



# Network Admission Control

---

NAC enables you to control the degree of access permitted from computers accessing your network through a AAA client configured to enforce NAC. The basis of NAC is the validation of the posture, or state, of computers on a network. The role of Cisco Secure Access Control Server (ACS) for Windows Server in NAC is to perform posture validation.

This chapter contains the following topics:

- [About Network Admission Control, page 14-1](#)
- [Implementing Network Admission Control, page 14-5](#)
- [NAC Databases, page 14-10](#)
- [NAC Policies, page 14-16](#)

## About Network Admission Control

This section contains the following topics:

- [NAC AAA Components, page 14-2](#)
- [Posture Validation, page 14-3](#)
- [Posture Tokens, page 14-4](#)
- [Non-Responsive NAC-Client Computers, page 14-5](#)

## NAC AAA Components

The following list defines the components of the NAC AAA paradigm. [Posture Validation, page 14-3](#), describes the posture validation process in which these components are used.

- **NAC-client computer**—A computer running NAC software, as follows:
  - **NAC client**—The NAC client is the Cisco Trust Agent (CTA) application. CTA collects data directly from the computer and from any NAC-compliant applications installed on the computer. It uses this data to create a set of attributes that contain information about the posture of the computer. These attributes are also called *credentials*. For more information about credentials, see [About NAC Credentials and Attributes, page 14-11](#).
  - **NAC-compliant applications**—Applications that integrate with the NAC client. Examples of such applications are Cisco Security Agent and anti-virus programs from Network Associates, Symantec, or Trend Micro. These applications provide the NAC client with attributes about themselves, such as the version number of a virus definition file.
- **AAA client**—A network access device, such as a router, whose operating system supports NAC.
- **Cisco Secure ACS**—Performs posture validation of the NAC-client computer, using either internal policies, external policies, or both. When external policies are used, Cisco Secure ACS forwards posture validation requests to a NAC server.
- **NAC server**—Performs posture validation of the NAC-client computer when Cisco Secure ACS is configured to use external policies.
- **Remediation server**—Provides support to NAC-client computers needing repairs or updates to comply with network admission requirements.

## Posture Validation

Cisco Secure ACS determines the posture of a computer by using the credentials received from a NAC-client computer. The following list provides an overview of 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. The NAC-client computer sends traffic on the network.
2. The NAC-compliant AAA client receives the traffic and initiates an EAP session, forwarding the EAP identity of the NAC-client computer to Cisco Secure ACS.
3. Cisco Secure ACS initiates a PEAP session with the NAC-client computer, so that all NAC communications are encrypted and trusted.
4. The NAC client sends to Cisco Secure ACS a posture validation request, containing credentials from each NAC-compliant application installed on the computer.
5. Using the received credentials, Cisco Secure ACS does the following:
  - a. Cisco Secure ACS uses the Unknown User Policy to determine which NAC database to use to perform the posture validation, selecting the first NAC database whose mandatory credential types are satisfied by the credentials in the validation request.



---

**Note**

If the Unknown User Policy cannot find a NAC database whose mandatory credential types are satisfied by the credentials in the validation request, Cisco Secure ACS rejects the request.

---

- b. Cisco Secure ACS applies all policies associated with the selected NAC database to derive application posture tokens, which are symbols representing the state of the associated application.
- c. Cisco Secure ACS compares all derived application posture tokens and uses the worst token as the system posture token, which symbolizes the overall posture of the NAC-client computer.
- d. Cisco Secure ACS uses the system posture token and group mappings for the selected NAC database to determine which user group contains the authorizations applicable to the NAC-client computer.

6. Cisco Secure ACS sends the NAC-client computer the system posture token and the results of each policy applied to the posture validation request, and then ends the PEAP session.
7. Cisco Secure ACS sends the AAA client the RADIUS attributes as configured in the mapped user group, including ACLs and attribute-value pairs configured in the Cisco IOS/PIX RADIUS attribute `cisco-av-pair`.
8. Cisco Secure ACS logs the results of the posture validation request. If the request resulted in a system posture token of Healthy, Cisco Secure ACS logs the results in the Passed Authentications log (if it is enabled). Cisco Secure ACS logs in the Failed Attempts log the result of a posture validation request resulting in a posture token of anything other than Healthy.

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

## Posture Tokens

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

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

There are five predefined, non-configurable posture tokens, used for both SPTs and APTs. Listed in order from best to worst, they are as follows:

- Healthy
- Checkup
- Quarantine
- Infected
- Unknown

From the perspective of Cisco Secure ACS, the meaning of an SPT is determined by which groups you map each SPT to and how you configure those groups. In other words, the SPTs for each NAC database are associated with configurable network authorizations.

Posture validation requests resulting in an SPT of Healthy are logged in the Passed Authentications log. Posture validation requests resulting in an SPT of anything other than Healthy are logged in the Failed Attempts log.

Aside from being used to determine the SPT, APTs are not meaningful to Cisco Secure ACS, but the NAC client receiving the results of the posture validation can use them based on their meanings to the relevant NAC-compliant application.

