Posture Validation in Network Access Control, page 13-2](#)
- [Posture Validation and Network Access Profiles, page 13-3](#)
- [Posture Tokens, page 13-3](#)
- [The Posture Validation Process, page 13-4](#)
- [Policy Overview, page 13-5](#)
- [Internal Policies, page 13-7](#)
- [External Policies, page 13-8](#)
- [External Posture Validation Audit Servers, page 13-9](#)
- [Configuring NAC in ACS, page 13-13](#)
- [Configuring ACS in a NAC/NAP Environment, page 13-15](#)
- [Configuring Policies, page 13-15](#) (including internal, external, and audit server)
- [Posture Validation Pages Reference, page 13-30](#)

## What is Posture Validation?

The term *posture* refers to the collection of attributes that play a role in the conduct and “health” of an 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 applies a set of rules to the posture data associated with an endpoint. The result is an assessment of the level of trust associated with the endpoint. A posture token, such as **Healthy** or **Infected**, represents the state of the endpoint.

The posture token becomes 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 and the user.

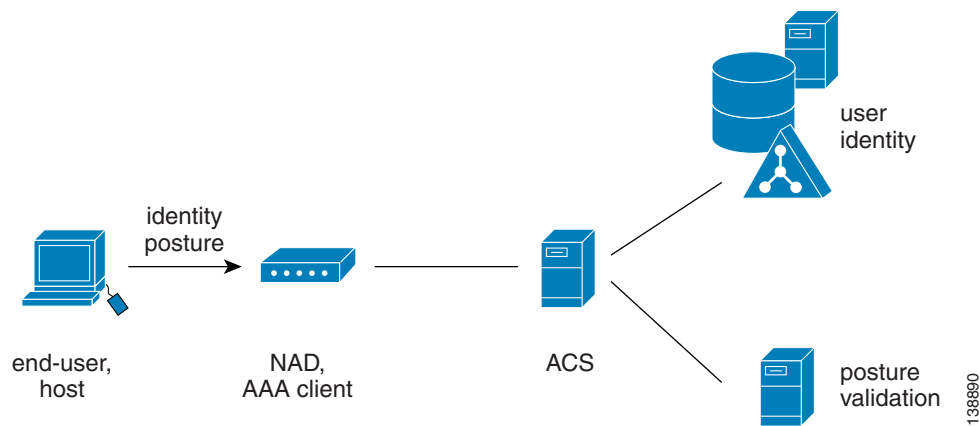
# Posture Validation in Network Access Control

Posture validation can work with Network Access Control (NAC). NAC uses the network infrastructure to enforce-security policy compliance on all devices seeking access to network computing resources.

Security-policy compliance limits damage from emerging security threats. By using NAC, customers can allow network access only to compliant and trusted endpoint devices (such as PCs, servers, and PDAs), and can restrict the access of noncompliant devices. For more information about the NAC solution, see <http://www.cisco.com/go/nac>.

Figure 13-1 shows the components of a typical NAC deployment, including posture validation.

**Figure 13-1** 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 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 13-6](#).

Examples of NAC-compliant applications are the CSA and antivirus programs from Network Associates, Symantec, or Trend Micro. These applications provide the Cisco Trust Agent 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 Trust Agent 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-band 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 Validation and Network Access Profiles

To understand the profile-based policy paradigm, you should understand network access profiles (NAPs). 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. By 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 14-30](#).

For more detailed information on policy-based profiles, see [Overview of NAPs, page 14-1](#).

## Posture Tokens

Posture tokens represent the state of an endpoint device or a NAC-compliant application that is installed on the computer. ACS recognizes two types of posture tokens:

- System posture tokens (SPTs) represent the state of the computer.
- Application posture tokens (APTs) represent the state of a NAC-compliant application.

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 13-1](#) 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 13-1 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 SPT. 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 4-10](#). For details on setting up your authorization rules as part of network access profiles, see [Classification of Access Requests, page 14-2](#).

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 [Update Packets in Accounting Logs, page 10-37](#).

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.

## The Posture Validation Process

ACS evaluates the posture attributes that it receives 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, 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, 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

This section contains:

- [About Posture Credentials and Attributes, page 13-5](#)
- [Extended Attributes, page 13-6](#)
- [Posture Validation Attribute Data Types, page 13-6](#)

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 antivirus 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 the Cisco Trust Agent 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 applications, application ID 1 corresponds to the Cisco Trust Agent. In the web interface, when you specify result credential types for a policy, the names that you assign to the vendor and application identify the credential types for the Cisco Trust Agent. For example, the credential type for the Cisco Trust Agent is *Cisco:PA* (where PA refers to posture agent, another term for the Cisco Trust Agent). In a posture validation response, ACS would use the numeric identifiers 9 and 1, which are the identifiers for Cisco and the Cisco Trust Agent, 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 web 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 Cisco Trust Agent 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, the Cisco Trust Agent, and the sixth attribute of the Cisco Trust Agent, 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 13-6](#). You can use **CSUtil.exe** to add and configure custom RADIUS vendor and VSA configurations. For information about using **CSUtil.exe** to export, add, or delete posture validation attributes, see [User-Defined RADIUS Vendors and VSA Sets, page C-17](#).

## 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.

ACS for Windows: You use the **CSUtil.exe** command. For details, see [Posture-Validation Attributes, page C-29](#).

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).

## 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 [Configuring Policies, page 13-15](#).
- **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:

- [About Internal Policies, page 13-7](#)
- [About Rules, Rule Elements, and Attributes, page 13-8](#)

## 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 [Classification of Access Requests, page 14-2](#).

For information on configuration, see [Creating an Internal Policy, page 13-17](#), and [Internal Posture Validation Setup Pages, page 13-30](#)

## External Policies

External policies are policies that an external NAC server defines, usually from an antivirus 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 server 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 a 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.

