



System Configuration: Advanced

This chapter addresses the CiscoSecure Database Replication and RDBMS Synchronization features found in the System Configuration section of Cisco Secure ACS Solution Engine. It contains the following sections:

This chapter contains the following topics:

- [CiscoSecure Database Replication, page 9-1](#)
- [RDBMS Synchronization, page 9-25](#)
- [IP Pools Server, page 9-39](#)
- [IP Pools Address Recovery, page 9-47](#)
- [NAC Attribute Management, page 9-47](#)

CiscoSecure Database Replication

This section provides information about the CiscoSecure Database Replication feature, including procedures for implementing this feature and configuring the Cisco Secure ACSes involved.

This section contains the following topics:

- [About CiscoSecure Database Replication, page 9-2](#)
- [Important Implementation Considerations, page 9-7](#)
- [Database Replication Versus Database Backup, page 9-10](#)
- [Database Replication Logging, page 9-11](#)
- [Replication Options, page 9-11](#)

- [Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes, page 9-16](#)
- [Configuring a Secondary Cisco Secure ACS, page 9-17](#)
- [Replicating Immediately, page 9-19](#)
- [Scheduling Replication, page 9-21](#)
- [Disabling CiscoSecure Database Replication, page 9-24](#)
- [Database Replication Event Errors, page 9-25](#)

About CiscoSecure Database Replication

Database replication helps make your AAA environment more fault tolerant. Database replication helps create mirror systems of Cisco Secure ACSes by duplicating parts of the primary Cisco Secure ACS setup to one or more secondary Cisco Secure ACSes. You can configure your AAA clients to use these secondary Cisco Secure ACSes if the primary Cisco Secure ACS fails or is unreachable. With a secondary Cisco Secure ACS whose CiscoSecure database is a replica of the CiscoSecure database on the primary Cisco Secure ACS, if the primary Cisco Secure ACS goes out of service, incoming requests are authenticated without network downtime, provided that your AAA clients are configured to failover to the secondary Cisco Secure ACS.

Database replication allows you to do the following:

- Select the parts of the primary Cisco Secure ACS configuration to be replicated.
- Control the timing of the replication process, including creating schedules.
- Export selected configuration items from the primary system.
- Securely transport selected configuration data from the primary Cisco Secure ACS to one or more secondary Cisco Secure ACSes.
- Update the secondary Cisco Secure ACSes to create matching configurations.

The following items cannot be replicated:

- IP pool definitions (for more information, see [About IP Pools Server, page 9-40](#)).
- Cisco Secure ACS certificate and private key files.
- All external user database configurations, including NAC databases.

- Unknown user group mapping configuration.
- User-defined RADIUS dictionaries (for more information, see [Important Implementation Considerations, page 9-7](#)).
- Settings on the ACS Service Management page in the System Configuration section.
- All logging configurations.
- RDBMS Synchronization settings.

With regard to database replication, we make the following distinctions about Cisco Secure ACSes:

- **Primary Cisco Secure ACS**—A Cisco Secure ACS that sends replicated CiscoSecure database components to other Cisco Secure ACSes.
- **Secondary Cisco Secure ACS**—A Cisco Secure ACS that receives replicated CiscoSecure database components from a primary Cisco Secure ACS. In the HTML interface, these are identified as replication partners.

A Cisco Secure ACS can be both a primary Cisco Secure ACS and a secondary Cisco Secure ACS, provided that it is not configured to be a secondary Cisco Secure ACS to a Cisco Secure ACS for which it performs as a primary Cisco Secure ACS.

**Note**

Bidirectional replication, wherein a Cisco Secure ACS both sends database components to and receives database components from the same remote Cisco Secure ACS, is not supported.

**Note**

All Cisco Secure ACSes involved in replication must run the same release of the Cisco Secure ACS software. For example, if the primary Cisco Secure ACS is running Cisco Secure ACS version 3.2, all secondary Cisco Secure ACSes should be running Cisco Secure ACS version 3.2. Because patch releases can introduce significant changes to the CiscoSecure database, we strongly recommend that Cisco Secure ACSes involved in replication use the same patch level, too.

Replication Process

This topic describes the process of database replication, including the interaction between a primary Cisco Secure ACS and each of its secondary Cisco Secure ACSes. The following steps occur in database replication:

1. The primary Cisco Secure ACS determines if its database has changed since the last successful replication. If it has, replication proceeds. If it has not, replication is aborted. No attempt is made to compare the databases of the primary and secondary Cisco Secure ACSes.



Tip

You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

2. The primary Cisco Secure ACS contacts the secondary Cisco Secure ACS. In this initial connection, the following four events occur:
 - a. The two Cisco Secure ACSes perform mutual authentication based upon the shared secret of the primary Cisco Secure ACS. If authentication fails, replication fails.



Note

On the secondary Cisco Secure ACS, the AAA Servers table entry for the primary Cisco Secure ACS must have the same shared secret that the primary Cisco Secure ACS has for itself in its own AAA Servers table entry. The secondary Cisco Secure ACS's shared secret is irrelevant.

- b. The secondary Cisco Secure ACS verifies that it is not configured to replicate to the primary Cisco Secure ACS. If it is, replication is aborted. Cisco Secure ACS does not support bidirectional replication, wherein a Cisco Secure ACS can act as both a primary and a secondary Cisco Secure ACS to the same remote Cisco Secure ACS.
 - c. The primary Cisco Secure ACS verifies that the version of Cisco Secure ACS that the secondary Cisco Secure ACS is running is the same as its own version of Cisco Secure ACS. If not, replication fails.
 - d. The primary Cisco Secure ACS compares the list of database components it is configured to send with the list of database components the secondary Cisco Secure ACS is configured to receive. If the

secondary Cisco Secure ACS is not configured to receive any of the components that the primary Cisco Secure ACS is configured to send, the database replication fails.

3. After the primary Cisco Secure ACS has determined which components to send to the secondary Cisco Secure ACS, the replication process continues on the primary Cisco Secure ACS as follows:
 - a. The primary Cisco Secure ACS stops its authentication and creates a copy of the CiscoSecure database components that it is configured to replicate. During this step, if AAA clients are configured properly, those that usually use the primary Cisco Secure ACS failover to another Cisco Secure ACS.
 - b. The primary Cisco Secure ACS resumes its authentication service. It also compresses and encrypts the copy of its database components for transmission to the secondary Cisco Secure ACS.
 - c. The primary Cisco Secure ACS transmits the compressed, encrypted copy of its database components to the secondary Cisco Secure ACS. This transmission occurs over a TCP connection, using port 2000. The TCP session uses a 128-bit encrypted, Cisco-proprietary protocol.
4. After the preceding events on the primary Cisco Secure ACS, the database replication process continues on the secondary Cisco Secure ACS as follows:
 - a. The secondary Cisco Secure ACS receives the compressed, encrypted copy of the CiscoSecure database components from the primary Cisco Secure ACS. After transmission of the database components is complete, the secondary Cisco Secure ACS decompresses the database components.
 - b. The secondary Cisco Secure ACS stops its authentication service and replaces its database components with the database components it received from the primary Cisco Secure ACS. During this step, if AAA clients are configured properly, those that usually use the secondary Cisco Secure ACS failover to another Cisco Secure ACS.
 - c. The secondary Cisco Secure ACS resumes its authentication service.

Cisco Secure ACS can act as both a primary Cisco Secure ACS and a secondary Cisco Secure ACS. [Figure 9-1](#) shows a cascading replication scenario. Server 1 acts only as a primary Cisco Secure ACS, replicating to servers 2 and 3, which act as secondary Cisco Secure ACSes. After replication from server 1 to server 2 has

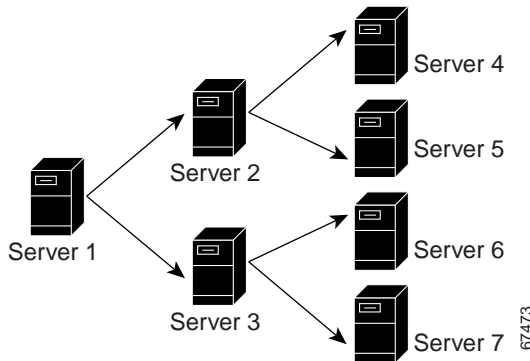
completed, server 2 acts as a primary Cisco Secure ACS while replicating to servers 4 and 5. Similarly, server 3 acts as a primary Cisco Secure ACS while replicating to servers 6 and 7.

**Note**

If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. In [Figure 9-1](#), server 1 must have an entry in its AAA Servers table for each of the other six Cisco Secure ACSes. If this is not done, after replication, servers 2 and 3 do not have servers 4 through 7 in their AAA Servers tables and replication will fail.

If server 2 were configured to replicate to server 1 in addition to receiving replication from server 1, replication to server 2 would fail. Cisco Secure ACS cannot support such a configuration, known as bidirectional replication. To safeguard against this, a secondary Cisco Secure ACS aborts replication when its primary Cisco Secure ACS appears on its Replication list.

Figure 9-1 Cascading Database Replication



Replication Frequency

The frequency with which your Cisco Secure ACSes replicate can have important implications for overall AAA performance. With shorter replication frequencies, a secondary Cisco Secure ACS is more up-to-date with the primary Cisco Secure ACS. This allows for a more current secondary Cisco Secure ACS if the primary Cisco Secure ACS fails.