## Non-Responsive NAC-Client Computers

NAC-compliant AAA clients can handle NAC for computers that do not respond to attempts to start a posture validation session with CTA. This occurs if CTA is not installed on the computer or is unreachable for other reasons. To account for this scenario, IOS enables you to define a username and password that it uses for authorization requests on behalf of all non-responsive computers.

In Cisco Secure ACS, you must create the corresponding user account and use one of the following features to control network access for non-responsive computers:

- **Downloadable IP ACLs**—You can create a downloadable IP ACL set that limits sessions originating from all non-responsive computers.
- **Network Access Restrictions**—You can create a non-shared network access restriction that disallows any network access for sessions originating from non-responsive computers.
- **Disabled Account**—You can disable the user account used to assign authorization to non-responsive computers, thus disallowing any network access from non-responsive computers.

## Implementing Network Admission Control

This procedure provides steps for implementing NAC support in Cisco Secure ACS, with references to more detailed procedures for each step.

To implement NAC, follow these steps:

- Step 1** Install a server certificate. Cisco Secure ACS requires a server certificate for NAC because NAC communication with an end-user client is protected by a TLS tunnel. You can use a certificate 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 a Cisco Secure ACS Server Certificate, page 10-35](#). For detailed steps about generating and installing a self-signed certificate, see [Generating a Self-Signed Certificate, page 10-49](#).



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

- Step 2** If you want to validate NAC clients with external policies and the following are both true:
- Cisco Secure ACS uses HTTPS to communicate with external NAC servers.
  - The external NAC servers use a different CA than the CA that issued the Cisco Secure ACS server certificate installed in [Step 1](#)

then you must configure the Certificate Trust List (CTL). For detailed steps, see [Editing the Certificate Trust List, page 10-38](#).

If the CA that issued the server certificates used by the external database servers does not appear on the CTL, you must add the CA. For detailed steps, see [Adding a Certificate Authority Certificate, page 10-37](#).

- Step 3** (Optional) If the Passed Authentications log is not enabled, consider enabling it. Posture validation requests receiving an SPT of Healthy are logged to the Passed Authentications log. You can configure the Passed Authentications log to record useful NAC information, such as posture token-group mapping results. If you enable the Passed Authentications log, be sure to move NAC-related attributes to the Logged Attributes column on the Passed Authentications File Configuration page.

For detailed steps about configuring this type of log, see [Configuring a CSV Log, page 11-19](#).

**Step 4** Configure the Failed Attempts log to include NAC attributes. Posture validation requests receiving an SPT other than Healthy are logged to the Failed Attempts log. Including NAC attributes in this log can help you debug errors in your NAC implementation. For example, a local policy may return a result that you did not anticipate because of errors in the rules that compose the policy. Using the Failed Attempts log, you can see the contents of the attributes received in the request from the NAC client and sent in the reply to the NAC client.

For detailed steps about configuring this type of log, see [Configuring a CSV Log, page 11-19](#).

**Step 5** On the Global Authentication Setup page, enable NAC by selecting “Enable CNAC” under PEAP.

For detailed steps, see [Configuring Authentication Options, page 10-33](#).

**Step 6** If the AAA clients supporting NAC are not already configured in the Network Configuration section, do so now.

For detailed steps, see [Adding a AAA Client, page 4-16](#).

**Step 7** Select the user groups that you want to use for NAC. You are likely to want a separate user group for each possible SPT; therefore, select five user groups. If possible, choose groups that have not been configured to authorize users. Additionally, consider using groups widely separated from groups used to authorize users. For example, assuming that the lowest numbered groups have been used for user authorization, consider using groups 494 through 499.



---

**Tip** To avoid confusion between groups intended to authorize users and groups intended to authorize NAC clients, consider renaming the groups with an easily understood name. For example, if you selected group 499 to contain authorizations related to the Unknown SPT, you could rename the group “NAC Unknown”. For detailed steps, see [Renaming a User Group, page 6-55](#).

---

**Step 8** For each NAC-client configuration (and, therefore, each unique set of credential types) that you want to validate, follow these steps:

- a. Create a NAC database, including configuring mandatory credential types and policies.

For detailed steps, see [Configuring a NAC Database, page 14-14](#).

- b. Create SPT-to-user-group mappings. Each NAC database has its own group mappings.

For detailed steps, see [Configuring NAC Group Mapping, page 17-13](#).

- Step 9** Configure the Unknown User Policy to include NAC databases. When unknown user processing is enabled, Cisco Secure ACS uses the Unknown User Policy to determine if it has a NAC database whose mandatory credential types are satisfied by the attributes received from the NAC client. Of the NAC databases included in the Selected Databases list on the Configure Unknown User Policy page, Cisco Secure ACS uses the first one whose mandatory credential types are satisfied to process the posture validation request.

For detailed steps, see [Configuring the Unknown User Policy, page 16-16](#).



---

**Note** You may want to create a default NAC database and place it at the bottom of the Selected Databases list. A default NAC database has no mandatory credential types and therefore can perform posture validation for any request, regardless of the credentials included in the request.