For information on external policy configuration options see [Editing an External Posture Validation Server, page 13-23](#), and [External Posture Validation Setup Pages, page 13-33](#).

# External Posture Validation Audit Servers

This section contains:

- [About External Audit Servers, page 13-9](#)
- [Auditing Device Types, page 13-10](#)
- [Configuring NAC in ACS, page 13-13](#)

## 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. 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 Agentless Host 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 13-2](#) defines the details required in applying the results of an audit.

**Table 13-2** *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 or IP addresses (or both), and groups that are exempt from audit.
<code>inverseExemptionFlag</code>	If this flag is set, the meaning of the exemption list will be inversed. 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 13-2 Audit Policy Requirements (continued)

Audit Policy	Description
staticAttributes	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.
tokenMappings	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 a functioning Cisco Trust Agent 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 exemption lists of groups and hosts. 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.

## Auditing Device Types

As an extra security check on MAC authentication, you can configure an audit policy that checks for device type and handles assignment of the device to an appropriate destination user group. For example, a questionable device might be assigned to a user group called *Mismatch*; or, if the process does not

assign a group, the device might be assigned to a user group called *Quarantine*. In the case where MAC authentication and the audit policy return the same device type, such as printer, your audit policy can assign the device to the printer group.

## Policy Formation

You use options on the External Posture Validation Audit Server Setup page to define the audit policy. These options can enable a request for device-type from the audit server or assign a group in the absence of the device-type. The options on this page also provide for construction of rules that can specifically manage group assignment based on logical comparisons.

The complete audit policy also depends on the elements that you have previously configured on the External Posture Validation Server Setup page, which include setup of the host(s), audit server(s), and audit flow. In addition, the policy includes an option for configuration of a secondary audit server that can function in a failover scenario.

ACS uses the **GAME** protocol in a conversation with an audit server. The conversation includes a request for device type, which the audit server determines by scanning the device. If the protocol or audit policy flows return errors, the system displays an error message.

When configuring policy, remember that:

- ACS does not allow configuration of this feature for vendors who do not have the device-type attribute. Qualys is the only vendor tested against this attribute and currently supporting it.
- If an audit server does not return a device-type attribute, policy evaluation continues as though the attribute was not requested.
- ACS logs the device-type attribute in the Passed and Failed logs.

## User Groups and Device Types

MAC authentication returns a device type in the form of a user group, such as Printer or PC. Audit policy relies on a list of NAC attribute device definitions, which include Printer and PC, for comparison with the MAC user group. Alternatively, the audit policy can rely on a user-defined device-type string.

When looking at the MAC user group, the policy supports a user group of *Any*, which ACS interprets to mean that the group returned can be any group or no group. When looking at the device type, the policy supports **Match-all** when interpreting the device type returned by the audit.

## Group Assignment

Group assignment depends on the configuration of your network. Your network might support multiple devices or only certain devices. To support the audit policy, you should add a destination device group such as **Mismatch** or **Quarantine**. Your particular configuration might require additional groups.

Assignment to a destination user group is based on the following conditions:

- **Device-Type Returned**—Group assignment is based on a rule that compares a MAC device type with a NAC device-type attribute.
- **No Device-Type**—Group assignment is based on a group that you chose.
- **No Device-Type or Group**—Group assignment is based on a group that you chose.
- **No Token or Group**—Group assignment is based on the Fail Open Configuration, which contains a posture token, timeout, and group. In the absence of a Fail Open Configuration, the system returns an error.

## Group Mapping Rules

Each group-mapping rule uses an operator, which compares the device user group that MAC authentication returns with the device type that an audit server returned. Any one of the following operators can be defined in a comparison:

- Match all device types (ACS performs a wildcard match on all device types)
- Device type equals
- Device type does not equal
- Contains
- Starts with
- Regular expression

For example:

- If group equals *printers* and device-type not equals *Printer* assign group *Mismatch* (or *Quarantine*).
- If group equals *NotKnown* and device-type equals *Printer* assign group *printers*.
- If group equals *embedded-os* and device-type not equals *Printer* assign group *quarantine*.
- If group equals *Any* and device-type equals *PC* assign group *reject* (maybe this is a LAN where the admin does not allow computers).
- If group equals *Any* and device-type equals *unknown* assign *quarantine*.

## Policy List

Each rule definition appears on a list of policies that is orderable by priority.

## Layer 2 Audit for Network Access Control

ACS first admits the device to a quarantined network, where the device can receive an IP address. The audit cannot begin until the device has received the IP address. When the audit begins, the audit is the same as an audit of a Layer 3 (L3) host.

The NAD must be pre-configured to learn the host's IP address. Then ACS responds to an initial access-request with a notification to the NAD to issue another access-request when the NAD has learned the IP address. If the NAD does not learn the host's IP address, ACS invokes a failure condition, and policy flow follows the audit fail-open policy. Using the audit fail-open policy, administrators can choose to reject the user, or assign a posture token and an optional user-group.

Audit policy can serve as a backup verification when MAC Authentication Bypass (MAB) fails. The audit policy tests whether MAB failed by applying policy conditions that test the ACS user group assigned to the current session. For example, you can test whether the user-group is equal to the user-group that MAB assigns to failed authentications, and, if so, only then continue the audit.

For configuration information, see [Chapter 14, "Network Access Profiles"](#).

# 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**

To design your posture policies, click the Posture Validation tab. You can assign those policies to profiles by clicking 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 [Posture Validation in Network Access Control, page 13-2](#).

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 9-22](#). For detailed steps about generating and installing a self-signed certificate, see [Generating a Self-Signed Certificate, page 9-35](#).

