

# Setting Up Replication for Cisco Secure ACS for Windows

Document ID: 23120

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions
- Important Implementation Considerations
- Network Diagram

#### Configuring a Primary ACS Server

#### Configuring a Secondary ACS Server

#### Scheduling Options

#### Reports

- Database Replication.csv on the Primary ACS
- Database Replication.csv on the Secondary ACS

#### Verify

#### Troubleshoot

#### Related Information

## Introduction

Database replication helps make the authentication, authorization, and accounting (AAA) environment more fault tolerant. It also duplicates parts of the primary server setup to one or more secondary servers, to help create mirror systems of Cisco Secure ACS for Windows (ACS) servers. You can configure your AAA clients to use these secondary servers if the primary server fails or is unreachable. If a secondary server database is a replica of the primary server database, and the primary server goes out of service, incoming requests are authenticated without network downtime. This happens provided that the AAA clients are configured to failover to the secondary server.

## Prerequisites

### Requirements

Ensure that you meet these requirements before you attempt this configuration:

- You own at least two Cisco Secure ACS for Windows servers.
- You are able to configure your ACS.

### Components Used

The information in this document is based on these software versions:

- ACS version 3.2.x and 3.3.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Important Implementation Considerations

Consider these points when the Cisco Secure database replication feature is implemented:

- ACS only supports database replication to other ACS servers. All ACS servers that participate in Cisco Secure database replication must run the same version and patch level of ACS.
- The primary server transmits the compressed, encrypted copy of its database components to the secondary server. This transmission occurs over a TCP connection, with port 2000. The Transmission Control Protocol (TCP) session is authenticated and uses an encrypted, Cisco–proprietary protocol.
- Only suitably configured, valid ACS hosts can be secondary servers. To add a secondary server, configure it in the AAA Servers table in the Network Configuration section of this document. When a server is added to the AAA Servers table, the server appears for selection as a secondary server in the AAA Servers list under Replication Partners, on the Cisco Secure database replication page.
- The primary server must be configured as an AAA server and must have a key. The secondary server must have the primary server configured as an AAA server and its key for the primary server must match the primary servers own key.
- Replication to secondary servers takes place sequentially in the order listed in the Replication list under Replication Partners, on the Cisco Secure database replication page.
- The secondary server, which receives the replicated components, must be configured to accept database replication from the primary server. To configure a secondary server for database replication, refer to the Configuring a Secondary Cisco Secure ACS Server section of this document.
- ACS does not support bi–directional database replication. The secondary server, which receives the replicated components, verifies that the primary server is not on its Replication list. If not, the secondary server accepts the replicated components. If so, it rejects the components.
- To replicate user–defined RADIUS vendor and vendor–specific attribute (VSA) configurations successfully, the definitions to be replicated must be identical on the primary and secondary servers. This includes the RADIUS vendor slots the user–defined RADIUS vendors occupy. For more information about user–defined RADIUS vendors and VSAs, refer to the User–Defined RADIUS Vendors and VSA Sets section of the document Cisco Secure ACS Command–Line Database Utility.

## Network Diagram

This document uses the network setup shown in this diagram:



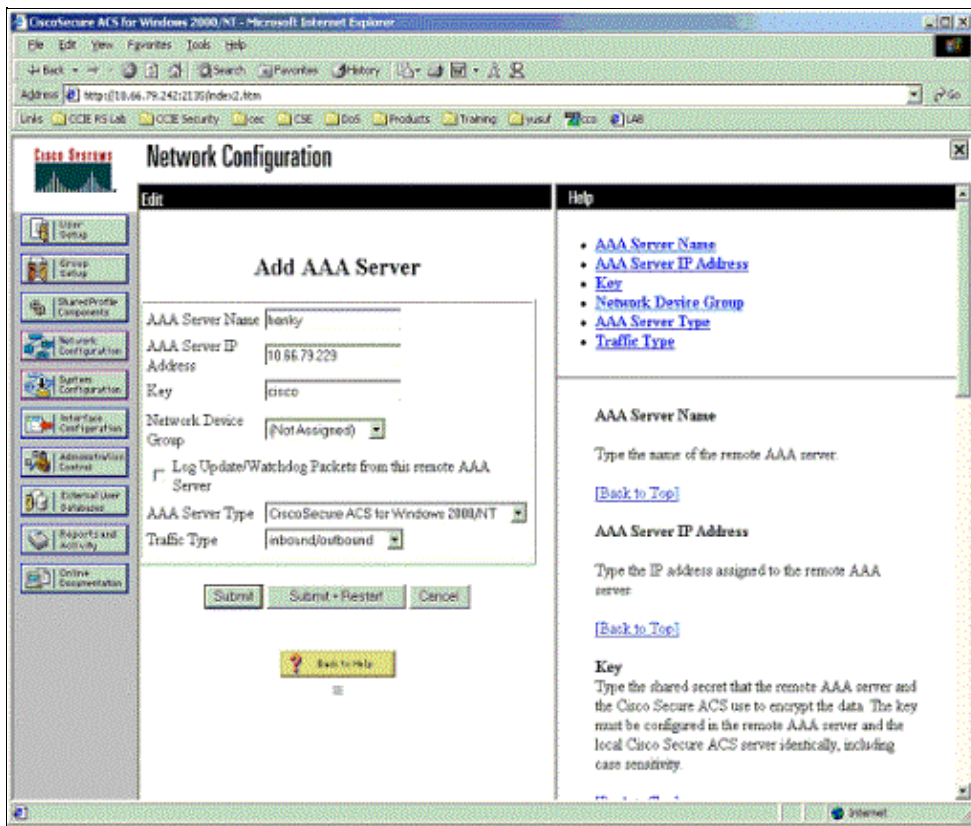
Hostname Arnie Primary ACS Server Microsoft Windows 2000 Domain Controller

Hostname Hanky Secondary ACS Server Microsoft Windows 2000 Domain Controller

# Configuring a Primary ACS Server

Use this procedure to configure a primary ACS server:

1. Log in to the primary ACS server HTML interface.
2. In the Network Configuration section, add each secondary server to the AAA Servers table.



**Note:** If this feature does not appear, select **Interface Configuration > Advanced Options**, and select the **Cisco Secure ACS Database Replication** check box. Also, verify that the **Distributed System Settings** check box is selected.

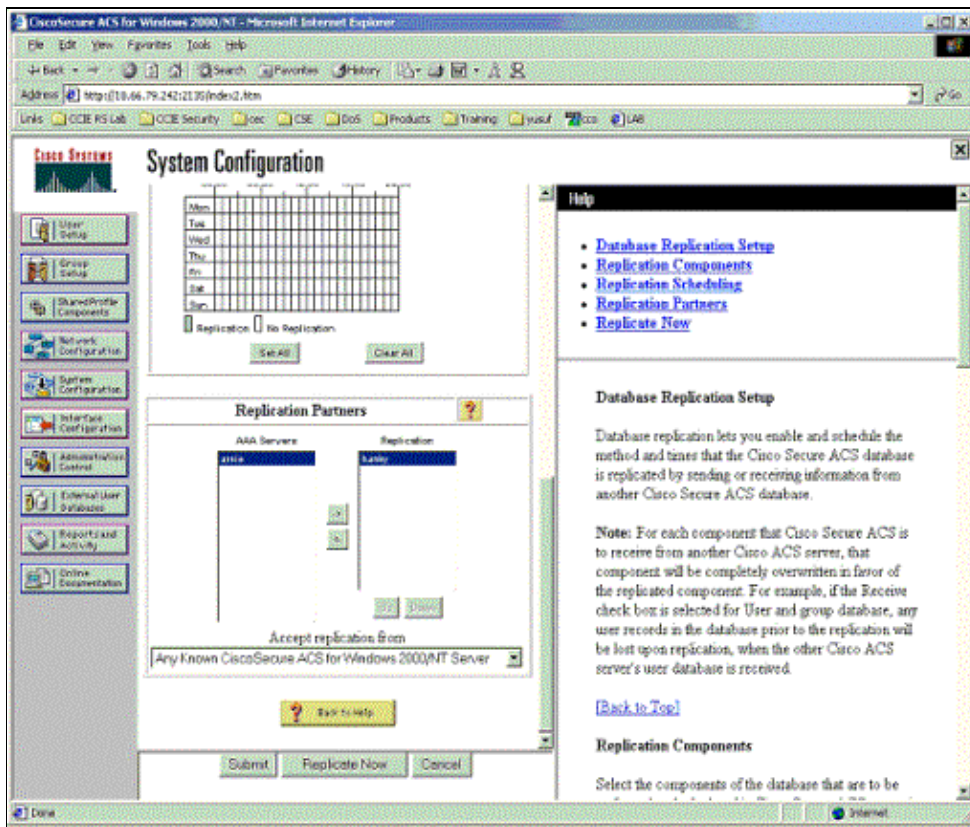
3. In the navigation bar, click **System Configuration**.
4. Click **Cisco Secure Database Replication**.