---

- Step 10** For each SPT, create a downloadable IP ACL set that limits network access appropriately. If you have more than one NAC database and need to control network access differently for the same SPT for each NAC, you must create downloadable IP ACLs per SPT per NAC database. For example, if you have two NAC databases, one for NAI posture validation and one for Symantec posture validation, you may want separate downloadable IP ACLs for a Quarantine SPT, one that allows access only to a Symantec anti-virus server and one that allows access only to a NAI anti-virus server.

For detailed steps, see [Adding a Downloadable IP ACL, page 5-10](#).

- Step 11** For each group to which you have mapped an SPT, follow these steps:
- a. Assign the appropriate ACLs to the group. For example, to the group intended to authorize NAI NAC clients whose posture validation returned an Infected SPT, assign the ACL you created to control access of NAI NAC clients whose system posture is Quarantine.

For detailed steps, see [Assigning a Downloadable IP ACL to a Group, page 6-30](#).

- b. (Optional) If AAA clients participating in NAC are configured to make use of NAC-related attribute-value (AV) pairs in the RADIUS (Cisco IOS/PIX) `cisco-av-pair` attribute, configure the RADIUS (Cisco IOS/PIX) `cisco-av-pair` attribute with the applicable AV pairs. NAC-related AV pairs include:
- `url-redirect`
  - `posture-token`
  - `status-query-timeout`

**Caution**

---

The `posture-token` AV pair is the only way that Cisco Secure ACS notifies the AAA client of the SPT returned by posture validation. Because you manually configure the `posture-token` AV pair, errors in configuring `posture-token` can result in the incorrect SPT being sent to the AAA client or, if the AV pair name is mistyped, the AAA client not receiving the SPT at all.

---



---

**Note** The AV pair names above are case sensitive.

---

For detailed steps about configuring the RADIUS (Cisco IOS/PIX) `cisco-av-pair` attribute in a group profile, see [Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-40](#). For more information about the RADIUS (Cisco IOS/PIX) `cisco-av-pair` attribute, see [About the cisco-av-pair RADIUS Attribute, page C-7](#).

Cisco Secure ACS is configured to process posture validation requests, return the results to the NAC client, and send the applicable ACLs to the AAA client.

- Step 12** Create a user account to support NAC in the event of a non-responsive computer. For more information, see [Non-Responsive NAC-Client Computers, page 14-5](#). Cisco Secure ACS is configured to support NAC of non-responsive computers.
-

# NAC Databases

This section contains the following topics:

- [About NAC Databases, page 14-10](#)
- [About NAC Credentials and Attributes, page 14-11](#)
- [NAC Database Configuration Options, page 14-12](#)
- [Policy Selection Options, page 14-13](#)
- [Configuring a NAC Database, page 14-14](#)

## About NAC Databases

NAC databases validate the posture of a NAC-client computer, using the credentials that the NAC clients sends to Cisco Secure ACS in the posture validation request.



### Tip

---

Despite the placement of NAC database pages in the External User Databases section of the HTML interface, NAC databases may not involve external databases and Cisco Secure ACS performs no user authentication with a NAC database.

---

A NAC database consists of the following:

- **Mandatory credential types**—A NAC database has zero or more mandatory credential types. Cisco Secure ACS determines whether to use a NAC database to evaluate a posture validation request by comparing the credentials received in the request to the mandatory credentials types associated with a NAC database. If the request includes each credential type specified, Cisco Secure ACS uses the NAC database to evaluate the request; otherwise, Cisco Secure ACS uses the Unknown User Policy to compare the credentials received to the mandatory credential types of other NAC databases.

A NAC database without any mandatory credential types is a valid configuration. Cisco Secure ACS considers any posture validation request to satisfy the mandatory credential types of a NAC database that has zero

mandatory credential types. This design enables you to create a default database so that no posture validation request is rejected due to missing credential types.

- **Credential validation policies**—A NAC database has one or more credential validation policies. When Cisco Secure ACS uses a NAC database to evaluate a posture validation request, it applies each policy associated with the NAC database to the attributes received in the request.

## About NAC Credentials and Attributes

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

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

Cisco Secure ACS uses NAC attributes in its response to the NAC client. These attributes are known as outbound attributes. For example, APTs and the SPT are sent to the NAC client in attributes.

Credential types are uniquely identified by the combination of two identifiers: vendor ID and application ID. The vendor ID is the number 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 they provide. For example, with Cisco Systems, Inc. applications, application ID 1 corresponds to CTA. In the HTML interface, when you specify result credential types for a local policy, credential types are identified by the names assigned to the vendor and application. For example, the credential type for CTA is Cisco:PA (“PA” refers to “posture agent”, another term for CTA). In a posture validation response, Cisco Secure ACS would use the numeric identifiers 9 and 1, which are the identifiers for Cisco and CTA.

Attributes are uniquely identified by the combination of 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

Cisco Secure ACS communicates with a NAC client, the identifiers are numerical. In the HTML interface, when you define rules for local policies, attributes are identified by the names assigned to vendor, application, and attribute. For example, the CTA attribute for the version of the operating system is Cisco:PA:OS-Version. The data that Cisco Secure ACS receives identifies the attribute with the numeric identifiers 9, 1, and 6, which are the identifiers for Cisco, CTA, and the sixth attribute of CTA.