**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).

You must add your audit vendor to the ACS internal dictionary.

ACS for Windows: You use the **CSUtil.exe** command before configuring an external posture validation audit server. For detailed instructions, see [Importing External Audit Posture-Validation Servers, page C-34](#).

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).

**Note**

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 9-28](#).

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

**Step 3**

On the Advanced Options page, check the check box for **Microsoft Network Access Protection Settings**.

**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 10-24](#).

**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 10-24](#).

**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 9-21](#).

**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 3-12](#).

**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 [Workflow for Configuring NAPs and Profile-based Policies, page 14-3](#).




---

**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 5-41](#).

---

**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, RACs, or both that limit network access appropriately.

For detailed steps on creating rules, see [Creating an Internal Policy, page 13-17](#). For detailed steps, see [Adding a Downloadable IP ACL, page 4-15](#) (and [Adding RADIUS Authorization Components, page 4-10](#).) To associate posture rules to profiles, see [Posture-Validation Policy Configuration for NAPs, page 14-29](#).

**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:

- Create a policy and its associated rules, including configuring mandatory credential types and policies.

For detailed steps, see [Configuring Policies, page 13-15](#).

- Use **Network Access Profiles** to assign posture validation policies to profiles to validate your endpoint devices.

For detailed steps, see [Posture-Validation Policy Configuration for NAPs, page 14-29](#).

---

## Configuring ACS in a NAC/NAP Environment

ACS 4.2 provides configuration options that you can use to configure ACS to work in a Cisco Network Access Control and Microsoft Network Access Protection (NAC/NAP) environment:

- Configuration of External AAA servers  
In the Microsoft NAP environment, these are NAP servers that send Statements of Health (SoHs) to ACS or other AAA servers. You can configure ACS to grant or deny access or levels of access based on processing of the SoHs. For more information on configuring external AAA servers, see [Setting Up an External AAA Server, page 13-23](#).
- Configuration of Statement of Health Posture Validation Rules  
You can set up SoH posture validation rules to enable ACS to make decisions about user access based on SoH attributes. For more information on setting up SoH posture validation rules, see [Setting a Posture-Validation Policy to Process Statements of Health, page 14-32](#).

**Note**

For detailed information on configuring ACS for a NAC/NAP environment, see Chapter 9 of the *Configuration Guide for Cisco Secure ACS, 4.2*, “NAC/NAP Configuration Scenario.”

---

## 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.

This section contains:

- [Posture Validation Options, page 13-15](#)
- [Setting Up Posture Validation Policies, page 13-16](#)
- [Setting Up an External Policy Server, page 13-22](#)
- [Setting Up an External Audit Posture Validation Server, page 13-25](#)
- [Audit Processing with MAC Authentication Bypass, page 13-27](#)

## Posture Validation Options

You can configure the following posture validation options:

- Internally within ACS. See [Setting Up Posture Validation Policies, page 13-16](#).
- 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 13-22](#).
- 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 13-25](#).

[Table 13-3](#) describes the setup options for posture validation.

Table 13-3 Posture Validation Options

Component	Description	Notes
Internal Posture Validation	Policy requirements for the network are internally (or locally) validated in ACS.	NAC policies for the Cisco Trust Agent, Windows, the CSA, and antivirus software applications are among recommended internal policies. See <a href="#">Creating an Internal Policy, page 13-17</a>
External Posture Validation	An outside posture validation server validates policies.	Externalizing the posture validation to an AV server allows you to handle proprietary AV posture credentials and antivirus policy administration by an AV administrator separate from the ACS administrator.
External Audit Posture Validation	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 Cisco Trust Agent. If no Cisco Trust Agent 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 13-7](#) or [Creating an Internal Policy, page 13-17](#)
  - **External Posture Validation Setup**—See [External Policies, page 13-8](#) or [Setting Up an External Policy Server, page 13-22](#)
  - **External Posture Validation Audit Setup**—See [External Posture Validation Audit Servers, page 13-9](#) or [Setting Up an External Audit Posture Validation Server, page 13-25](#)
- Step 3** Complete the required steps to set up internal or external posture validation.
- 

## Setting Up Posture Validation Policies

This section contains:

- [Creating an Internal Policy, page 13-17](#)
- [Cloning a Policy or Policy Rule, page 13-20](#)
- [External Posture Validation Audit Servers, page 13-9](#)

- [Editing a Policy, page 13-19](#)
- [Deleting a Policy or Rule, page 13-21](#)

## 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 [Configuring Policies, page 13-15](#).

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 [Posture-Validation Policy Configuration for NAPs, page 14-29](#).

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 13-20](#).

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** For each condition set that you want to add to the rule:
    - a. Select an attribute. For more information about attribute types, see [Posture Validation Attribute Data Types, page 13-6](#).
    - b. Select an entity (only available for extended attributes).
    - c. Select an operator.
    - d. Type a value.
    - e. Click **Enter** and then **Submit**.

For example, if you create a policy for the 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 [Configuring Policies, page 13-15](#).

For information on the Cisco Trust Agent posture plug-in attributes and values, see the Cisco Trust Agent documentation.

The condition set appears in the Conditions Sets table.

**Step 7** 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.

**Step 8** 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**.

**Step 9** For the new rule, do each of the following:

- a. Select a credential type.
- b. Select a token.
- c. Type an action (in the form of a notification string).

For more information about tokens, see [Posture Tokens, page 13-3](#).