Once this step is completed, the Database Replication Setup page appears.

5. Select the **Send** check box for each database component to send to the secondary server.

Replication Components		
Component	Send	Receive
User and group database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
AAA Servers and AAA Clients tables	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Distribution table	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Interface configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Interface security settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password validation settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>

6. Under the Replication Partners, add the secondary ACS server to the Replication Partner column.



7. Click **Submit**.

ACS saves the replication configuration and the frequency or times specified. ACS begins to send the components to the other ACS servers specified.

## Configuring a Secondary ACS Server

Use this procedure to configure the secondary ACS server:

1. Log in to the secondary server HTML interface.
2. In the Network Configuration section, add the primary server to the AAA Servers table (in the same way as on the primary ACS).

**Note:** If this feature does not appear, select **Interface Configuration > Advanced Options**, and select the **Cisco Secure ACS Database Replication** check box. Also, verify that the **Distributed System Settings** check box is selected.

3. In the navigation bar, click **System Configuration**.
4. Click **Cisco Secure Database Replication**.

Once this step is completed, the Database Replication Setup page appears.

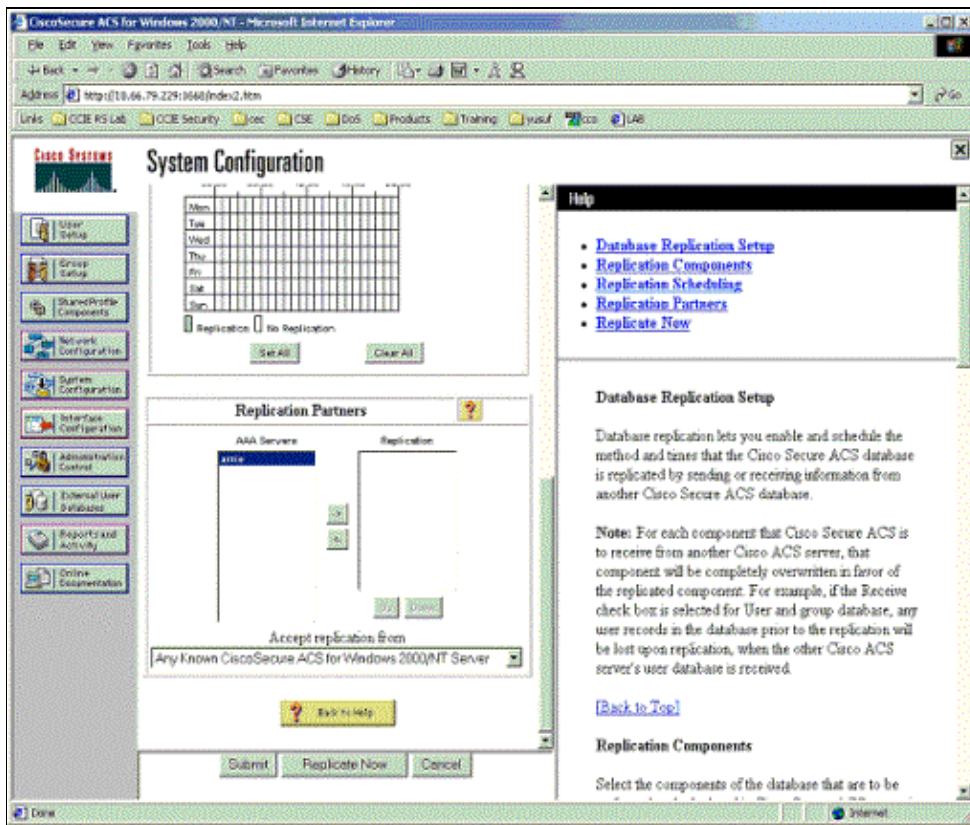
5. Click the **Receive** check box for each database component to be received from a primary server.