For more information about attributes, including data types and operators used in rules for local policies, see [About Rules, Rule Elements, and Attributes](#), page 14-19.

## NAC Database Configuration Options

On the Expected Host Configuration page you can configure a NAC database. The options for configuring a NAC database are as follows:

- **Mandatory Credential Types**—Displays the following options:
  - **Credential Types**—Displays the credential types that must be present in a posture validation request in order for Cisco Secure ACS to use the database to evaluate the request. If a request does not contain the mandatory credential types, Cisco Secure ACS will not use the database to evaluate the request.



### Note

---

The Unknown User Policy uses the mandatory credential types to determine if Cisco Secure ACS can use a given NAC database to evaluate a posture validation request. For more information, see [Chapter 16, “Unknown User Policy”](#).

---

- **Edit List button**—Enables you to access the Edit Credential Types page for the NAC database.
- **Credential Validation Policies**—Lists the policies Cisco Secure ACS applies to each posture validation request evaluated by the NAC database. This table contains the following options:
  - **Type**—Indicates whether the policy is a local policy or an external policy.

- **Name**—Displays the policy name as a link. You can click the link to open the applicable policy configuration page, which enables you to view policy details, edit the policy, or delete the policy.
- **Description**—Displays the description associated with the policy. The text displayed in the Description column for a given policy corresponds to the text last saved in the Description box.
- **Local Policies button**—Enables you to go to the Select Local Policies page for the current NAC database. From that page, you can select local policies that the current NAC database uses and you can also access the Local Policy Configuration page to create additional local policies.
- **External Policies button**—Enables you to go to the Select External Policies page for the current NAC database. From that page, you can select external policies that the current NAC database uses and you can also access the External Policy Configuration page to create additional local policies.

## Policy Selection Options

Policy selection pages enable you to specify the policies that Cisco Secure ACS should use to evaluate posture validation requests with the current NAC database. On the Select Local Policies page, you specify the local policies to be used. On the Select External Policies page, you can specify the external policies to be used. The options for selecting policies are as follows:

- **Available Policies**—Lists the policies that Cisco Secure ACS *does not* use to evaluate the posture validation request with this database.
- **Selected Policies**—Lists the policies that Cisco Secure ACS *does* use to evaluate the posture validation request with this database.
- **New Policy button**—Enables you to go to the applicable policy configuration page.

## Configuring a NAC Database

This procedure describes how you can configure a NAC database.

### Before You Begin

For descriptions of the options available on the Expected Host Configuration page, see [NAC Database Configuration Options, page 14-12](#).

For descriptions of the options available on the Select Local Policies page and Select Local Policies page, see [Policy Selection Options, page 14-13](#).

To configure a NAC database, follow these steps:

- 
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
- Cisco Secure ACS displays a list of all possible external user database types.
- Step 3** Click **Network Admission Control**.
- If no NAC database exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.
- Step 4** If you are creating a configuration, follow these steps:
- Click **Create New Configuration**.
  - Type a name for the new NAC database in the box provided.
  - Click **Submit**.
- Cisco Secure ACS lists the new configuration in the External User Database Configuration table.
- Step 5** Under External User Database Configuration, select the name of the NAC database that you need to configure.



---

**Note** If only one NAC database exists, the name of that database appears instead of the list. Proceed to the next step.

---

**Step 6** Click **Configure**.



**Caution**

---

If you click Delete, the selected NAC database is deleted.

---

Cisco Secure ACS displays the Expected Host Configuration page for the selected NAC database.

**Step 7** Configure mandatory credential types. To do so, follow these steps:

a. Under Mandatory Credential Types, click **Edit List**.

The Edit Credential Types page appears.

b. For each credential type that you want to require for validation with this NAC database, select the credential type in the Available Credentials list and click the right arrow (-->).

The credential type appears in the Selected Credentials list.



**Tip**

---

To remove a credential type from the Selected Credentials list, select it and click the left arrow (<--).

---

c. Click **Submit**.

The Expected Host Configuration page for this NAC database reappears.

The Mandatory Credential Types table lists the selected credential types.

Cisco Secure ACS will use this NAC database for posture validation only when the validation request contains attributes for the credential types displayed in the Mandatory Credential Types table.

**Step 8** Select the policies that Cisco Secure ACS must use to validate NAC clients with this NAC database. You can select local policies, external policies, or both. To do so, follow these steps:

a. Click either **Local Policies** or **External Policies**, as applicable.

A policy selection page displays Available Policies and Selected Policies lists.

- b. If you need to create a policy, do one of the following, as applicable:
  - Click **New Local Policy** and follow the steps in [Creating a Local Policy, page 14-25](#) before continuing this procedure.
  - Click **New External Policy** and follow the steps in [Creating an External Policy, page 14-32](#) before continuing this procedure.
- c. For each policy that you want to use to validate NAC clients with this NAC database, select the policy in the Available Policies list and click the right arrow (-->).