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 10** 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 11** 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 12** Configure the Default Rule at the bottom of the Posture Validation Rules page by clicking **Default**:

- a. Select a credential type.
- b. Select a token.
- c. 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 13** Click **Submit**.  
The Posture Validation Rules page displays the new rule.
- Step 14** Click **Done**.  
The current configuration has been changed.
- Step 15** 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:
    - a. Select the condition element.
    - b. Click **Remove**.
    - c. Update its attribute, entity, operator, or value; then click **Enter**.
  - c. To add a new condition:
    - a. 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 13-21](#).
  - f. To move a rule:
    - a. Select the rule by clicking the button to the left of the rule.
    - b. 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 13-17](#).

---

- 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:
- a. In the navigation bar, click **Posture Validation**.



- 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 choose 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 [Classification of Access Requests, page 14-2](#).

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 [Configuring Policies, page 13-15](#).

- 
- Step 1** After you choose **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. Check 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 [Configuring Policies, page 13-15](#).
- Step 5** (Optional) In the **Secondary Server configuration** pane:
- a. Check 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 [Configuring Policies, page 13-15](#).

- 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 AAA Server

This procedure describes how you can create an external policy that uses an external AAA server.

### Before You Begin


You can choose 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 [Classification of Access Requests, page 14-2](#).

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

For descriptions of the options available on the External Policy Configuration page, see [Configuring Policies, page 13-15](#).

You can also set up an external AAA server that is used to evaluate SoHs from networks that include Microsoft Vista clients (NAC/NAP networks).

To set up an external posture validation server:

- 
- Step 1** After you choose **External Posture Validation Setup**, the External Posture Validation Servers page displays.
- Step 2** Under the External Posture AAA Servers table, click **Add Server**.  
The Add/Edit External Posture AAA 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. Check the **Primary Server configuration** check box.
-  **Note** If you do not choose the **Primary Server Configuration** check box, ACS uses the secondary server configuration. If no secondary server configuration exists or the secondary server is unreachable, ACS rejects the posture validation request.
- 
- b. Provide configuration details about the primary external AAA server. For more information about the boxes and list in this area, see [Configuring Policies, page 13-15](#).
- Step 5** (Optional) In the **Secondary Server configuration** pane:
- a. Check the **Secondary Server configuration** check box
  - b. Enter configuration details about the secondary external AAA server. For more information about the boxes and list in this area, see [Configuring Policies, page 13-15](#).
- Step 6** Determine the forwarding attributes to send to the primary or secondary external server by moving the available forwarding attributes to the chosen forwarding attributes 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 AAA Server

You can edit an external posture AAA 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 AAA Server page appears.
- Step 4** Edit the fields and click **Submit**.
-

## Deleting an External Posture AAA 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 AAA Server page appears.
- Step 4** Click **Delete**.
- 

## Setting Up an External Audit Posture Validation Server

Use External Posture Validation Audit Server Setup page to add, edit, and delete external posture validation audit servers. Policies are reusable; you can associate an audit policy with more than one network access profile.

ACS does not include any non-Cisco attributes by default. Therefore, you must import a NAC Attribute Definition File (ADF) from each vendor application that you would like to validate in your NAC posture-validation policies. You can use the attributes that you add to create conditions for internal policies.

NAC introduces the ability to authorize network hosts not only based on user or machine identity; but also on a host's posture validation. The posture validation is determined by comparing the host's credentials to a posture-validation policy that you create from attribute-value pairs (AVPs), which Cisco and other vendors who are NAC partners define. Since the range of NAC attributes extends across many vendors and applications, you must import the non-Cisco attributes.

### Before You Begin

Before you begin, you must:

- Add your audit vendor to the ACS internal dictionary.

ACS for Windows: You use the **CSUtil.exe** command. For detailed instructions, see [Importing External Audit Posture-Validation Servers, page C-34](#).

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).

- Define destination user groups. See [Auditing Device Types, page 13-10](#).
- Configure RACs, if needed. See [RADIUS Authorization Components, page 4-6](#).

## Adding an External Posture Validation Audit Server

To add an audit server for external posture validation:

- 
- Step 1** Click **Posture Validation** in the navigation bar.  
The Posture Validation Components Setup page appears.

- Step 2** Click **External Posture Validation Audit Setup**.  
The External Posture Validation Audit Server page appears.
- Step 3** Click **Add Server**.  
The External Posture Validation Audit Server Setup page appears.
- Step 4** Type the **Name** that identifies the audit policy. See [Table 13-13 on page 13-37](#) for complete information on all options in this procedure.
- Step 5** Type a **Description** of the audit policy.
- Step 6** Select the appropriate options in the **Which Groups and Hosts are Audited** area. If necessary, identify hosts by using IP and MAC addresses.
- Step 7** Choose a **Posture Token**.
- Step 8** Choose an **Audit Server Vendor** in the **Use These Audit Servers** area.
- Step 9** Check the **Primary Server Configuration** option to configure a primary server.
- Step 10** Provide the configuration information for the primary server.  
If your audit vendor does not appear, you must define an audit APT for the vendor in the internal ACS dictionary.  
ACS for Windows: You use the `CSUtil.exe` command. For detailed instructions, see [Posture-Validation Attributes, page C-29](#).  
ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).
- Step 11** Check the **Secondary Server Configuration** option to configure a secondary server.
- Step 12** Provide the configuration information for the secondary server.
- Step 13** Choose a temporary posture token from the drop-down list in the **Audit Flow Settings** area.
- Step 14** Choose a timeout option.
- Step 15** Type a polling interval.
- Step 16** Choose the **Maximum amount of times the Audit Server should be polled**.
- Step 17** Type a **Policy string to be sent to the Audit Server**.
- Step 18** Check the **Request Device Type from Audit Server** option in the **Audit Policy** area if you want to cross-check the device types that the audit server and MAC authentication return.  
If this check box is not available (greyed out), define an audit device type attribute for the vendor in the internal ACS dictionary.  
ACS for Windows: You use the `CSUtil.exe` command. See [Posture-Validation Attributes, page C-29](#) for information.  
ACS SE: You use the NAC Attributes Management page in the web interface. See [NAC Attribute Management \(ACS SE Only\), page 8-44](#) for more information.
- Step 19** Check the **Assign This Group if Audit Server Did not Return a Device-Type** option if you want to configure a default destination group.
- Step 20** Click **Add** to add a device-type feedback rule.
- Step 21** Choose a device type.
- Step 22** Choose the **User Group** that will be initially compared with the device type that MAC authentication returned.