Replication Components		
Component	Send	Receive
User and group database	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AAA Servers and AAA Clients tables	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Distribution table	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interface configuration	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interface security settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Password validation settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>

6. If the secondary server is to receive replication components from only one primary server, select the other Cisco Secure ACS server name, from the Accept replication list.
7. If the secondary server is to receive replication components from more than one primary server, select **Any Known Cisco Secure ACS for Windows 2000/NT Server** from the Accept replication list.

The Any Known Cisco Secure ACS for Windows 2000/NT Server option is limited to the servers listed in the AAA Servers table in the Network Configuration section.

8. Do not add the primary server to the Replication Partner column. Under Replication Partners, ideally the replication partner column is blank.



9. Click **Submit**.

ACS saves the replication configuration and the frequency or times specified. ACS accepts the replicated components from the other servers specified.

# Scheduling Options

You can specify when a Cisco Secure database replication occurs; this is configured on the primary server, not the secondary. These options that control when replication occurs appear in the Replication Scheduling table on the Cisco Secure database replication page. Here are the options:

- **Manually** ACS does not perform automatic database replication.
- **Automatically Triggered Cascade** ACS performs database replication to the configured list of secondary servers when database replication from a primary server completes. This enables you to build a propagation hierarchy of servers, which does not require a primary server to propagate the replicated components to other servers.
- **Every  $x$  minutes** ACS performs, on a set frequency, database replication to the configured list of secondary servers. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times** ACS performs, at the time specified in the day and hour graph, database replication to the configured list of secondary servers. The minimum resolution is one hour, and the replication takes place on the hour selected.

## Reports

Go to **Reports and Activity**, select **Database Replication**, and check the **active Database Replication.csv log**. If the replication is successful, you see these logs.

### Database Replication.csv on the Primary ACS

Date	Time	Status	Message
06/12/2002	14:14:26	INFO	Outbound replication cycle completed.
06/12/2002	14:14:26	ERROR	Replication to ACS "Hanky" was successful.
06/12/2002	14:14:00	INFO	Outbound replication cycle is about to start.

### Database Replication.csv on the Secondary ACS

Date	Time	Status	Message
06/12/2002	16:32:02	INFO	Inbound database replication from ACS "Arnie" completed.
06/12/2002	16:31:41	INFO	Inbound database replication from ACS "Arnie" started.

**Note:** In the log messages on the primary server, the message-type shows an ERROR. For further information, refer to Cisco bug ID CSCdw51174 (registered customers only). Replication still completes correctly, regardless of the ERROR keyword.

Workaround: Ignore the ERROR status.

You see these logs if replication is not successful. Possible symptoms include:

- The shared secret key does not match in the AAA Server table for the remote end(s).
- Remote server does not respond.

Date	Time	Status	Message
06/14/2002	10:02:30	INFO	Outbound replication cycle completed.
06/14/2002	10:02:30	WARNING	Cannot replicate to "Hanky" – server does not respond.
06/14/2002	10:02:23	INFO	Outbound replication cycle is about to start.

## Verify

Add a new user or group to the primary server, or make any changes in current user or group settings, and then click **Replicate Now** from the Database Replication setup section under System Configuration. On the secondary server, check the user or group and see that the changes take effect.

## Troubleshoot

These are some of the error messages that are encountered, and the solutions for each:

- The Authentication failing with the error; Authentication Failed: Proxy failure error message could present due to an incorrect proxy distribution configuration. On the primary ACS, check that the proxy distribution entry is not set to forward to the secondary ACS or the reverse. The correct configuration is to point the corresponding ACS to itself.
- If replication does not work, make sure the primary ACS is listed as a replication partner on the secondary ACS. If it is removed, the No AAA Replication Partners have been selected. At least one needs to be selected for replication to take place. error is returned.

If outbound replication is configured with Specific Times, change the settings to Manual. This usually resolves the issue.

---

## Related Information

- [Cisco Secure ACS for Windows Support Page](#)
  - [Documentation for Cisco Secure ACS for Windows](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 02, 2006

Document ID: 23120

---