There is a cost to having frequent replications. The more frequent the replication, the higher the load on a multi-Cisco Secure ACS architecture and on your network environment. If you schedule frequent replication, network traffic is much higher. Also, processing load on the replicating systems is increased. Replication consumes system resources and briefly interrupts authentication; thus the more often replication is repeated, the greater the impact on the AAA performance of the Cisco Secure ACS.



Note

Regardless of how frequently replication is scheduled to occur, it only occurs when the database of the primary Cisco Secure ACS has changed since the last successful replication.

This issue is more apparent with databases that are large or that frequently change. Database replication is a non-incremental, destructive backup. In other words, it completely replaces the database and configuration on the secondary Cisco Secure ACS every time it runs. Therefore, a large database results in substantial amounts of data being transferred, and the processing overhead can also be large.

Important Implementation Considerations

You should consider several important points when you implement the CiscoSecure Database Replication feature:

- Cisco Secure ACS only supports database replication to other Cisco Secure ACSes. All Cisco Secure ACSes participating in CiscoSecure database replication must run the same version of Cisco Secure ACS. We strongly recommend that Cisco Secure ACSes involved in replication use the same patch level, too.

- You must ensure correct configuration of the AAA Servers table in all Cisco Secure ACSes involved in replication.
 - In its AAA Servers table, a primary Cisco Secure ACS must have an accurately configured entry for each secondary Cisco Secure ACS.

**Note**

If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from that primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

- In its AAA Servers table, a secondary Cisco Secure ACS must have an accurately configured entry for each of its primary Cisco Secure ACSes.
- On a primary Cisco Secure ACS and all its secondary Cisco Secure ACSes, the AAA Servers table entries for the primary Cisco Secure ACS must have identical shared secrets.
- Only suitably configured, valid Cisco Secure ACSes can be secondary Cisco Secure ACSes. To configure a secondary Cisco Secure ACS for database replication, see [Configuring a Secondary Cisco Secure ACS, page 9-17](#).
- Replication only occurs when the database of the primary Cisco Secure ACS has changed since the last successful replication, regardless of how frequently replication is scheduled to occur. When a scheduled or manually started replication begins, the primary Cisco Secure ACS automatically aborts replication if its database has not changed since the last successful replication.

**Tip**

You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

- Replication to secondary Cisco Secure ACSes takes place sequentially in the order listed in the Replication list under Replication Partners on the CiscoSecure Database Replication page.
- A secondary Cisco Secure ACS receiving replicated components must be configured to accept database replication from the primary Cisco Secure ACS. To configure a secondary Cisco Secure ACS for database replication, see [Configuring a Secondary Cisco Secure ACS, page 9-17](#).
- Cisco Secure ACS does not support bidirectional database replication. The secondary Cisco Secure ACS receiving the replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.
- If you replicate user accounts, be sure to name external database configurations identically on primary and secondary Cisco Secure ACSes. A replicated user account retains its association with the database assigned to provide authentication or posture validation service, regardless of whether a database configuration of the same name exists on the secondary Cisco Secure ACS. For example, if user account is associated with a database named “WestCoast LDAP” on the primary Cisco Secure ACS, the replicated user account on all secondary Cisco Secure ACSes remains associated with an external user database named “WestCoast LDAP” even if you have not configured an LDAP database instance of that name.
- If you replicate NAC policies, secondary Cisco Secure ACSes associate policies to NAC databases by the order in which the NAC databases were created, not by the database name. For example, if the primary Cisco Secure ACS has the following NAC database and policy configuration:
 - “NAC DB One” with “Policy One” selected.
 - “NAC DB Two” with “Policy Two” selected.and if a secondary Cisco Secure ACS is configured first with a NAC database named “NAC DB Two” and second with a NAC database named “NAC DB One”, then the following policy selection results after replication occurs:
 - “NAC DB One” with “Policy Two” selected.
 - “NAC DB Two” with “Policy One” selected.
- To replicate user and group settings that use user-defined RADIUS vendor and VSAs, you must manually add the user-defined RADIUS vendor and VSA definitions on primary and secondary Cisco Secure ACSes, making sure

that the RADIUS vendor slots that the user-defined RADIUS vendors occupy are identical on each Cisco Secure ACS. After you have done so, replication of settings using user-defined RADIUS vendors and VSAs is supported. For more information about user-defined RADIUS vendors and VSAs, see [Custom RADIUS Vendors and VSAs, page 9-28](#).

Database Replication Versus Database Backup

Do not confuse database replication with system backup. Database replication does *not* replace System Backup. While both features provide protection from partial or complete server loss, each feature addresses the issue in a different way.

System Backup archives data into a format that you can later use to restore the configuration if the system fails or the data becomes corrupted. The backup data is stored on the local hard drive and can be copied and removed from the system for long-term storage. You can store several generations of database backup files.

CiscoSecure Database Replication offers the convenience of copying various components of the CiscoSecure database to other Cisco Secure ACSes. This can help you plan a failover AAA architecture and can help reduce the complexity of your configuration and maintenance tasks. While it is unlikely, it is possible that CiscoSecure Database Replication can propagate a corrupted database to the Cisco Secure ACSes that generate your backup files.



Caution

The possibility of backing up a corrupted database exists regardless of whether you use CiscoSecure Database Replication. Because of this small risk, if you are using Cisco Secure ACS in mission-critical environments, we strongly recommend that you implement a backup plan that accounts for this possibility. For more information about backing up the Cisco Secure ACS system or the CiscoSecure database, see [Cisco Secure ACS Backup, page 8-8](#).

Due to the necessity of local configuration, replication does not process IP pool definitions (however, IP pool assignments are replicated as part of the user and group profiles). Therefore, if applicable, common IP pool definitions must be manually configured in a manner that uses common pool names while establishing different address ranges. Certificate configuration is not replicated either, because certificate information is specific to each Cisco Secure ACS.

Also, network device group (NDG) settings, if employed, must remain constant between Cisco Secure ACSes. That is, you must guard against the primary Cisco Secure ACS sending a user or group profile that invokes an NDG that is not defined on the secondary Cisco Secure ACS.

Database Replication Logging

Regardless of whether replication events are successful or not, Cisco Secure ACS logs all replication events in the Database Replication report, available in the Reports and Activity section of the HTML interface. For more information about Cisco Secure ACS reports, see [Chapter 1, “Overview”](#).

Replication Options

The Cisco Secure ACS HTML interface provides three sets of options for configuring CiscoSecure Database Replication, documented in this section.

This section contains the following topics:

- [Replication Components Options, page 9-11](#)
- [Outbound Replication Options, page 9-12](#)
- [Inbound Replication Options, page 9-15](#)

Replication Components Options

You can specify both the CiscoSecure database components that a Cisco Secure ACS sends as a primary Cisco Secure ACS and the components that it receives as a secondary Cisco Secure ACS.



Note

The CiscoSecure database components received by a secondary Cisco Secure ACS *overwrite* the CiscoSecure database components on the secondary Cisco Secure ACS. Any information unique to the overwritten database component is lost.

The options that control the components replicated appear in the Replication Components table on the CiscoSecure Database Replication page and are as follows:

- **User and group database**—Replicate information for groups and users. Using this option excludes the use of the “Group database only” option.
- **Group database only**—Replicate information for groups, but not for users. Using this option excludes the use of the “User and group database” option.
- **Network Configuration Device tables**—Replicate the AAA Servers tables, the AAA Clients tables, and the Remote Agent tables in the Network Configuration section.
- **Distribution table**—Replicate the Proxy Distribution Table in the Network Configuration section.
- **Interface configuration**—Replicate most of the Advanced Options settings from the Interface Configuration section.
- **Interface security settings**—Replicate the security information for the Cisco Secure ACS HTML interface.
- **Password validation settings**—Replicate the password validation settings.
- **EAP-FAST master keys and policies**—Replicate active and retired master keys and policies for EAP-FAST.
- **CNAC policies**—Replicate NAC local policies, external policies, and attribute definitions.

If mirroring the entire database might send confidential information to the secondary Cisco Secure ACS, such as the Proxy Distribution Table, you can configure the primary Cisco Secure ACS to send only a specific category of database information.

Outbound Replication Options

In the Outbound Replication table on the CiscoSecure Database Replication page, you can schedule outbound replication and you can specify the secondary Cisco Secure ACSes for this primary Cisco Secure ACS.

- **Scheduling Options**—You can specify when CiscoSecure database replication occurs. The options that control when replication occurs appear in the Scheduling section of Outbound Replication table and are as follows:
 - **Manually**—Cisco Secure ACS does not perform automatic database replication.
 - **Automatically Triggered Cascade**—Cisco Secure ACS performs database replication to the configured list of secondary Cisco Secure ACSes when database replication from a primary Cisco Secure ACS completes. This enables you to build a propagation hierarchy of Cisco Secure ACS, relieving a primary Cisco Secure ACS from the burden of propagating the replicated components to every other Cisco Secure ACS. For an illustration of cascade replication, see [Figure 9-1](#).