- Step 23** Complete the **Device Type** comparison logic by choosing an operator and a device type. If the device type does not appear in the drop-down box, type a device type in the text box.
- Step 24** Choose the user group that ACS will assign based on the outcome of the device type comparison logic.
- Step 25** 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**.
- 

## Audit Processing with MAC Authentication Bypass

An audit request can include a check against Agentless Host authentication. Audit server processing can double-check an audit request against a MAB authentication policy and an audit policy, and then combine the evaluation of the two policies.

Evaluating the combined policies is only possible in Layer 2 IP and Layer 3 NAC deployments because the audit request must contain the MAC address and IP address of an endpoint.

ACS requires the following key attributes for MAB and audit interoperability:

- [10] Service-type = 10

- [31] Calling-Station-ID = Endpoint *MAC Address*
- [8] Framed-IP-Address = Endpoint *IP address*
- [26:9:1] Cisco-AV-Pair = audit-session-id = *Id*
- [26:9:1] Cisco-AV-Pair = aaa:service = ip\_admission

## Workflow

This feature requires the following configuration options:

- A NAP using the Agentless Host template
- MAB authentication
- External posture validation audit
  - A GAME group feedback policy
  - User groups that will be audited
- Association of the audit serve with the network access profile

## Processing

When the request is processed:

1. The audit request is evaluated against the Agentless Host policy.
2. The Agentless Host policy assigns a user group for the audit request.
3. The audit policy compares the assigned user group to its configured set of groups.
4. If the assigned group matches the configured set of groups, a GAME request is generated and the response is processed. If the assigned group does not match, a GAME request is not generated.
5. If there is a match, the authorization policy is processed and the resulting audit response is sent to the originating network access device.

## Policy Configurations

ACS supports a number of configurations and capabilities for authenticating and authorizing agentless hosts. [Table 13-4](#) summarizes the policy combinations, capabilities, and configurations.

**Table 13-4 Agentless Host Authentication and Authorization Support**

Use Case	Audit				Authorization Based On	
	MAB	Grp Filter	Posture	Device Type	Token	Group from
MAB only.	Y	N	N	N	N	MAB
Audit for posture only.	N	N	Y	N	Y	None
Audit for posture and device type only. For example, differentiated azn based on the device type.	N	N	Y	Y	Y	None* or device type

Table 13-4 Agentless Host Authentication and Authorization Support (continued)

Use Case	Audit				Authorization Based On	
	Description	MAB	Grp Filter	Posture	Device Type	Token
MAB and audit for posture. For example, even if MAB fails, healthy can be assigned.	Y	N	Y	N	Y	MAB
MAB and audit for posture and device type. For example, even if the MAC is not authenticated, printers get in.	Y	N	Y	Y	Y	MAB or device type
MAB and audit for posture. MAB success is mandatory. There is no need to audit if the MAC is not authenticated.	Y	Audit all but MAB failure group	Y	N	Y	MAB
MAB, Audit for posture and device type. MAB success is mandatory. There is no need to audit if the MAC is not authenticated.	Y	Audit all but MAB failure group	Y	Y	Y	MAB or device type
MAB, but if the MAC is not authenticated, then audit for posture. For example, MAB or a healthy token can be admitted to the network.	Y	Audit only MAB failure group	Y	N	Y	MAB
MAB, but if the MAC is not authenticated, audit for posture and device type. For example, managed devices are admitted to the network. Otherwise, azn is based on the device type or a token.	Y	Audit only MAB failure group	Y	Y	Y	MAB or device type

\*In this case, group assignment depends on matching a device. Without matching, the group assignment policy for device types does not produce a user group.

You use the following procedure to configure Agentless Hosts and Audit interoperability.

- 
- Step 1** In the navigation bar, click **Network Access Profiles**.
  - Step 2** Click **Add Template Profile**.
  - Step 3** Type a Name and Description for the profile.
  - Step 4** Select the **Agentless Host** template.
  - Step 5** Check **Active** to activate the profile, or leave it inactive.
  - Step 6** In the navigation bar, click **Network Access Profiles**.
  - Step 7** In the Protocols for the agentless host <profile\_name>, check **Allow Agentless Request Processing**.
  - Step 8** In Authentication for the agentless host <profile\_name>, fill in the **Authenticate MAC With** section. See [Agentless Request Processing, page 14-24](#).
  - Step 9** In the navigation bar, click **Posture Validation** and select External Posture validation Audit Setup.
  - Step 10** Set up the Game Group Feedback Features. See [“Adding an External Posture Validation Audit Server” procedure on page 13-25](#).
  - Step 11** Associate the Audit server to the Network Access Profile. See [Configuring Posture Validation for Agentless Hosts, page 14-33](#).
-

## Posture Validation Pages Reference

The following topics describe the pages that you access from the **Posture Validation** button on the navigation bar:

- [Posture Validation Components Setup Page](#), page 13-30
- [Internal Posture Validation Setup Pages](#), page 13-30
- [External Posture Validation Setup Pages](#), page 13-33
- [External Posture Validation Audit Setup Pages](#), page 13-36

### Posture Validation Components Setup Page

Use this page to access the posture validation pages.