The policy appears in the Selected Policies list.




---

**Tip** To remove a policy from the Selected Policies list, select it and click the left arrow (<--).

---

- d. Click **Submit**.

In the Credential Validation Policies table, the Expected Host Configuration page displays the policies you selected.

- e. Repeat [a.](#) through [d.](#), as needed.

#### Step 9 Click **Save Configuration**.

Cisco Secure ACS saves the NAC database you created.

You can add the new NAC database to the Unknown User Policy and you can configure group mapping for the NAC database.




---

**Note** Until group mapping is established, posture validation with the new NAC database does not control access of the NAC client.

---

## NAC Policies

Cisco Secure ACS applies to a validation request the policies that you have selected for the NAC database that Cisco Secure ACS uses to evaluate the request.

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

The results of applying a policy are as follows:

- **Result credential type**—The credential type and, therefore, the NAC-compliant application to which the policy evaluation result applies.
- **Token**—One of five predefined tokens that represents the posture of the NAC client and, specifically, the application defined by the result credential type.
- **Action**—An optional text string, sent in the posture validation response to the application defined by the result credential type.

There are two kinds of policies: local and external.

This section contains the following topics:

- [Local Policies, page 14-17](#)
- [External Policies, page 14-28](#)
- [Editing a Policy, page 14-34](#)
- [Deleting a Policy, page 14-36](#)

## Local Policies

This section contains the following topics:

- [About Local Policies, page 14-18](#)
- [About Rules, Rule Elements, and Attributes, page 14-19](#)
- [Local Policy Configuration Options, page 14-22](#)
- [Rule Configuration Options, page 14-24](#)
- [Creating a Local Policy, page 14-25](#)

## About Local Policies

Local policies consist of one or more rules that you that define in Cisco Secure ACS. When Cisco Secure ACS applies a local policy, it uses the policy rules to evaluate credentials 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 the APT and action are associated with.

Cisco Secure ACS applies each rule in the order they appear on the Policy Configuration 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 received in a posture validation request, the result of applying the policy is the result credential type, APT, and action associated with the rule. Cisco Secure ACS does not evaluate the credentials with any additional rules.
- **No configurable rule matches**—When the attributes included in the posture validation request satisfy no policy rules, Cisco Secure ACS uses the result credential type, application posture token, and action 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, either 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 NAC clients as a second rule, but posture validation may occur more than twice as often for NAC clients 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 consisting of the following three items:

- A posture validation attribute
- An operator
- A value

Cisco Secure 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 “anded” together.

This section contains the following topics:

- [NAC Attribute Data Types, page 14-19](#)
- [Rule Operators, page 14-20](#)

### NAC Attribute Data Types

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

- **boolean**—The attribute can contain a value of either 1 or 0 (zero). In the HTML interface, when you define a rule element with a boolean attribute, valid input are the words `false` and `true`. 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, Cisco Secure 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 [Rule Operators, page 14-20](#).
- **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).

## Rule Operators

When you construct a rule on the Rule Configuration page, Cisco Secure ACS only allows you to select an operator that is applicable to the type of attribute you select. For example, if you select the `Cisco:PA:PA-Name` attribute, Cisco Secure ACS permits the use of the `contains` operator in addition to standard mathematical operators; however, if you choose the `Cisco:PA:OS-Version` attribute, Cisco Secure ACS only permits the use of mathematical operators. For more information about attribute types, see [NAC Attribute Data Types, page 14-19](#).

The following are the operators that Cisco Secure ACS supports:

- **= (equal to)**—The rule element is true if the value contained in the attribute is exactly equal to the value that you specify.
- **!= (not equal to)**—The rule element is true if the value contained in the attribute does not equal to the value that you specify.

**Tip**

Using the `!=` operator can lead to confusion, especially with boolean attributes. 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`, Cisco Secure ACS would evaluate the rule element to be true. To avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **> (greater than)**—The rule element is true if the value contained in the attribute is greater than the value that you specify.
- **< (less than)**—The rule element is true if the value contained in the attribute is less than the value that you specify.
- **<= (less than or equal to)**—The rule element is true if the value contained in the attribute is less than or equal to the value that you specify.
- **>= (greater than or equal to)**—The rule element is true if the value contained in the attribute is greater than or equal to the value that you specify.
- **contains**—The rule element is true if the attribute contains a string and if any part of that string matches the string that you specify. For example, using the contains operator and a value of `sc` would match an attribute containing the string `Cisco`, the string `scsi`, or the string `disc`.
- **starts-with**—The rule element is true if the attribute contains a string and if the beginning of that string matches the string that you specify. For example, using the starts-with operator and a value of `ci` would match an attribute containing the string `Cisco` or the string `Ciena`.
- **regular-expression**—The rule element is true if the attribute contains a string and if the string matches the regular expression that you specify. Cisco Secure ACS supports the following regular expression operators:
  - **^ (caret)**—The `^` operator matches the start of a string. For example `^ci` would match the string `Cisco` or the string `Ciena`.