**Note**

If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

- **Every X minutes**—Cisco Secure ACS performs, on a set frequency, database replication to the configured list of secondary Cisco Secure ACSes. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times...**—Cisco Secure ACS performs, at the time specified in the day and hour graph, database replication to the configured list of secondary Cisco Secure ACSes. The minimum interval is one hour, and the replication takes place on the hour selected.

- **Partner Options**—You can specify the secondary Cisco Secure ACSes for this primary Cisco Secure ACS. The options that control the secondary Cisco Secure ACSes to which a primary Cisco Secure ACS replicates appear in the Partners section of the Outbound Replication table.

**Note**

The items in the AAA Server and Replication lists reflect the AAA servers configured in the AAA Servers table in Network Configuration. To make a particular Cisco Secure ACS available as a secondary Cisco Secure ACS, you must first add that Cisco Secure ACS to the AAA Servers table of the primary Cisco Secure ACS.

- **AAA Server**—This list represents the secondary Cisco Secure ACSes that this primary Cisco Secure ACS *does not* send replicated components to.
- **Replication**—This list represents the secondary Cisco Secure ACSes that this primary Cisco Secure ACS *does* send replicated components to.
- **Replication timeout**—Use this text box to specify the number of minutes that this primary Cisco Secure ACS continues replicating to a secondary Cisco Secure ACS. When the timeout value is exceeded, Cisco Secure ACS terminates replication to the secondary Cisco Secure ACS it was attempting to replicate to and then it restarts the CSAuth service. The replication timeout feature helps prevent loss of AAA services due to stalled replication communication, which can occur when the network connection between the primary and secondary Cisco Secure ACS is abnormally slow or when a fault occurs within either Cisco Secure ACS. The default value is five minutes.

**Tip**

The size of the components replicated affects the time required for replication. For example, replicating a user database containing 80,000 user profiles takes more time than replicating a user database containing 500 user profiles. You may need to monitor successful replication events to determine a reasonable timeout value for your implementation.

**Note**

Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.

Inbound Replication Options

You can specify the primary Cisco Secure ACSes from which a secondary Cisco Secure ACS accepts replication. This option appears in the Inbound Replication table on the CiscoSecure Database Replication page.

The **Accept replication from** list controls which Cisco Secure ACSes the current Cisco Secure ACS does accept replicated components from. The list contains the following options:

- **Any Known CiscoSecure ACS Server**—If this option is selected, Cisco Secure ACS accepts replicated components from any Cisco Secure ACS configured in the AAA Servers table in Network Configuration.
- **Other AAA servers**—The list displays all the AAA servers configured in the AAA Servers table in Network Configuration. If a specific AAA server name is selected, Cisco Secure ACS accepts replicated components only from the Cisco Secure ACS specified.

**Note**

Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.

For more information about the AAA Servers table in Network Configuration, see [AAA Server Configuration, page 4-22](#).

Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes

If you implement a replication scheme that uses cascading replication, the Cisco Secure ACS configured to replicate only when it has received replicated components from another Cisco Secure ACS acts both as a primary Cisco Secure ACS and as a secondary Cisco Secure ACS. First, it acts as a secondary Cisco Secure ACS while it receives replicated components, and then it acts as a primary Cisco Secure ACS while it replicates components to other Cisco Secure ACSes. For an illustration of cascade replication, see [Figure 9-1](#).

To implement primary and secondary replication setups on Cisco Secure ACSes, follow these steps:

-
- Step 1** On each secondary Cisco Secure ACS, follow these steps:
- a. In the Network Configuration section, add the primary Cisco Secure ACS to the AAA Servers table.

For more information about adding entries to the AAA Servers table, see [AAA Server Configuration, page 4-22](#).
 - b. Configure the secondary Cisco Secure ACS to receive replicated components. For instructions, see [Configuring a Secondary Cisco Secure ACS, page 9-17](#).
- Step 2** On the primary Cisco Secure ACS, follow these steps:
- a. In the Network Configuration section, add each secondary Cisco Secure ACS to the AAA Servers table.

**Note**

If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

For more information about adding entries to the AAA Servers table, see [AAA Server Configuration, page 4-22](#).

- b. If you want to replicate according to a schedule, at intervals, or whenever the primary Cisco Secure ACS has received replicated components from another Cisco Secure ACS, see [Scheduling Replication, page 9-21](#).
 - c. If you want to initiate replication immediately, see [Replicating Immediately, page 9-19](#).
-

Configuring a Secondary Cisco Secure ACS



Note

If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Select the **Distributed System Settings** check box if not already selected.

The CiscoSecure Database Replication feature requires that you configure specific Cisco Secure ACSes to act as secondary Cisco Secure ACSes. The components that a secondary Cisco Secure ACS is to receive must be explicitly specified, as must be its primary Cisco Secure ACS.

Replication is always initiated by the primary Cisco Secure ACS. For more information about sending replication components, see [Replicating Immediately, page 9-19](#) or [Scheduling Replication, page 9-21](#).



Caution

The CiscoSecure database components received by a secondary Cisco Secure ACS *overwrite* the CiscoSecure database components on the secondary Cisco Secure ACS. Any information unique to the overwritten database component is lost.

Before You Begin

Ensure correct configuration of the AAA Servers table in the secondary Cisco Secure ACS. This secondary Cisco Secure ACS must have an entry in its AAA Servers table for each of its primary Cisco Secure ACSes. Also, the AAA Servers table entry for each primary Cisco Secure ACS must have the same shared

secret that the primary Cisco Secure ACS has for its own entry in its AAA Servers table. For more information about the AAA Servers table, see [AAA Server Configuration, page 4-22](#).

To configure a Cisco Secure ACS to be a secondary Cisco Secure ACS, follow these steps:

-
- Step 1** Log in to the HTML interface on the secondary Cisco Secure ACS.
- Step 2** In the navigation bar, click **System Configuration**.
- Step 3** Click **CiscoSecure Database Replication**.
The Database Replication Setup page appears.
- Step 4** In the Replication Components table, select the **Receive** check box for each database component to be received from a primary Cisco Secure ACS.
For more information about replication components, see [Replication Components Options, page 9-11](#).
- Step 5** Make sure that no Cisco Secure ACS that the secondary Cisco Secure ACS is to receive replicated components from is included in the Replication list. If so, select the primary Cisco Secure ACS in the Replication list and click the <-- (left arrow) to move it to the AAA Servers list.



Note Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it aborts replication.

- Step 6** If the secondary Cisco Secure ACS is to receive replication components from *only one* primary Cisco Secure ACS, from the Accept replication from list, select the name of the primary Cisco Secure ACS.
The primary Cisco Secure ACSes available in the Accept replication from list are determined by the AAA Servers table in the Network Configuration section. For more information about the AAA Servers table, see [AAA Server Configuration, page 4-22](#).



Note On the primary Cisco Secure ACS and all secondary Cisco Secure ACSes, the AAA Servers table entries for the primary Cisco Secure ACS must have identical shared secrets.

Step 7 If the secondary Cisco Secure ACS is to receive replication components from *more than one* primary Cisco Secure ACS, from the Accept replication from list, select **Any Known CiscoSecure ACS Server**.

The Any Known CiscoSecure ACS Server option is limited to the Cisco Secure ACSes listed in the AAA Servers table in Network Configuration.



Note For each primary Cisco Secure ACS for this secondary Cisco Secure ACS, on both the primary and secondary Cisco Secure ACS, the AAA Servers table entries for the primary Cisco Secure ACS must have identical shared secrets.

Step 8 Click **Submit**.

Cisco Secure ACS saves the replication configuration, and at the frequency or times you specified, Cisco Secure ACS begins accepting the replicated components from the other Cisco Secure ACSes you specified.

Replicating Immediately

You can manually start database replication.



Note Replication cannot occur until you have configured at least one secondary Cisco Secure ACS. For more information about configuring a secondary Cisco Secure ACS, see [Configuring a Secondary Cisco Secure ACS, page 9-17](#).

Before You Begin

Ensure correct configuration of the primary and secondary Cisco Secure ACSes. For detailed steps, see [Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes, page 9-16](#).

For each secondary Cisco Secure ACS that this Cisco Secure ACS is to send replicated components to, make sure that you have completed the steps in [Configuring a Secondary Cisco Secure ACS, page 9-17](#).

To initiate database replication immediately, follow these steps:

-
- Step 1** Log in to the HTML interface on the primary Cisco Secure ACS.
 - Step 2** In the navigation bar, click **System Configuration**.
 - Step 3** Click **CiscoSecure Database Replication**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Select the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

- Step 4** For each CiscoSecure database component you want to replicate to a secondary Cisco Secure ACS, under Replication Components, select the corresponding **Send** check box.
- Step 5** For each secondary Cisco Secure ACS that you want the primary Cisco Secure ACS to replicate its select components to, select the secondary Cisco Secure ACS from the AAA Servers list, and then click --> (right arrow button).



Tip If you want to remove a secondary Cisco Secure ACSes from the Replication list, select the secondary Cisco Secure ACS in the Replication list, and then click <-- (left arrow button).



Note Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.

Step 6 In the **Replication timeout** text box, specify how long this Cisco Secure ACS will perform replication to each of its secondary Cisco Secure ACS before terminating the replication attempt and restarting the CSAuth service.