To display the Posture Validation Components Setup page, click **Posture Validation** on the navigation bar.

**Table 13-5** Posture Validation Components Setup Page

Option	Description
Internal Posture Validation Setup	Opens the Posture Validation Policies page. Internal policies contain rules that determine the posture token that ACS applies to a posture validation request.
External Posture Validation Setup	Opens the External Posture Validation Servers page. ACS forwards credentials to external posture validation servers, and the server then returns a posture token.
External Posture Validation Audit Setup	Opens the External Posture Validation Audit Server page. Audit servers return posture information for agentless hosts.

### Internal Posture Validation Setup Pages

The following topics describe the Internal Validation Setup pages:

- [Posture Validation Policies Page](#), page 13-30
- [Posture Validation Policy Page](#), page 13-31
- [Posture Validation Rules for <policy\\_name> Page](#), page 13-31
- [Posture Validation Rule - <policy\\_name> Page](#), page 13-32
- [Add/Edit Condition Page](#), page 13-33

### Posture Validation Policies Page

Use this page to add policies or to access existing policies for editing.

To display the Posture Validation Policies page, click **Posture Validation** on the navigation bar, then choose **Internal Posture Validation Setup**.

**Table 13-6** Posture Validation Policies Page

Option	Description
<b>Posture Validation Policies</b>	The Name and Description identify the policy. The Policy Details list the rules associated with the policy, by ID number.
Name <policy_name>	Opens the Posture Validation Policy page for editing.
Add Policy	Opens the Posture Validation Policy page for creation of a new policy.

## Posture Validation Policy Page

Use this page to specify the name and description for a new policy.

To display the Posture Validation Policy page, choose **Posture Validation > Internal Posture Validation Setup > Add Policy**.

**Table 13-7** Posture Validation Policy Page

Option	Description
Name	Defines the policy name. The name should be descriptive because the Descriptions do not appear when a policy name is selected.  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 (,), or the slash (/).
Description	Provides a text description of the policy, up to 255 characters.  Because the same policy can apply to more than one profile, a useful description helps to prevent accidental configuration errors when someone modifies a policy without understanding the servers that use it.
Submit	Opens the Posture Validation Rules for <policy_name> page, where <policy_name> is the name of the new policy.

## Posture Validation Rules for <policy\_name> Page

Use this page to display and order rules.

To display the Posture Validation Rules for <policy\_name> page when editing a rule, choose **Posture Validation > Internal Posture Validation Setup > <policy\_name>**.

Table 13-8 Posture Validation Rules for &lt;policy\_name&gt; Page

Option	Description
Posture Validation Rules for <Name>	Lists each rule by ID number. Provides the rule Conditions and Actions (as Posture Token and Notification String). The Description (if specified) provides information about the policy.
Condition <condition_name>	<p>Opens the Posture Validation Rule - &lt;policy_name&gt; page, where you can edit an existing condition.</p> <p>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.</p> <p>Under the 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.</p>
Add Rule	Opens the Posture Validation Rule - <policy_name> page where you can create a rule.
Up, Down	Moves a selected rule. Submits the sort order to the database.
Rename	Opens the Posture Validation Policy page where you can rename the policy.
Clone	Creates a policy identical to a selected policy. Edit the cloned policy to create a new policy.
Delete	Deletes a policy.
Done	Opens the Posture Validation Policies page.

## Posture Validation Rule - <policy\_name> Page

Use this page to view and edit rules.

To display the Posture Validation Rules for <policy\_name> page when adding a rule, choose **Posture Validation > Internal Posture Validation Setup > <policy\_name> > <condition>**.

Table 13-9 Posture Validation Rule - &lt;policy\_name&gt; Page

Option	Description
Condition Sets	<p>Lists the condition sets that are associated with a rule. A &lt;condition_name&gt; opens the Add/Edit Condition page.</p> <p>When adding or editing a rule, a compound Boolean expression determines the logical treatment of the conditions that are associated with a rule.</p> <ul style="list-style-type: none"> <li>Match OR inside Condition and AND between Condition Sets—Provides a less strict treatment of conditions.</li> <li>Match AND inside Condition and OR between Condition Sets—Provides a more strict treatment of conditions.</li> </ul>
Add Condition Set	Opens the Add/Edit Condition page.

**Table 13-9** Posture Validation Rule - *<policy\_name> Page* (continued)

Option	Description
Posture Token	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 <a href="#">Posture Tokens, page 13-3</a> .
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.

## Add/Edit Condition Page

Use this page to add or edit conditions.

To display the Posture Validation Rules for *<policy\_name>* page when adding a rule, choose **Posture Validation > Internal Posture Validation Setup > <policy\_name> > <condition> > <condition\_set>**.

**Table 13-10** Add/Edit Condition Page

Option	Description
Condition Elements Table	Lists each 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, the Cisco Trust Agent appears on the list as <code>CISCO:PA</code> . For more information about credential types, see <a href="#">About Posture Credentials and Attributes, page 13-5</a> .
Attribute	Lists the available attributes.
Entity	Lists the available entities for attributes that require entities.
Operator	Lists the appropriate operators for this attribute.
Value	Specifies an appropriate value for the attribute.

## External Posture Validation Setup Pages

The following topics describe the External Posture Validation Setup pages:

- [External Posture Validation Servers Page, page 13-33](#)
- [Add/Edit External Posture Validation Server Page, page 13-34](#)

## External Posture Validation Servers Page

Use this page to view existing external posture validation servers.

To display the External Posture Validation Servers page, choose **Posture Validation > External Posture Validation Setup**.