- **\$ (dollar)**—The \$ operator matches the end of a string. For example, `co$` would match the string `Cisco` or the string `Tibco`.
- **days-since-last-update**—The rule element is true if the attribute contains a date and if the difference in days between that date and the current date is less than or equal to the number that you specify. For example, in the following rule element:

```
Symantec:AV:DAT-Date days-since-last-update 14
```

the rule element is true for posture validation requests whose `Symantec:AV:DAT-Date` attribute contain a date that is no more than 14 days in the past.

- **mask**—The rule element is true if the attribute contains an IP address and if that address belongs to the subnet identified by the netmask and IP address that you specify as the rule element value. The format for the rule element value is:

```
mask/IP
```

For example, using the mask operator with a value of `255.255.255.0/192.168.73.8` would match an attribute containing an IP address of 192.168.73.0 to 192.168.73.255. Any mask is permissible and Cisco Secure ACS determines the set of IP addresses matching the value specified using standard subnet masking logic.

## Local Policy Configuration Options

On the Local Policy Configuration page you can specify the rules that make up a policy, including their order. The options for configuring a local policy are as follows:

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



### Note

The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the following four characters: `[ ] , /`

- **Description**—Specifies a text description of the policy, up to 255 characters. Use the Description box to provide details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules. Because you can apply the same policy to more than one NAC database, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which databases use it.
- **Configurable Rules**—Lists rules that you define in the order in which Cisco Secure ACS uses them to evaluate the posture validation request. Each rule appears as a separate row in the table and is identified by its rule elements, which appear as a blue link. You can order the rules in this table by selecting the option directly to the left of a rule and clicking Up and Down to position it as needed. For more information about the order of rules, see [About Local Policies, page 14-18](#).

The Configurable Rules table contains the following options:

- **Result Credential Type**—Specifies a vendor and application. If the rule is true, the Result Credential Type determines the application to which the token in the corresponding Token list is associated. Credential types are listed by the vendor name and application name. For example, CTA appears on the list as `CISCO:PA`. For more information about credential types, see [About NAC Credentials and Attributes, page 14-11](#).
- **Token**—Specifies a token, specifically, an APT. If the rule is true, the Token list determines the APT associated with the vendor and application selected in the corresponding Result Credential Type list. For more information about tokens, see [Posture Tokens, page 14-4](#).
- **Action**—Specifies a text message sent to the application indicated by the Result Credential Type list. Use of the text message is determined by the vendor. Some NAC-compliant applications do not implement the use of the Action box.
- **Default Rule**—If no configurable rule is true, the Default Rule table specifies the credential type, token, and action that Cisco Secure ACS uses as the result of applying the policy.




---

**Note** Under Default Rule, the meanings of the Result Credential Type list, Token list, and Action box are identical to the options of the same name in the Configurable Rules table, except that the default rule is automatically true, provided that no rule in the Configurable Rules table is true.

---

## Rule Configuration Options

On the Rule Configuration page you can specify the rule elements that make up a rule. For more information about rules, see [About Rules, Rule Elements, and Attributes, page 14-19](#).

The options for configuring a rule are as follows:

- **Rule Elements Table**—Lists the rule elements that make up the rule. The information displayed in Attribute, Operator, and Value columns for each rule element reflect the settings specified when the rule element was created. For details about the meaning of each column, see the corresponding option description below.

The Rule Elements Table is limited to displaying 27 characters in the Attribute column and 11 characters in the Value column.

- **Remove button**—Removes the selected rule element from the Rule Elements Table and sets the Attribute, Operator, and Value options to the values in the corresponding columns of the removed rule element. You can also double-click a rule element to remove it from the table.



**Tip**

---

The Remove button enables you to edit a rule element previously added to the table. After you select the rule and click **remove**, you can change the Attribute, Operator, and Value options (described below) and then click **enter** to return the edited rule to the Rule Elements Table.

---

- **Attribute**—Lists all posture validation attributes that you can use to specify rules. The attributes listed are only those that can be received from a NAC client. Attributes that can only be sent, such as Cisco:PA:System-Posture-Token, cannot be used in a rule and thus never

appear in the Attribute list. Each attribute is uniquely identified by the vendor name, application name, and attribute name, displayed alphabetically in the following format:

*vendor-name : application-name : attribute-name*

- **Operator**—Defines the comparison method by which Cisco Secure ACS evaluates whether the rule element is true. The operators available in the Operator list vary depending upon the type of attribute selected from the Attribute list. In addition to common operators, such as >, <, and =, the Operator list supports a few special operators. For more information about special operators, see [About Rules, Rule Elements, and Attributes, page 14-19](#).
- **Value**—Specifies the value to which Cisco Secure ACS compares the contents of the attribute.
- **Enter button**—Adds the rule element defined in the Attribute, Operator, and Value options to the Rule Elements Table.

## Creating a Local Policy

This procedure describes how you can create a local policy.

### Before You Begin

Although local policies can be selected for more than one NAC database, the page for creating a local policy must be accessed through the configuration pages of a specific NAC database. The NAC database you use to access the Local Policy Configuration page does not limit which NAC databases can select the new local policy.