Step 7 At the bottom of the browser window, click **Replicate Now**.

Cisco Secure ACS saves the replication configuration. Cisco Secure ACS immediately begins sending replicated database components to the secondary Cisco Secure ACSes you specified.



Note Replication only occurs when the database of the primary Cisco Secure ACS has changed since the last successful replication. You can force replication to occur by making one change to a user or group profile, such as changing a password or RADIUS attribute.

Scheduling Replication

You can schedule when a primary Cisco Secure ACS sends its replicated database components to a secondary Cisco Secure ACS. For more information about replication scheduling options, see [Outbound Replication Options, page 9-12](#).



Note Replication cannot occur until the secondary Cisco Secure ACSes are configured properly. For more information, see [Configuring a Secondary Cisco Secure ACS, page 9-17](#).

Before You Begin

Ensure correct configuration of the primary and secondary Cisco Secure ACSes. For detailed steps, see [Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes, page 9-16](#).

For each secondary Cisco Secure ACS of this primary Cisco Secure ACS, ensure that you have completed the steps in [Configuring a Secondary Cisco Secure ACS, page 9-17](#).

To schedule when a primary Cisco Secure ACS replicates to its secondary Cisco Secure ACSes, follow these steps:

-
- Step 1 Log in to the HTML interface on the primary Cisco Secure ACS.
 - Step 2 In the navigation bar, click **System Configuration**.
 - Step 3 Click **CiscoSecure Database Replication**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Select the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

- Step 4 To specify which CiscoSecure database components the primary Cisco Secure ACS should send to its secondary Cisco Secure ACSes, under Replication Components, select the corresponding **Send** check box for each database component to be sent.

For more information about replicated database components, see [Replication Components Options, page 9-11](#).

- Step 5 To have the primary Cisco Secure ACS send replicated database components to its secondary Cisco Secure ACSes at regular intervals, under Replication Scheduling, select the **Every X minutes** option and in the X box type the length of the interval at which Cisco Secure ACS should perform replication (up to 7 characters).



Note Because Cisco Secure ACS is momentarily shut down during replication, a short replication interval may cause frequent failover of your AAA clients to other Cisco Secure ACSes. If AAA clients are not configured to failover to other Cisco Secure ACSes, the brief interruption in authentication service may prevent users from authenticating. For more information, see [Replication Frequency, page 9-7](#).

- Step 6** If you want to schedule times at which the primary Cisco Secure ACS sends its replicated database components to its secondary Cisco Secure ACSes, follow these steps:
- In the Outbound Replication table, select the **At specific times** option.
 - In the day and hour graph, click the times at which you want Cisco Secure ACS to perform replication.

**Tip**

Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click Clear All to clear all hours, or you can click Set All to select all hours.

- Step 7** If you want to have this Cisco Secure ACS send replicated database components immediately upon receiving replicated database components from another Cisco Secure ACS, select the **Automatically triggered cascade** option.

**Note**

If you specify the Automatically triggered cascade option, you must configure another Cisco Secure ACS to act as a primary Cisco Secure ACS to this Cisco Secure ACS; otherwise, this Cisco Secure ACS never replicates to its secondary Cisco Secure ACSes.

- Step 8** You must specify the secondary Cisco Secure ACSes that this Cisco Secure ACS should replicate to. To do so, follow these steps:

**Note**

Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated database components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated database components. If so, it rejects the components. For more information about replication partners, see [Inbound Replication Options, page 9-15](#).

- In the Outbound Replication table, from the AAA Servers list, select the name of a secondary Cisco Secure ACS to which you want the primary Cisco Secure ACS to send its selected replicated database components.



Note The secondary Cisco Secure ACSes available in the AAA Servers list are determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see [AAA Server Configuration, page 4-22](#).

- b. Click --> (right arrow button).

The selected secondary Cisco Secure ACS moves to the Replication list.

- c. Repeat Step a and Step b for each secondary Cisco Secure ACS to which you want the primary Cisco Secure ACS to send its selected replicated database components.

Step 9 In the **Replication timeout** text box, specify how long this Cisco Secure ACS will perform replication to each of its secondary Cisco Secure ACS before terminating the replication attempt and restarting the CSAuth service.

Step 10 Click **Submit**.

Cisco Secure ACS saves the replication configuration you created.

Disabling CiscoSecure Database Replication

You can disable scheduled CiscoSecure database replications without losing the schedule itself. This allows you to cease scheduled replications temporarily and later resume them without having to re-enter the schedule information.

To disable CiscoSecure database replication, follow these steps:

Step 1 Log in to the HTML interface on the primary Cisco Secure ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **CiscoSecure Database Replication**.

The Database Replication Setup page appears.

Step 4 In the Replication Components table, clear all check boxes.

Step 5 In the Outbound Replication table, select the **Manually** option.

Step 6 Click **Submit**.

Cisco Secure ACS does not permit any replication to or from this Cisco Secure ACS server.

Database Replication Event Errors

The Database Replication report contains messages indicating errors that occur during replication. For more information about the Database Replication report, see [Cisco Secure ACS System Logs, page 11-12](#).

RDBMS Synchronization

This section provides information about the RDBMS Synchronization feature, including procedures for implementing this feature, within both Cisco Secure ACS and the external data source involved.

This section contains the following topics:

- [About RDBMS Synchronization, page 9-26](#)
 - [Users, page 9-27](#)
 - [User Groups, page 9-27](#)
 - [Network Configuration, page 9-28](#)
 - [Custom RADIUS Vendors and VSAs, page 9-28](#)
- [RDBMS Synchronization Components, page 9-29](#)
 - [About CSDBSync, page 9-29](#)
 - [About the accountActions File, page 9-30](#)
- [Cisco Secure ACS Database Recovery Using the accountActions Table, page 9-30](#)
- [Preparing to Use RDBMS Synchronization, page 9-31](#)

- [RDBMS Synchronization Options, page 9-33](#)
 - [FTP Setup Options, page 9-33](#)
 - [Synchronization Scheduling Options, page 9-34](#)
 - [Synchronization Partners Options, page 9-34](#)
- [Performing RDBMS Synchronization Immediately, page 9-35](#)
- [Scheduling RDBMS Synchronization, page 9-36](#)
- [Disabling Scheduled RDBMS Synchronizations, page 9-39](#)

About RDBMS Synchronization

The RDBMS Synchronization feature provides the ability to update the CiscoSecure user database with information from a text file on an FTP server. The text file can be generated by a third-party application. Cisco Secure ACS gets the file from the FTP server, reads the file, and performs the configuration actions specified in the file. You can also regard RDBMS Synchronization as an API—much of what you can configure for a user, group, or device through the Cisco Secure ACS HTML interface, you can alternatively maintain through this feature. RDBMS Synchronization supports addition, modification, and deletion for all data items it can access.

You can configure synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the CiscoSecure user database on demand.

Synchronization performed by a single Cisco Secure ACS can update the internal databases of other Cisco Secure ACSes, so that you only need configure RDBMS Synchronization on one Cisco Secure ACS. Communication between Cisco Secure ACSes for the purposes of RDBMS Synchronization occurs using an encrypted, Cisco-proprietary protocol. Cisco Secure ACSes listen on TCP port 2000 for synchronization data.

Users

Among the user-related configuration actions that RDBMS Synchronization can perform are the following:

- Adding users.
- Deleting users.
- Setting passwords.
- Setting user group memberships.
- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Assigning IP addresses.
- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.



Note

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).

User Groups

Among the group-related configuration actions that RDBMS Synchronization can perform are the following:

- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.

- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.

**Note**

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).

Network Configuration

Among the network device-related configuration actions that RDBMS Synchronization can perform are the following:

- Adding AAA clients.
- Deleting AAA clients.
- Setting AAA client configuration details.
- Adding AAA servers.
- Deleting AAA servers.
- Setting AAA server configuration details.
- Adding and configuring Proxy Distribution Table entries.

**Note**

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).

Custom RADIUS Vendors and VSAs

RDBMS Synchronization enables you to configure custom RADIUS vendors and VSAs. In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), Cisco Secure ACS supports RADIUS vendors and VSAs that you define. Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26.

You can define up to ten custom RADIUS vendors. Cisco Secure ACS allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and by the vendor name.

**Note**

If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACSes, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see [CiscoSecure Database Replication, page 9-1](#).

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).

RDBMS Synchronization Components

The RDBMS Synchronization feature comprises two components:

- **CSDBSync**—A service that performs automated user and group account management services for Cisco Secure ACS.
- **accountActions File**—The file that holds information used by CSDBSync to update the CiscoSecure user database.

About CSDBSync

The CSDBSync service reads the accountActions file. While “accountActions.csv” is the default name for the accountActions file, you can name the file however you like. Synchronization events fail if CSDBSync cannot access the accountActions file.

CSDBSync reads each record from the accountActions file and updates the CiscoSecure user database as specified by the action code in the record. For example, a record could instruct CSDBSync to add a user or change a user password. In a distributed environment, a single Cisco Secure ACS, known as the senior synchronization partner, accesses the accountActions table and sends synchronization commands to its synchronization partners.