**Table 13-11 External Posture Validation Servers Page**

Option	Description
Name	Opens the Add/Edit External Posture Validation Server page for editing of an existing policy. Description, Forward Credential Type, and Server Details show the current configuration of the policy.
Add Server	Opens the Add/Edit External Posture Validation Server page for creation of a new policy.

## Add/Edit External Posture Validation Server Page

Use this page to add or edit external posture validation servers.

To display the Add/Edit External Posture Validation Server page, choose **Posture Validation > External Posture Validation Setup**. Then click **Add Server** to add a server or click `<server_name>` to edit a server.

**Table 13-12 Add/Edit External Posture Validation Server Page**

Option	Description
Name	Specifies the name by which to identify the server.  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 (,), or the slash (/).
Description	Specifies a text description of the server, up to 255 characters. For each profile using the policy, the text you type in the <b>Description</b> box appears beside the policy. In the Description box you can add the 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.
Primary Server Configuration Secondary Server Configuration	Enables a primary NAC server (and an optional secondary NAC server). ACS relies on these servers to apply the policy and configure the set of credential types that ACS forwards.  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.

Table 13-12 Add/Edit External Posture Validation Server Page (continued)

Option	Description
URL	<p>Specifies the HTTP or HTTPS URL for the server. The format for URLs is:</p> <pre>[http[s]://]host[:port]/resource</pre> <p>where <i>host</i> is the hostname or IP address of the NAC server, <i>port</i> is the port number used, and <i>resource</i> is the rest of the URL, as required by the NAC server itself. The URL varies depending on the server vendor and configuration. For the URL that your NAC server requires, refer to your NAC server documentation.</p> <p>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 <code>https://</code> and import a self-generated CA certificate into ACS for this policy server. See <a href="#">ACS Certificate Setup, page 9-22</a>.</p> <p>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.</p> <p>If the NAC server hostname is <i>antivirus1</i>, which uses port 8080 to respond to HTTP requests for the service provided <i>policy.asp</i>, a script kept in a web directory called <i>cnac</i>, valid URLs would be:</p> <pre>http://antivirus1:8080/cnac/policy.asp antivirus1:8080/cnac/policy.asp</pre> <p>If the same server used the default HTTP port, valid URLs would be:</p> <pre>http://antivirus1/cnac/policy.asp http://antivirus1:80/cnac/policy.asp antivirus1/cnac/policy.asp antivirus1:80/cnac/policy.asp</pre> <p>If the same server used HTTPS on the default port, valid URLs would be:</p> <pre>https://antivirus1/cnac/policy.asp https://antivirus1:443/cnac/policy.asp</pre>
Username	Specifies the username required for access to the server. The server ignores the values in the Username and Password fields if the server is not password protected.
Password	Specifies the password required for access to the server. The server ignores the values in the Username and Password fields if the server is not password protected.
Timeout (Sec)	<p>The number of seconds that ACS waits for a result from the external server, including domain name resolution. The Timeout value must be greater than zero (0). The default is 10.</p> <p>ACS forwards requests to the secondary server (if configured) when the primary server times out. If no secondary server is configured or if a request to the secondary server also times out, ACS cannot apply the external policy and therefore rejects the posture validation request.</p> <p>For each posture validation request, ACS always tries the primary server first, regardless of whether previous requests timed out.</p>

Table 13-12 Add/Edit External Posture Validation Server Page (continued)

Option	Description
Trusted Root CA	<p>The certificate authority (CA) that issued the server certificate, which the server uses. 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.</p> <p>The Trusted Root CA list does must contain the CA that issued a NAC server certificate. For information, see <a href="#">Adding a Certificate Authority Certificate, page 9-26</a>.</p> <p>ACS does not check NAC server certificates against Certificate Revocation Lists (CRLs), even if a configured CRL issuer for the CA of the NAC server certificate is present.</p> <p>The certificate name and type must match. 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.</p>
Forwarding Credential Types	<p>The Available Credentials list specifies the credential types that <i>are not</i> sent to the external server. The Selected Credentials list contains the credential types that <i>are</i> sent to the external server.</p> <p>See the following information to add credential types to the Available Credentials list. ACS for Windows: You use the <b>CSUtil.exe</b> command. For detailed instructions, see <a href="#">Importing External Audit Posture-Validation Servers, page C-34</a>.</p> <p>ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see <a href="#">NAC Attribute Management (ACS SE Only), page 8-44</a>.</p>

## External Posture Validation Audit Setup Pages

The following topics describe the External Posture Validation Audit Setup pages:

- [External Posture Validation Audit Server Page, page 13-36](#)
- [External Posture Validation Audit Server Setup Page, page 13-36](#)

### External Posture Validation Audit Server Page

Use the External Posture Audit Server page view the name, description, server details, and current posture tokens for each configured server.

To display the Add/Edit External Posture Validation Server page, choose **Posture Validation > External Posture Validation Audit Setup**.

### External Posture Validation Audit Server Setup Page

Use this page to add or edit external posture validation audit servers.

#### Add Server Page

To display this page, choose **Posture Validation > External Posture Validation Audit Setup > Add Server**.

**Edit Server Page**

To display this page, choose **Posture Validation > External Posture Validation Audit Setup**, then click the `<server_name>`. You can edit the Audit Server settings as needed, but:

- If the audit policy is associated with more than one NAP, changes to the policy affect posture validation for each associated NAP.
- If you change the name of a policy, you are creating a new policy when you click **Submit**. You cannot rename a policy and change the settings of an existing policy at the same time.