For descriptions of the options available on the Local Policy Configuration page, see [Local Policy Configuration Options, page 14-22](#).

For descriptions of the options available on the Rule Configuration page, see [Rule Configuration Options, page 14-24](#).

To create a local policy, follow these steps:

- 
- Step 1** If you have not already done so, access the Local Policy Configuration page. To do so, follow these steps:
- a. In the navigation bar, click **External User Databases**.

- b. Click **Database Configuration > Network Admission Control**.  
Cisco Secure ACS displays a list of NAC databases.
- c. Select a NAC database from the list of NAC databases and click **Configure**.




---

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

---

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

- d. Under Credential Validation Policies, click **Local Policies**.  
The Select Local Policies page appears.
- e. Click **New Local Policy**.

The Local Policy Configuration page appears.

- 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** Create one or more rules, as needed to define the policy.

For each rule you want to create, follow these steps:

- a. Click **New Rule**.  
The Edit Rule page appears.
- b. For each rule element you want to add, do each of the following:
  - Select an attribute.
  - Select an operator.
  - Type a value.
  - Click **enter**.

For more information about attribute types, see [NAC Attribute Data Types, page 14-19](#). For more information about operators, see [Rule Operators, page 14-20](#).

The rule element appears in the Rule Elements table.

- c. Verify that the rule elements are configured as intended.

**Tip**

---

If you want to change a rule element that you have already added to the Rules Elements table, you edit it by selecting the rule element, clicking **remove**, editing its attribute, operator, or value, and clicking **enter** again.

---

**d. Click **Submit**.**

The Policy Configuration page appears again. The new rule appears at the bottom of the Configurable Rules table.

**Tip**

---

You can return to the Edit Rule page by clicking the rule.

---

**e. For the new rule, do each of the following:**

- Select a result credential type.
- Select a token.
- Type an action.

For more information about tokens, see [Posture Tokens, page 14-4](#).

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

**Step 5** After you create the rules required to define the policy, order the rules as needed. Cisco Secure ACS applies a policy by attempting to match rules in the order they appear on the Policy Configuration page, from top to bottom. Policy processing stops upon the first successful rule match, so order is important. To move a rule, follow these steps:

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

**Step 6** Configure the Default Rule; in the Default Rule table, do each of the following.

- Select a result credential type.
- Select a token.
- Type an action.

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

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

The Select Local Policies page displays the new policy in the Available Policies list.



---

**Tip** You can add the policy to any NAC database, not just the NAC database you clicked through to reach the Local Policy Configuration page.

---

**Step 8** If you are in the process of configuring a new NAC database, resume performing the steps in [Configuring a NAC Database, page 14-14](#).

---

## External Policies

This section contains the following topics:

- [About External Policies, page 14-28](#)
- [External Policy Configuration Options, page 14-29](#)
- [Creating an External Policy, page 14-32](#)

## About External Policies

External policies are policies that define an external NAC server, usually from an anti-virus vendor, and a set of credential types to be forwarded to the external database. You also have the option of defining a secondary external NAC server.

Cisco Secure 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 associated with a NAC database must return a result; otherwise, Cisco Secure ACS rejects policy validation requests evaluated with a NAC database whose external policies do not return a result. For example, if

Cisco Secure ACS evaluates a posture validation request using a NAC database that has 10 local policies and one external policy, but the external NAC servers associated with the external policy are not online, it is irrelevant that the 10 local policies all return SPTs. The failure of the single external policy causes Cisco Secure ACS to reject the posture validation request.

## External Policy Configuration Options

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

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



---

**Note** The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the following four characters:  
[ ], /

---

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

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

- **Server Configuration**—You must specify a primary server. You have the option to specify a secondary server for failover operation. For each posture validation request that an external policy is applied to, Cisco Secure 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 Cisco Secure

ACS cannot reach the primary server or the primary server fails to respond to the request, Cisco Secure ACS will use the secondary server, if it is configured and enabled.

For the primary and secondary server configurations, each have the following options:

- **URL**—Specifies the HTTP or HTTPS URL for the server. URLs must conform to the following format:

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

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

The default protocol is HTTP. URLs beginning with the hostname are assumed to be using HTTP. To use HTTPS, you must specify the URL beginning with `https://`.

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

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

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

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

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

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

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

- **Username**—Specifies the username by which Cisco Secure ACS submits forwarded credentials to the server. If the server is not password protected, the values provided in the Username and Password boxes are ignored.

- **Password**—Specifies the password for the username in the Username box.
- **Timeout (Sec)**—The number of seconds that Cisco Secure ACS waits for a reply from a server after it forwards the credentials.

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

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

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

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

If the CA that issued a NAC server certificate is not present on the Trusted Root CA list, you must add the CA certificate to Cisco Secure ACS. For more information, see [Adding a Certificate Authority Certificate, page 10-37](#).

**Note**

---

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

---

**Tip**

---

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

---

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

## Creating an External Policy

This procedure describes how you can create an external policy.