**Note**

The senior synchronization partner must have AAA configurations for each Cisco Secure ACS that is a synchronization partners. In turn, each of the synchronization partners must have a AAA server configuration for the senior

partner. Synchronization commands from the senior partner are ignored if the Cisco Secure ACS receiving the synchronization commands does not have a AAA server configuration for the senior partner.

For more information about CSDBSync or other Windows services used by Cisco Secure ACS, see [Chapter 1, “Overview”](#).

About the accountActions File

The accountActions file contains a set of rows that define actions CSDBSync is to perform in the CiscoSecure user database. Each row in the accountActions file holds user, user group, or AAA client information. Except for the first row (which is used for field headers and thus is ignored during synchronization), each row also contains an action field and several other fields. These fields provide CSDBSync with the information it needs to update the CiscoSecure user database.

For full details of the accountActions file format and available actions, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).

Cisco Secure ACS Database Recovery Using the accountActions Table

Combining all instances of accountActions files in the order they were processed by RDBMS Synchronization produces, in effect, a transaction queue. The RDBMS Synchronization feature does not maintain a transaction log/audit trail. If a log is required, the external system that generates accountActions files must create it. Unless the external system can recreate the entire transaction history in the accountActions file, we recommend that you construct a transaction log file for recovery purposes. To do this, create a transaction log file that is stored in a safe location and backed up on a regular basis. In that second file, mirror all the additions and updates to records in the accountActions file. The transaction log file would therefore be a concatenation of all actions recorded in the many instances of the accountActions file processed by RDBMS Synchronization.

If the database is large, it is not practical to recreate the CiscoSecure user database by replaying the transaction log for the entire history of the system. Instead, create regular backups of the CiscoSecure user database and replay the transaction logs

from the time of most recent backup to bring the CiscoSecure user database back in synchronization with the external system. For information on creating backup files, see [Cisco Secure ACS Backup, page 8-8](#).

Replaying transaction logs that slightly predate the checkpoint does not damage the CiscoSecure user database, although some transactions might be invalid and reported as errors. As long as the entire transaction log is replayed, the CiscoSecure user database is consistent with the database of the external system.

Preparing to Use RDBMS Synchronization

Synchronizing the CiscoSecure user database using data from a `accountActions` file requires that you complete several significant steps external to Cisco Secure ACS before configuring the RDBMS Synchronization feature within Cisco Secure ACS.

To prepare to use RDBMS Synchronization, follow these steps:

-
- Step 1** Determine the following items:
- How to create the `accountActions` file. For more information about the `accountActions` file, see [About the accountActions File, page 9-30](#). For details on the format and content of the `accountActions` file, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).
 - The FTP server you want to use to make the `accountActions` file accessible to Cisco Secure ACS.
 - How to copy the `accountActions` file to the applicable directory on the FTP server, if the `accountActions` file is generated in a directory different from the directory that Cisco Secure ACS is to get it from on the FTP server.
- Step 2** Configure your third-party system to generate the `accountActions` file periodically. The mechanism for maintaining your `accountActions` file is unique to your implementation. If the third-party system you are using to update the `accountActions` file is a commercial product, for assistance, refer to the documentation supplied by your third-party system vendor.
- For information about the format and content of the `accountActions` file, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).
- Step 3** If needed, configure the mechanism that is to copy the `accountActions` file from where it is generated to the applicable directory on the FTP server.

- Step 4** Validate that your third-party system updates the accountActions file properly. Rows generated in the accountActions file must be valid. For details on the format and content of the accountActions file, see [Appendix E, “RDBMS Synchronization Import Definitions”](#).



Note After testing that the third-party system updates the accountActions file properly, discontinue updating the accountActions file until after you have completed [Step 6](#).

- Step 5** If you have a distributed AAA environment and want to synchronize multiple Cisco Secure ACSes, follow these steps:
- Determine which Cisco Secure ACS you want to use to communicate with the third-party system. This is the senior synchronization partner, which you will later configure to send synchronization data to its synchronization partners, which are the other Cisco Secure ACSes needing synchronization.
 - On the senior synchronization partner, verify that there is a AAA server configuration for each synchronization partner. Add AAA server configuration for each missing synchronization partner. For detailed steps about adding a AAA server, see [Adding a AAA Server, page 4-25](#).
 - On all the other synchronization partners, verify that there is a AAA server configuration for the senior synchronization partner. If no AAA server configuration for the senior synchronization partner exists, create one. For detailed steps about adding a AAA server, see [Adding a AAA Server, page 4-25](#).

Synchronization between the senior synchronization partner and the other synchronization partners is enabled.

- Step 6** Schedule RDBMS synchronization on the senior synchronization partner. For steps, see [Scheduling RDBMS Synchronization, page 9-36](#).
- Step 7** Configure your third-party system to begin updating the accountActions file with information to be imported into the CiscoSecure user database. If needed, activate the mechanism that is to copy the accountActions file to the applicable directory on the FTP server.

- Step 8** Confirm that RDBMS synchronization is operating properly by monitoring the RDBMS Synchronization report in the Reports and Activity section. For more information about the RDBMS Synchronization log, see [Cisco Secure ACS System Logs, page 11-12](#).

Also, monitor the CSDBSync service log. For more information about the CSDBSync service log, see [Service Logs, page 11-25](#).

RDBMS Synchronization Options

The RDBMS Synchronization Setup page, available from System Configuration, provides control of the RDBMS Synchronization feature. It contains three tables whose options are described in this section.

This section contains the following topics:

- [FTP Setup Options, page 9-33](#)
- [Synchronization Scheduling Options, page 9-34](#)
- [Synchronization Partners Options, page 9-34](#)

FTP Setup Options

The FTP Setup For Account Actions Download table defines how Cisco Secure ACS accesses the accountActions table. It contains the following options:

- **Actions File**—The name of the accountActions file. The default name is “actions.csv”. The filename provided must match the name of the accountActions file on the FTP server.
- **FTP Server**—The IP address or hostname of the FTP server that Cisco Secure ACS is to get the accountActions file from. If you specify a hostname, DNS must be enabled on your network.
- **Directory**—The relative path from the FTP server root directory to the directory where the accountActions file is. To specify the FTP root directory, enter a single period or “dot”.
- **Username**—A valid username to enable Cisco Secure ACS to access the FTP server.
- **Password**—The password for the username provided in the Login box.

Synchronization Scheduling Options

The Synchronization Scheduling table defines when synchronization occurs. It contains the following scheduling options:

- **Manually**—Cisco Secure ACS does not perform automatic RDBMS synchronization.
- **Every X minutes**—Cisco Secure ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times...**—Cisco Secure ACS performs synchronization at the time specified in the day and hour graph. The minimum interval is one hour, and the synchronization takes place on the hour selected.

Synchronization Partners Options

The Synchronization Partners table defines which Cisco Secure ACSes are synchronized with data from the accountActions table. It provides the following options:

- **AAA Server**—This list represents the AAA servers configured in the AAA Servers table in Network Configuration for which the Cisco Secure ACS *does not* perform RDBMS synchronization.
- **Synchronize**—This list represents the AAA servers configured in the AAA Servers table in Network Configuration for which the Cisco Secure ACS *does* perform RDBMS synchronization. The AAA servers on this list are the synchronization partners of this Cisco Secure ACS. During synchronization, communication between this Cisco Secure ACS and its synchronization partners is 128-bit encrypted with a Cisco-proprietary protocol. The synchronization partners receive synchronization data on TCP port 2000.



Note

Each synchronization partner *must* have a AAA server configuration in its Network Configuration section that corresponds to this Cisco Secure ACS; otherwise, the synchronization commands this Cisco Secure ACS sends to it are ignored.

For more information about the AAA Servers table in Network Configuration, see [AAA Server Configuration, page 4-22](#).

Performing RDBMS Synchronization Immediately

You can manually start an RDBMS synchronization event.

To perform manual RDBMS synchronization, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **RDBMS Synchronization** check box.

The RDBMS Synchronization Setup page appears.

The status of the CSDBSync service appears below the page title.

Step 3 To specify options in the FTP Setup For Account Actions Download table, follow these steps:



Note For more information about FTP setup, see [FTP Setup Options, page 9-33](#).

- a. In the Actions Files box, type the name of the accountActions file that you want to use to update Cisco Secure ACS.
- b. In the FTP Server box, type the IP address or hostname of the FTP server that you want Cisco Secure ACS to get the accountActions file from.
- c. In the Directory box, type the relative path to the directory on the FTP server where the accountActions file is.
- d. In the Username box, type a valid username to enable Cisco Secure ACS to access the FTP server.
- e. In the Password box, type the password for the username provided in the Login box.

Cisco Secure ACS has the information necessary to get the accountActions file from the FTP server.



Note It is *not* necessary to select **Manually** under **Replication Scheduling**. For more information, see [Disabling Scheduled RDBMS Synchronizations](#), page 9-39.

Step 4 For each Cisco Secure ACS that you want this Cisco Secure ACS to update using the actions in the `accountActions` file, select the Cisco Secure ACS in the **AAA Servers** list, and then click --> (right arrow button).



Note The Cisco Secure ACSes available in the **AAA Servers** list is determined by the **AAA Servers** table in **Network Configuration**, with the addition of the name of the current Cisco Secure ACS server. For more information about the **AAA Servers** table, see [AAA Server Configuration Options](#), page 4-23.