**Table 13-13 External Posture Validation Audit Server Setup Options**

Option	Description
Name	The name for the audit policy.  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 (,), or the slash (/).
Description	Describes the audit policy (up to 255 characters).
<b>Which Groups and Hosts are Audited</b>	
Audit all user groups Audit these user groups Do not audit these user groups	The user group options determine the auditing of the groups in the Selected Groups list.
Audit all hosts Audit these hosts Do not audit these hosts	Audit all hosts that do not contain a posture agent.  Audit only certain hosts or exclude certain hosts as defined in the Host IP Addresses and Ranges (IP/MASK) (comma-separated values) field.  For Host MAC Address (comma-separated values), ACS accepts two MAC address formats, <code>00-0D-60-FB-16-D3</code> or <code>000D.60FB.16D3</code> . MAC prefixes that serve as ranges are acceptable. For example, <code>00-0D-60-FB-16</code> or <code>000D.60</code> would match any MAC address that begins with these bytes.  MAC prefixes must contain an even number of hexadecimal digits.  MAC address matching is case sensitive.
Select a Posture Token for the hosts that will not be audited	A posture token that ACS will apply to hosts that are not audited.
<b>Use These Audit Servers</b>	
Audit Server Vendor	Vendors that have an audit Application Posture Token (APT) defined in the internal ACS dictionary appear in the drop-down list.  If no audit servers appear in the drop-down list, see <a href="#">Posture-Validation Attributes, page C-29</a> (ACS for Windows) or <a href="#">NAC Attribute Management (ACS SE Only), page 8-44</a> . for information on setting up audit servers.
Primary Server Configuration, Secondary Server Configuration	Each option enables configuration of audit servers. ACS requires a primary server. The secondary server provides failover capability (not required). The options for a Secondary Server Configuration are identical to the options for a Primary Server Configuration.

Table 13-13 External Posture Validation Audit Server Setup Options (continued)

Option	Description
URL	<p>The URL of the audit server. Specify the HTTP or HTTPS protocol.</p> <p>URLs must conform to the following format:</p> <pre>[http[s]://]host[:port]/resource</pre> <p>where host is the hostname or IP address of the external server, port is the port number used, and resource is the rest of the URL, as required by the external server. The URL varies depending on the server vendor and configuration.</p> <p>The audit server documentation contains specific format guidelines.</p>
Username	The username that the audit server requires.
Password	The password that the audit server requires.
Timeout (sec)	The number of seconds that ACS waits for a result from the audit server, including domain name resolution. The Timeout value must be greater than zero (0).
Trusted Root CA	A certification authority that is required if the URL of the audit server specifies the HTTPS protocol. This option should match the certification authority that issued the audit server certificate installed on the primary server.
Validate Certificate Common Name	When checked (enabled), this option shows the host name within the URL for purposes of comparison with the common name in the certificate. If the names do not match, ACS closes the SSL connection, posture validation fails, and user access is denied.
<b>Audit Flow Settings</b>	
Use this Posture Token while Audit Server does not yet have a posture validation result	Interim posture token sent from ACS to the NAD while waiting for a result. ACS uses the In Progress token before the Audit Server determines the actual posture of the nonresponsive host.
Polling Intervals and Session-Timeout	Either the timeout values that are sent by the audit server or that are set in the authorization policy. ACS requires a polling interval if the configuration uses the values that are set in the authorization policy. The authorization policy must include the necessary RACs in order to assign specific timeout values in the final resulting tokens. See <a href="#">Configuring an Authorization Rule, page 14-36</a> .
Maximum amount of times the Audit Server should be polled	The maximum number of times that ACS will query the audit server for a result (posture token). Range of 1–10 times.
Policy string to be sent to the Audit Server	The name of the policy, if the audit server supports named policy invocation.
<b>GAME Group Feedback</b>	
Request Device Type from Audit Server	<p>Enables the audit policy configuration options. When enabled, the Audit feature can request a device type from the audit server and then check the device type against the device type that MAC authentication returns.</p> <p>If this check box is not available, define an audit device type attribute for the vendor in the internal ACS dictionary.</p> <p>ACS for Windows: Use the CSUtil.exe command. See <a href="#">Posture-Validation Attributes, page C-29</a> for information.</p> <p>ACS SE: Use the NAC Attributes Management page in the web interface. See <a href="#">NAC Attribute Management (ACS SE Only), page 8-44</a> for more information.</p>

**Table 13-13 External Posture Validation Audit Server Setup Options (continued)**

Option	Description
Assign This Group if Audit Server Did not Return a Device Type	Enables assignment of a device to any administrator-defined group when the audit server does not return a device type.
User Group	Lists all user groups, including Any. The device type that MAC authentication returns is initially compared with this list of device types.
Device Type	<p>Defines the comparison criteria for the User Group, using an operator and device type.</p> <p>Valid values for the operator are:</p> <ul style="list-style-type: none"> <li>match-all</li> <li>=</li> <li>!=</li> <li>contains</li> <li>starts-with</li> <li>regular-expression</li> </ul> <p>Valid values for the device type drop-down are not editable. They include:</p> <ul style="list-style-type: none"> <li>Printer</li> <li>IP Phone</li> <li>Network Infrastructure</li> <li>Wireless Access Point</li> <li>Windows</li> <li>Unix</li> <li>Mac</li> <li>Integrated Device</li> <li>PDA</li> <li>Unknown</li> </ul> <p>Type a device type in the text box if the device type drop-down does not contain a particular device.</p>
Assign User Group	A drop-down list of administrator-defined user groups. If the comparison of the initial User Group with the Device Type succeeds, ACS will assign this user group.
Add, Delete, Up, Down	Controls that affect the user groups.
Submit, Delete, Cancel	<p>Controls that affect the whole policy.</p> <p>An audit policy can be in use with more than one NAC Network Access Profile. Before deleting a policy, you must identify the NAC Network Access Profiles that the deletion will affect.</p>