### Before You Begin

Although external policies can be selected for more than one NAC database, the page for creating an external policy must be accessed through the configuration pages of a specific NAC database. The NAC database you use to access the External Policy Configuration page does not limit which NAC databases can select the new external policy.

For descriptions of the options available on the External Policy Configuration page, see [External Policy Configuration Options, page 14-29](#).

To create an external policy, follow these steps:

- 
- Step 1** If you have not already done so, access the External Policy Configuration page. To do so, follow these steps:
- a. In the navigation bar, click **External User Databases**.
  - b. Click **Database Configuration > Network Admission Control**.  
Cisco Secure ACS displays a list of all possible external user database types.
  - c. Select a NAC database from the list of NAC databases and click **Configure**.




---

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

---

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

- d. Under Credential Validation Policies, click **External Policies**.

The Select External Policies page appears.

- e. Click **New External Policy**.

The External Policy Configuration page appears.

**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** In the **Primary Server configuration** area, do the following:

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



---

**Note**

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

---

- b. Provide configuration details about the primary NAC server. For more information about the boxes and list in this area, see [External Policy Configuration Options, page 14-29](#).

**Step 5** (Optional) In the **Secondary Server configuration** area, do the following:

- a. Select the **Secondary Server configuration** check box
- b. Provide configuration details about the secondary NAC server. For more information about the boxes and list in this area, see [External Policy Configuration Options, page 14-29](#).

**Step 6** Select the posture validation credential types that Cisco Secure ACS should send to the external NAC server.

For each posture validation credential type that you want Cisco Secure ACS to send to the external NAC server, select the credential type in the Available Credentials list and click the right arrow (-->).

The credential type appears in the Selected Credentials list.



---

**Tip**

To remove a credential type from the Selected Credentials list, select it and click the left arrow (<--).

---

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

The Select External Policies page displays the new policy in the Available Policies list.



**Tip** You can add the policy to any NAC database, not just the NAC database you clicked through to reach the External Policy Configuration page.

- Step 8** If you are in the process of configuring a NAC database, resume performing the steps in [Configuring a NAC Database, page 14-14](#).

## Editing a Policy

### Before You Begin

A policy can be edited only by accessing it through a NAC database that includes the policy in its Credential Validation Policies table.

To edit a policy, follow these steps:

- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration > Network Admission Control**.  
Cisco Secure ACS displays a list of NAC databases.
- Step 3** Select a NAC database from the list of NAC databases and click **Configure**.



**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

- Step 4** Under **Name**, click the name of the policy you want to edit.

**Tip**

---

If the policy you want to edit does not appear in the Credential Validation Policies table, click **Local Policies** or **External Policies**, as applicable, move the policy you want to edit to the Selected Policies list, and click **Submit**. You can remove the policy from the Credential Validation Policies table when you are done editing it.

---

The applicable policy configuration page appears.

**Step 5** Edit the policy as needed. Be aware of the following:

- If you change the name of the policy, clicking Submit creates a new policy. Cisco Secure ACS stores the new policy and does not change the configuration of the old policy. The old policy remains on the Credential Validation Policies table of each database that it was on before creating the new policy.

When you click Submit after changing the policy name, the applicable policy selection page for the NAC database you selected in [Step 3](#). You can modify the policy selection, if desired, and then click **Submit**.

- To edit a local policy rule, in the Configurable Rules table, click the rule name. The Edit Rule page displays the Rule Elements table. Add, modify, or remove rule elements from the rule as needed, and then click **Submit** to return to the Policy Configuration page.

**Step 6** Click **Submit**.

Cisco Secure ACS saves the changes you made to the policy. The Expected Host Configuration page reappears, or if you changed the policy name, a policy selection page appears, enabling you to select the new policy for the NAC database you selected in [Step 3](#).

**Tip**

---

If you added the policy to the NAC database only so that you could edit it, be sure to remove it from the applicable Selected Policies list. To do so, click **Local Policies** or **External Policies**, as applicable, move the policy to the Available Policies list, and click **Submit**.

---

## Deleting a Policy

### Before You Begin

A policy can be deleted only by accessing it through a NAC database that includes the policy in its Credential Validation Policies table.

To delete a policy, follow these steps:

- 
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration > Network Admission Control**.  
Cisco Secure ACS displays a list of all possible external user database types.
- Step 3** Select a NAC database from the list of NAC databases and click **Configure**.



---

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

---

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

- Step 4** Under **Name**, click the name of the policy you want to delete.



---

**Tip** If the policy you want to delete does not appear in the Credential Validation Policies table, click **Local Policies** or **External Policies**, as applicable, move the policy you want to delete to the Selected Policies list, and click **Submit**. After you delete the policy, it will no longer appear in the Credential Validation Policies table for this NAC database and will no longer appear on a policy selection page.

---

The applicable policy configuration page appears.

**Step 5** Click **Delete Policy**.

**Step 6** Click **Submit**.

Cisco Secure ACS deletes the policy. The Expected Host Configuration page reappears and the Credential Validation Policies table no longer lists the deleted policy. All NAC databases that were configured to use the policy no longer include the deleted policy.

---