The selected Cisco Secure ACS appears in the **Synchronize** list.



Note At least one Cisco Secure ACS must be in the **Synchronize** list. This includes the Cisco Secure ACS on which you are configuring RDBMS Synchronization. RDBMS Synchronization does not automatically include the internal database of the current Cisco Secure ACS.

Step 5 To remove Cisco Secure ACSes from **Synchronize** list, select the Cisco Secure ACS in the **Synchronize** list, and then click <-- (left arrow button).

The selected Cisco Secure ACS appears in the **AAA Servers** list.

Step 6 At the bottom of the browser window, click **Synchronize Now**.

Cisco Secure ACS immediately begins a synchronization event. To check on the status of the synchronization, view the RDBMS Synchronization report in **Reports and Activity**.

Scheduling RDBMS Synchronization

You can schedule when a Cisco Secure ACS performs RDBMS synchronization.

To schedule when a Cisco Secure ACS performs RDBMS synchronization, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **RDBMS Synchronization** check box.

The RDBMS Synchronization Setup page appears.

The status of the CSDBSync service appears below the page title.

Step 3 To specify options in the FTP Setup For Account Actions Download table, follow these steps:



Note For more information about FTP setup, see [FTP Setup Options, page 9-33](#).

- a. In the Actions Files box, type the name of the accountActions file that you want to use to update Cisco Secure ACS.
- b. In the FTP Server box, type the IP address or hostname of the FTP server that you want Cisco Secure ACS to get the accountActions file from.
- c. In the Directory box, type the relative path to the directory on the FTP server where the accountActions file is.
- d. In the Username box, type a valid username to enable Cisco Secure ACS to access the FTP server.
- e. In the Password box, type the password for the username provided in the Login box.

Cisco Secure ACS has the information necessary to get the accountActions file from the FTP server.

Step 4 To have this Cisco Secure ACS perform RDBMS synchronization at regular intervals, under Synchronization Scheduling, select the **Every X minutes** option and in the X box type the length of the interval at which Cisco Secure ACS should perform synchronization (up to 7 characters).

- Step 5** To schedule times at which this Cisco Secure ACS performs RDBMS synchronization, follow these steps:
- Under Synchronization Scheduling, select the **At specific times** option.
 - In the day and hour graph, click the times at which you want Cisco Secure ACS to perform replication.

**Tip**

Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

- Step 6** For each Cisco Secure ACS you want to synchronize using the actions in the accountActions file, follow these steps:

**Note**

For more information about synchronization targets, see [Inbound Replication Options, page 9-15](#).

- In the Synchronization Partners table, from the AAA Servers list, select the name of a Cisco Secure ACS that you want this Cisco Secure ACS to update with data from the accountActions file.

**Note**

The Cisco Secure ACSes available in the AAA Servers list is determined by the AAA Servers table in Network Configuration, with the addition of the name of the current Cisco Secure ACS server. For more information about the AAA Servers table, see [AAA Server Configuration Options, page 4-23](#).

- Click --> (right arrow button).

The selected Cisco Secure ACS moves to the Synchronize list.

**Note**

At least one Cisco Secure ACS must be in the Synchronize list. This includes the Cisco Secure ACS on which you are configuring RDBMS Synchronization. RDBMS Synchronization does not automatically include the internal database of the current Cisco Secure ACS.

Step 7 Click **Submit**.

Cisco Secure ACS saves the RDBMS synchronization schedule you created.

Disabling Scheduled RDBMS Synchronizations

You can disable scheduled RDBMS synchronization events without losing the schedule itself. This allows you to end scheduled synchronizations and resume them later without having to re-create the schedule.

To disable scheduled RDBMS synchronizations, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

Step 3 Under Synchronization Scheduling, select the **Manually** option.

Step 4 Click **Submit**.

Cisco Secure ACS does not perform scheduled RDBMS synchronizations.

IP Pools Server

This section provides information about the IP Pools feature, including procedures for creating and maintaining IP pools.

This section contains the following topics:

- [About IP Pools Server, page 9-40](#)
- [Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges, page 9-41](#)
- [Refreshing the AAA Server IP Pools Table, page 9-42](#)
- [Adding a New IP Pool, page 9-43](#)
- [Editing an IP Pool Definition, page 9-44](#)
- [Resetting an IP Pool, page 9-45](#)
- [Deleting an IP Pool, page 9-46](#)

About IP Pools Server

If you are using VPNs you may have to overlap IP address assignments; that is, it may be advantageous for a PPTP tunnel client within a given tunnel to use the same IP address as that used by another PPTP tunnel client in a different tunnel. The IP Pools Server feature enables you to assign the same IP address to multiple users, provided that the users are being tunnelled to different home gateways for routing beyond the boundaries of your own network. This means you can conserve your IP address space without having to resort to using illegal addresses. When you enable this feature, Cisco Secure ACS dynamically issues IP addresses from the IP pools you have defined by number or name. You can configure up to 999 IP pools, for approximately 255,000 users.

If you are using IP pooling and proxy, all accounting packets are proxied so that the Cisco Secure ACS that is assigning the IP addresses can confirm whether an IP address is already in use.



Note

IP pool definitions are not replicated by the CiscoSecure Database Replication feature; however, user and group assignments to IP pools are replicated. By not replicating IP pool definitions, Cisco Secure ACS avoids inadvertently assigning an IP address that a replication partner has already assigned to a different workstation. To support IP pools in a AAA environment that uses replication, you must manually configure each secondary Cisco Secure ACS to have IP pools with names identical to the IP pools defined on the primary Cisco Secure ACS.

To use IP pools, the AAA client must have network authorization (in IOS, **aaa authorization network**) and accounting (in IOS, **aaa accounting**) enabled.

**Note**

To use the IP Pools feature, you must set up your AAA client to perform authentication and accounting using the same protocol — either TACACS+ or RADIUS.

For information on assigning a group or user to an IP pool, see [Setting IP Address Assignment Method for a User Group, page 6-28](#), or [Assigning a User to a Client IP Address, page 7-9](#).

Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges

Cisco Secure ACS provides automated detection of overlapping pools.

**Note**

To use overlapping pools, you must be using RADIUS with VPN, and you cannot be using Dynamic Host Configuration Protocol (DHCP).

You can determine whether overlapping IP pools are allowed by checking which button appears below the AAA Server IP Pools table:

- **Allow Overlapping Pool Address Ranges**—Indicates that overlapping IP pool address ranges are *not allowed*. Clicking this button allows IP address ranges to overlap between pools.
- **Force Unique Pool Address Range**—Indicates that overlapping IP pool address ranges are *allowed*. Clicking this button prevents IP address ranges from overlapping between pools.

To allow overlapping IP pools or to force unique pool address ranges, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **IP Pools Server**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **IP Pools** check box.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

- Step 3** If you want to allow overlapping IP pool address ranges, follow these steps:
- If the Allow Overlapping Pool Address Ranges button appears, click that button.
Cisco Secure ACS allows overlapping IP pool address ranges.
 - If the Force Unique Pool Address Range button appears, do nothing.
Cisco Secure ACS already allows overlapping IP pool address ranges.
- Step 4** If you want to deny overlapping IP pool address ranges, follow these steps:
- If the Allow Overlapping Pool Address Ranges button appears, do nothing.
Cisco Secure ACS already does not permit overlapping IP pool address ranges.
 - If the Force Unique Pool Address Range button appears, click that button.
Cisco Secure ACS does not permit overlapping IP pool address ranges.
-

Refreshing the AAA Server IP Pools Table

You can refresh the AAA Server IP Pools table. This allows you to get the latest usage statistics for your IP pools.

To refresh the AAA Server IP Pools table, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click **Refresh**.

Cisco Secure ACS updates the percentages of pooled addresses in use.

Adding a New IP Pool

You can define up to 999 IP address pools.

To add an IP pool, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have already configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click **Add Entry**.

The New Pool table appears.

Step 4 In the Name box, type the name (up to 31 characters) you want to assign to the new IP pool.

Step 5 In the Start Address box, type the lowest IP address (up to 15 characters) of the range of addresses for the new pool.



Note All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.


Step 6 In the End Address box, type the highest IP address (up to 15 characters) of the range of addresses for the new pool.

Step 7 Click **Submit**.

The new IP pool appears in the AAA Server IP Pools table.

Editing an IP Pool Definition

To edit an IP pool definition, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.
- The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.
- Step 3** Click the name of the IP pool you need to edit.
- The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays how many IP addresses in this pool are allocated to a user. The Available field displays how many IP addresses are unallocated to users.
- Step 4** To change the name of the pool, in the Name box, type the name (up to 31 characters) to which you want to change the IP pool.
- Step 5** To change the starting address of the pool range of IP addresses, in the Start Address box, type the lowest IP address (up to 15 characters) of the new range of addresses for the pool.
-  **Note** All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.
-
- Step 6** To change the ending address of the pool range of IP addresses, in the End Address box, type the highest IP address (up to 15 characters) of the new range of addresses for the pool.
- Step 7** Click **Submit**.
- The edited IP pool appears in the AAA Server IP Pools table.
-

Resetting an IP Pool

The Reset function recovers IP addresses within an IP pool when there are “dangling” connections. A dangling connection occurs when a user disconnects and Cisco Secure ACS does not receive an accounting stop packet from the applicable AAA client. If the Failed Attempts log in Reports and Activity shows a large number of “Failed to Allocate IP Address For User” messages, consider using the Reset function to reclaim all allocated addresses in this IP pool.



Note

Using the Reset function to reclaim all allocated IP addresses in a pool can result in users being assigned addresses that are already in use.

To reset an IP pool and reclaim all its IP addresses, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.
- The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.
- Step 3** Click the name of the IP pool you need to reset.
- The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays how many IP addresses in this pool are assigned to a user. The Available field displays how many IP addresses are not assigned to users.
- Step 4** Click **Reset**.
- Cisco Secure ACS displays a dialog box indicating the possibility of assigning user addresses that are already in use.
- Step 5** To continue resetting the IP pool, click **OK**.
- The IP pool is reset. All its IP addresses are reclaimed. In the In Use column of the AAA Server IP Pools table, zero percent of the IP pool addresses are assigned to users.
-

Deleting an IP Pool

**Note**

If you delete an IP pool that has users assigned to it, those users cannot authenticate until you edit the user profile and change their IP assignment settings. Alternatively, if the users receive their IP assignment based on group membership, you can edit the user group profile and change the IP assignment settings for the group.

To delete an IP pool, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.
- The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.
- Step 3** Click the name of the IP pool you need to delete.
- The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use column displays how many IP addresses in this pool are assigned to a user. The Available column displays how many IP addresses are not assigned to users.
- Step 4** Click **Delete**.
- Cisco Secure ACS displays a dialog box to confirm that you want to delete the IP pool.
- Step 5** To delete the IP pool, click **OK**.
- The IP pool is deleted. The AAA Server IP Pools table does not list the deleted IP pool.
-

IP Pools Address Recovery

The IP Pools Address Recovery feature enables you to recover assigned IP addresses that have not been used for a specified period of time. You must configure an accounting network on the AAA client for Cisco Secure ACS to reclaim the IP addresses correctly.

Enabling IP Pool Address Recovery

To enable IP pool address recovery, follow these steps:

-
- Step 1 In the navigation bar, click **System Configuration**.
 - Step 2 Click **IP Pools Address Recovery**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **IP Pools** check box.

The IP Address Recovery page appears.

- Step 3 Select the **Release address if allocated for longer than X hours** check box and in the X box type the number of hours (up to 4 characters) after which Cisco Secure ACS should recover assigned, unused IP addresses.
- Step 4 Click **Submit**.

Cisco Secure ACS implements the IP pools address recovery settings you made.

NAC Attribute Management

You can use the CNAC Attributes Management page to add, delete, or export NAC attributes, which are used with posture validation requests. For more information about posture validation attributes, see [About NAC Credentials and Attributes, page 14-11](#).

This section contains the following topics:

- [Posture Validation Attribute Definition File, page 9-48](#)
- [Adding NAC Attributes, page 9-52](#)
- [Deleting a NAC Attribute, page 9-54](#)
- [Exporting NAC Attributes, page 9-55](#)
- [Default Posture Validation Attribute Definition File, page 9-56](#)

Posture Validation Attribute Definition File

A posture validation attribute definition file is a text file that contains one or more posture validation attribute definitions. Each definition consists of a definition header and several values, described below. For an example of the contents of a posture validation attribute definition file, see [Default Posture Validation Attribute Definition File, page 9-56](#).

With the exception of the attribute definition header, each attribute definition value must be formatted as follows:

name=value

where *name* is the value name and *value* is a string or integer, as specified in the list below.



Tip

Use a semi-colon to identify lines that are comments.

[Example 9-1](#) shows an example of a posture validation attribute definition, including a comment after the attribute definition:

Example 9-1 Example Attribute Definition

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
; attribute 1 is reserved for the APT
```

A posture validation attribute is uniquely defined by the combination of its vendor ID, application ID, and attribute ID. The following list provides details of these values and of each line required in an attribute definition:

- **[attr#*n*]**—Attribute definition header, where *n* is a unique, sequential integer, beginning with zero. CSUtil.exe uses the definition header to distinguish the beginning of a new attribute definition. Each attribute definition *must* begin with a line containing the definition header. The first attribute definition in the file *must* have the header [attr#0], the second attribute definition in a file must have the header [attr#1], and so on. A break in the numbering causes CSUtil.exe to ignore attribute definitions at the break and beyond. For example, if a file with 10 attribute definitions the fifth attribute is defined as [attr#5] instead of [attr#4], CSUtil.exe ignores the attribute defined as [attr#5] and remaining five the attributes following it.



Tip

The value of *n* is irrelevant to any of the ID values in the attribute definition file. For example, the 28th definition in a file must have the header [attr#27], but this does not limit or otherwise define valid values for vendor-id, application-id, attribute-id. Neither does it limit or define the number of posture validation attributes supported by Cisco Secure ACS.

- **vendor-id**—An unsigned integer, the vendor number is of the vendor associated with the posture validation attribute. The vendor number should be the number assigned to the vendor in the [IANA Assigned Numbers RFC](#). For example, vendor ID 9 corresponds to Cisco Systems, Inc.

Vendor IDs have one or more applications associated with them, identified by the application-id value.

- **vendor-name**—A string, the vendor name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, any attribute definition with a vendor ID of 9 could have a vendor name “Cisco”.



Note

The vendor name cannot differ for each attribute that shares the same vendor ID. For example, you cannot add an attribute with a vendor-id of 9 if the vendor-name is not “Cisco”.

- **application-id**—An unsigned integer, the application ID uniquely identifies the vendor application associated with the posture validation attribute. For example, if the vendor ID is 9 and the application ID is 1, the posture validation attribute is associated with the Cisco application with an ID of 1, which is the Cisco Trust Agent (CTA), also known as a posture agent (PA).
- **application-name**—A string, the application name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, if the vendor ID is 9 and the application ID is 1, the application name would be “PA”, an abbreviation of posture agent, which is another term for CTA.



Note The application name cannot differ for each attribute that shares the same vendor ID and application ID pair. For example, you cannot add an attribute with a vendor-id of 9 and application ID of 1 if the application-name is not “PA”.

- **attribute-id**—An unsigned integer in the range of 1 to 65535, the attribute ID uniquely identifies the posture validation attribute for the vendor ID and application ID specified.



Note For each application, attributes 1 and 2 are reserved. If you add attributes that imply a new application, CSUtil.exe automatically creates attribute 1 as Application-Posture-Token and attribute 2 as System-Posture-Token.

- **attribute-name**—A string, the attribute name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, if the vendor ID is 9, the application ID is 1, and the attribute ID is 1, the attribute name is “Application-Posture-Token”.

- **attribute-profile**—A string, the attribute profile specifies whether Cisco Secure ACS can send the attribute in a posture validation response, can receive the attribute in a posture validation request, or can both send and receive the attribute during posture validation. Valid values for attribute-profile are:
 - **in**—Cisco Secure ACS accepts the attribute in posture validation requests and can log the attribute, and you can use it in local policy rule definitions. Attributes with an “in” attribute-profile are also known as inbound attributes.
 - **out**—Cisco Secure ACS can send the attribute in posture validation responses but you cannot use it in local policy rule definitions. Attributes with an “out” attribute-profile are also known as outbound attributes. The only outbound attributes that you can configure Cisco Secure ACS to log are the attributes for Application Posture Tokens and System Posture Tokens; however, these are system-defined attributes that you cannot modify.
 - **in out**—Cisco Secure ACS both accepts the attribute in posture validation requests and can send the attribute in posture validation responses. Attributes with an “in out” attribute-profile are also known as both inbound and outbound attributes.
- **attribute-type**—A string, the attribute type specifies the kind of data that is valid in the associated attribute. For attributes whose attribute-profile is `in` or `in out`, the attribute-type determines the types of operators available for defining local policy rules that use the attribute. An example of an inbound attribute is the ServicePacks attribute sent by CTA. An example of an outbound attribute is the System-Posture-Token attribute, sent to CTA.

Valid values of attribute-type are:

- boolean
- string
- integer
- unsigned integer
- ipaddr
- date
- version
- octet-array

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

Adding NAC Attributes

This procedure describes how you can add posture validation attributes.

This procedure describes how you can add attributes by importing posture validation attribute definitions from an attribute definition file. For an explanation of the contents of a posture validation attribute definition file, see [Posture Validation Attribute Definition File, page 9-48](#). For an example of an attribute definition file, see [Default Posture Validation Attribute Definition File, page 9-56](#).

Before You Begin

Because completing this procedure requires restarting the CSAuth service, which temporarily suspends authentication services, consider performing this procedure when demand for Cisco Secure ACS services is low.

Use the steps in [Exporting NAC Attributes, page 9-55](#), to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of current posture validation attributes.

To add NAC attributes, follow these steps:

-
- Step 1** Use the discussion in [Posture Validation Attribute Definition File, page 9-48](#) to create a properly formatted attribute definition file.
 - Step 2** Place the attribute definition file in a directory that Cisco Secure ACS can access using FTP.
 - Step 3** In the navigation bar, click **System Configuration**.
 - Step 4** Click **CNAC Attribute Management**.
The CNAC Attribute Management page appears. Under Add Attributes, the FTP Server, Login, Password, and Remote Directory options contain the values from the most recent previous session on this page.
 - Step 5** Select the **Add Attributes** option.

Step 6 Provide the details required to transfer the attribute definition file to Cisco Secure ACS. To do so, follow these steps:

- a. In the **FTP Server** box, type the IP address or hostname of the FTP server that has the attribute definition file you want to download.



Tip If you specify the hostname, DNS must be working correctly on your network.

- b. In the **Login** box, type a valid username that Cisco Secure ACS can use to access the FTP server.
- c. In the **Password** box, type the password for the username you specified in the Login box.
- d. In the **Remote Directory** box, type relative path from the FTP server root directory to the directory containing the attribute definition file you want Cisco Secure ACS to download from the FTP server.
- e. In the **Attributes File Name** box, type the name of the attribute definition file you want Cisco Secure ACS to download from the FTP server.

Step 7 Click **Submit**.

Cisco Secure ACS downloads the attribute definition file and updates its attribute definitions according to the information you provided in the file. The System Configuration page appears.



Tip If Cisco Secure ACS has problems transferring the file, a self-explanatory error message appears in the page on the right.

Step 8 If you have no more changes to make to the attribute definitions in Cisco Secure ACS and you want your changes to take effect, restart the following services:

- **CSAuth and CSLog**—See [Stopping, Starting, or Restarting Services, page 8-2](#).
 - **CSAdmin**—Use the **restart** command at the console. For more information about this command, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.
-

Deleting a NAC Attribute

This procedure describes how you can delete a posture validation attribute.



Caution

Cisco Secure ACS provides no confirmation step when you delete a posture validation attribute. Be sure you use the steps in [Exporting NAC Attributes, page 9-55](#) to create a backup of posture validation attribute definitions.

Before You Begin

Because completing this procedure requires restarting the CSAuth service, which temporarily suspends authentication services, consider performing this procedure when demand for Cisco Secure ACS services is low.

Use the steps in [Exporting NAC Attributes, page 9-55](#) to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of the posture validation attribute you want to delete.

For more information about posture validation attributes and how they are identified, see [About NAC Credentials and Attributes, page 14-11](#).

To delete a NAC attribute, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **CNAC Attribute Management**.
- The CNAC Attribute Management page appears.
- Step 3** Select the **Delete Attribute** option.
- Step 4** Provide the details required to identify the attribute that you want Cisco Secure ACS to delete. To do so, follow these steps:
- In the **Vendor ID** box, type the number that identifies the vendor.
 - In the **Application ID** box, type the number that identifies the application.
 - In the **Attribute ID** box, type the number that identifies the attribute.
- The attribute you want to delete is uniquely identified.
- Step 5** Click **Submit**.
- Cisco Secure ACS deletes its definition for the attribute you specified.

- Step 6** If you have no more changes to make to the attribute definitions in Cisco Secure ACS and you want your changes to take effect, restart the following services:
- **CSAuth and CSLog**—See [Stopping, Starting, or Restarting Services](#), page 8-2.
 - **CSAdmin**—Use the **restart** command at the console. For more information about this command, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.
-

Exporting NAC Attributes

This procedure describes how you can download an attribute definition file for all the posture validation attributes currently defined in Cisco Secure ACS. This file is especially useful as a backup for attribute definitions and as a reference for existing definitions prior to adding, modifying, or deleting attributes.

To export a file of definitions for all NAC attributes, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **CNAC Attribute Management**.
- The CNAC Attribute Management page appears.
- Step 3** Select the **Dump Attributes** option.
- Step 4** Click **Submit**.
- A message about file generation status appears.
- Step 5** If the status message indicates the file is not ready, click **Refresh** until the file is ready.
- Step 6** Click **Download**.
- A dialog box prompts you for a location to save a file named AvpDump.txt. “AVP” is an abbreviation for “attribute-value pair”.
- Step 7** Choose a location for saving the file and, if you prefer, change the name of the file to a more meaningful name.

**Tip**

Consider identifying the attribute definition file by the hostname of Cisco Secure ACS and the current date. For example, if the hostname is acs01primary and the date is June 13, 2004, saving the file as avp-acs01primary-06132004.txt would readily identify the origin of the file.

Step 8 Save the file.

Cisco Secure ACS continues to display the status message.

**Tip**

To leave this page, you can click Cancel, Refresh, or any of the buttons on the navigation bar.

Default Posture Validation Attribute Definition File

[Example 9-2](#) provides the definitions for the posture validation attributes that we provide with Cisco Secure ACS. Should you need to reset the default attributes to their original definitions, use [Example 9-2](#) to create a posture validation attribute definition file. For more information about the format of an attribute definition file, see [Posture Validation Attribute Definition File, page 9-48](#).

Example 9-2 Default Posture Validation Attribute Definitions

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#1]
vendor-id=9
vendor-name=Cisco
application-id=1
```

```
application-name=PA
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#2]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00003
attribute-name=PA-Name
attribute-profile=in out
attribute-type=string
```

```
[attr#3]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00004
attribute-name=PA-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#4]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00005
attribute-name=OS-Type
attribute-profile=in out
attribute-type=string
```

```
[attr#5]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00006
attribute-name=OS-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#6]
vendor-id=9
```

```
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00007
attribute-name=PA-User-Notification
attribute-profile=out
attribute-type=string

[attr#7]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#8]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#9]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00006
attribute-name=ServicePacks
attribute-profile=in
attribute-type=string

[attr#10]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00007
attribute-name=HotFixes
attribute-profile=in
attribute-type=string
```

```
[attr#11]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00008
attribute-name=HostFQDN
attribute-profile=in
attribute-type=string
```

```
[attr#12]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#13]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#14]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00005
attribute-name=CSAVersion
attribute-profile=in
attribute-type=version
```

```
[attr#15]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00009
attribute-name=CSAOperationalState
attribute-profile=in
```

```
attribute-type=unsigned integer
```

```
[attr#16]  
vendor-id=9  
vendor-name=Cisco  
application-id=5  
application-name=HIP  
attribute-id=00011  
attribute-name=TimeSinceLastSuccessfulPoll  
attribute-profile=in  
attribute-type=unsigned integer
```

```
[attr#17]  
vendor-id=9  
vendor-name=Cisco  
application-id=5  
application-name=HIP  
attribute-id=32768  
attribute-name=CSAMCName  
attribute-profile=in  
attribute-type=string
```

```
[attr#18]  
vendor-id=9  
vendor-name=Cisco  
application-id=5  
application-name=HIP  
attribute-id=32769  
attribute-name=CSAStates  
attribute-profile=in  
attribute-type=string
```

```
[attr#19]  
vendor-id=393  
vendor-name=Symantec  
application-id=3  
application-name=AV  
attribute-id=00001  
attribute-name=Application-Posture-Token  
attribute-profile=out  
attribute-type=unsigned integer
```

```
[attr#20]  
vendor-id=393  
vendor-name=Symantec  
application-id=3  
application-name=AV  
attribute-id=00002
```

```
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#21]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string
```

```
[attr#22]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#23]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#24]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00006
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#25]
vendor-id=393
vendor-name=Symantec
application-id=3
```

```
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#26]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date
```

```
[attr#27]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#28]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string
```

```
[attr#29]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#30]
vendor-id=3401
```

```
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#31]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string
```

```
[attr#32]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#33]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#34]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00006
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#35]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#36]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date
```

```
[attr#37]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#38]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00010
attribute-name>Action
attribute-profile=out
attribute-type=string
```

```
[attr#39]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
```

```
attribute-type=unsigned integer
```

```
[attr#40]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#41]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string
```

```
[attr#42]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer
```

```
[attr#43]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version
```

```
[attr#44]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00006
```

```
attribute-name=Scan-Engine-Version  
attribute-profile=in out  
attribute-type=version
```

```
[attr#45]  
vendor-id=6101  
vendor-name=Trend  
application-id=3  
application-name=AV  
attribute-id=00007  
attribute-name=Dat-Version  
attribute-profile=in out  
attribute-type=version
```

```
[attr#46]  
vendor-id=6101  
vendor-name=Trend  
application-id=3  
application-name=AV  
attribute-id=00008  
attribute-name=Dat-Date  
attribute-profile=in out  
attribute-type=date
```

```
[attr#47]  
vendor-id=6101  
vendor-name=Trend  
application-id=3  
application-name=AV  
attribute-id=00009  
attribute-name=Protection-Enabled  
attribute-profile=in out  
attribute-type=unsigned integer
```

```
[attr#48]  
vendor-id=6101  
vendor-name=Trend  
application-id=3  
application-name=AV  
attribute-id=00010  
attribute-name=Action  
attribute-profile=out  
attribute-type=string
```

```
[attr#49]  
vendor-id=10000  
vendor-name=out  
application-id=1
```

```
application-name=CNAC
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=string
```

```
[attr#50]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=string
```

```
[attr#51]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00003
attribute-name=Reason
attribute-profile=out
attribute-type=string
```

