

Secure ACS Database Replication Configuration Example

Document ID: 71320

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

- Scenario I
- Scenario II

Scenario I: Configure Database Replication Without Intervening Firewall

Scenario II: Configure Database Replication With Intervening Firewall (NAT Configuration)

Procedures

- Configure the Primary ACS Server
- Configure the Secondary ACS Server
- Invoke Database Replication Through Secure ACS
- Configure Database Replication Through a NAT Device

Verify the Configuration

Troubleshoot the Configuration

- Replication Problem
- Secondary ACS Server does not Restart the Service
- Procedures
- Tips

Related Information

Introduction

Cisco Secure Access Control Server (ACS) is a powerful tool that allows network administrators to centrally manage AAA (authentication, authorization, and accounting) on a wide range of Cisco devices. You can deploy an ACS server in a standalone configuration or in a redundant topology. In order to provide failover capability, two or more ACS machines share database components at preconfigured times. AAA clients, such as routers, switches, and firewalls, must list two or more ACS servers in their configuration in order to benefit from a redundant implementation. An administrator need only make changes to the primary ACS server. A configured secondary ACS server receives database information through manual or automatic database replication.

AAA clients attempt to communicate with the first ACS server listed in their configuration. If a client cannot reach this server after a specified amount of time, it attempts to communicate with the second ACS server listed in its configuration. You cannot force a client to attempt to communicate with the second server first. If the AAA client receives a response from the first server, it will not attempt to communicate with the second server.

This document describes two configuration scenarios for database replication between two ACS servers:

- **Scenario I** Scenario I configures database replication between two ACS servers without an intervening firewall.

- **Scenario II** Scenario II configures database replication between two ACS servers with an intervening firewall that acts as a Network Address Translation (NAT) device.

In order to better understand the procedures described in these scenarios, you must be familiar with these definitions:

- **Primary ACS server** The Cisco Secure ACS server that is configured to send components of its database to one or more Cisco Secure ACS servers.
- **Secondary ACS server** The Cisco Secure ACS server that is configured to receive database components from another Cisco Secure ACS server.
- **Database replication** Copies the database or portions of the database to other secondary ACS servers. These secondary ACS servers provide redundancy. Replication occurs over a TCP connection by using port 2000. The TCP session uses a 128-bit encrypted, Cisco-proprietary protocol for replication.
- **Database backup** Backs up the ACS database into a dump file. You can use this file to restore ACS functionality in the event of an operating system or hardware failure.
- **Relation database management system (RDBMS) synchronization** Allows your ACS database to synchronize with the external database. You can enter ACS configuration into an ODBC compliant database in order to allow your ACS databases to synchronize with the external database. For example, in large scale deployments your ACS servers need only point to the external ODBC database to receive their configurations.

Note: Bidirectional replication is not supported. A Cisco Secure ACS server can act as a primary and a secondary at the same time as long it is configured with different replication partners.

Note: The ACS appliance can be replicated with ACS for Windows. However, both appliances must be on the same version and patch level.

Prerequisites

Requirements

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

- All machines must use the same version of Secure ACS software.
- TCP port 2000 (destination port used for replication) must not be blocked anywhere along the path between the ACS servers. Also, TCP port inspection must be disabled in order for replication to occur successfully.

Note: Make sure that port 2000 and any other necessary ports are not in use by any other application. Otherwise, it can stop services like CSAuth, CSRadius, and CSTacacs.

- Make sure that network interface cards (NICs) are not firewalled within the operating system.
- Enable Java and JavaScript; disable HTTP proxy.
- Ensure that remote access to the Secure ACS user interface uses TCP port 2002. For example, **https://ipaddress:2002**

Note: If you use Microsoft Internet Explorer Version 6.0 in order to access the Secure ACS HTML user interface, ensure that your browser meets these requirements:

- ◆ Microsoft Windows Service Pack 1 (English and Japanese language versions)
- ◆ Microsoft Java Virtual Machine (JVM) version 5.00.3810
- ◆ Sun Java plug-in version 1.5

Note: For more information, refer to Supported and Interoperable Devices for Cisco Secure ACS for

Windows 4.0.

Components Used

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

- Windows 2003 Server
- Cisco Secure ACS version 4.x
- Cisco PIX Firewall 515e version 6.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.

Related Products

You can also use this configuration with these hardware and software versions:

- Windows ACS Server 3.x or later
- Any Network Address Translation (NAT) device

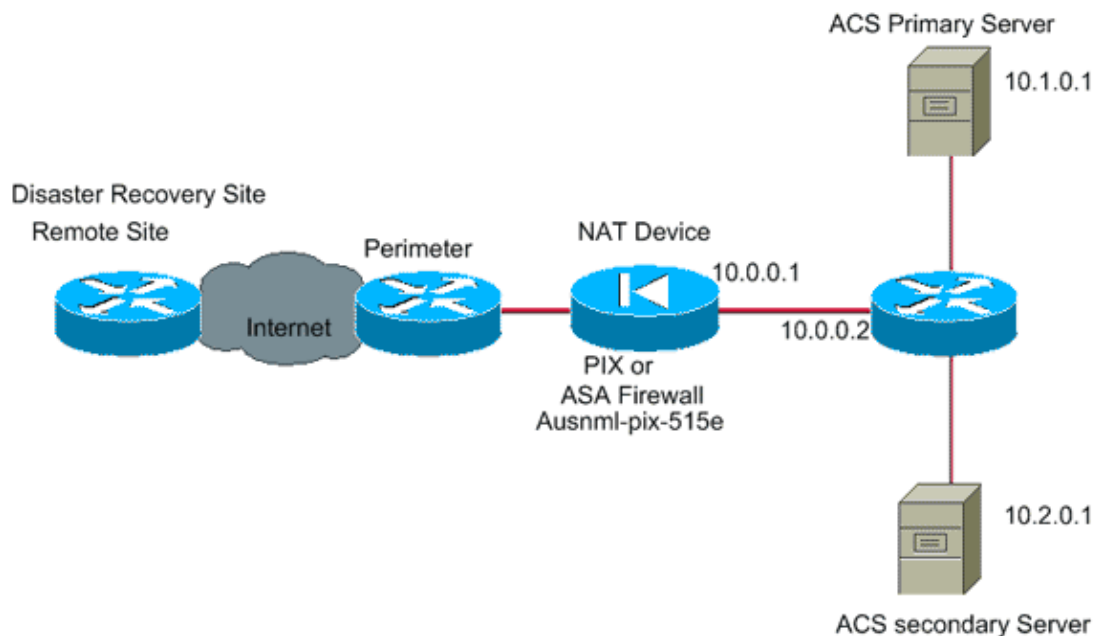
Conventions

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

Background Information

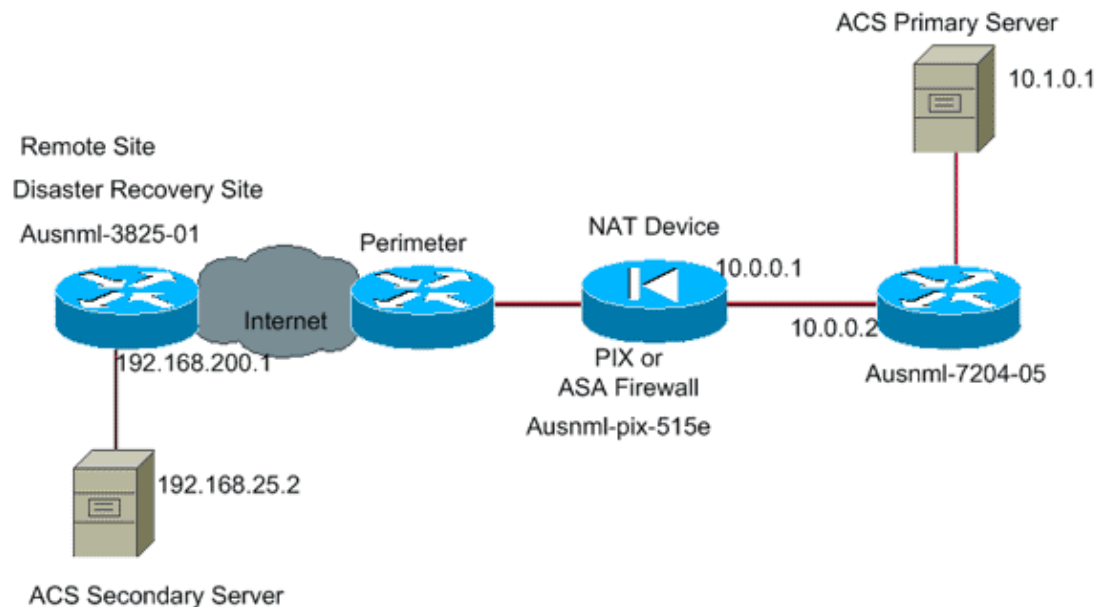
Scenario I

Scenario I uses this network configuration:



Scenario II

Scenario II uses this network configuration:



Scenario I: Configure Database Replication Without Intervening Firewall

In Scenario I, data does not transit a NAT device when the two Cisco Secure ACS servers communicate. The data is encrypted with a Cisco proprietary protocol, and then TCP is used to send the data to destination port 2000.

To configure database replication without an intervening firewall, complete these procedures:

1. Configure the Primary ACS Server
2. Configure the Secondary ACS Server
3. Invoke Database Replication Through Secure ACS

Scenario II: Configure Database Replication With Intervening Firewall (NAT Configuration)

Successful database replication can occur only if the secondary ACS server perceives no change in the IP header or content of the data it receives. The primary ACS server uses a key to make calculations on the headers and content sent to the secondary server. The secondary server uses the same key to calculate the results. If differences in these calculations occur, the database replication is denied.

Cisco Secure ACS does not support distributed deployments in a NAT environment. If a primary or secondary address is translated through a NAT device, the database replication log file indicates shared secret mismatch. If a NAT device is located between the primary and secondary servers, the differences in the calculations cause the replication to be rejected. However, several options exist that bypass the influence of the NAT device on the network traffic and achieve a successful database replication:

- Generic routing encapsulation (GRE) tunnels
- Virtual private networks (VPNs) with IP security (IPsec) in tunnel mode

- GRE+IPsec tunnels
- IPsec tunnels directly between the Windows servers with Microsoft Internet Security and Acceleration (ISA) Server. For more information, refer to Microsoft Internet Security and Acceleration (ISA) Server TechCenter .

Scenario II uses a simple GRE tunnel to achieve database replication, since the traffic is already encrypted when it is sent from one ACS server to another. The secondary ACS server is located outside the PIX/ASA firewall, and a GRE tunnel is built from router to router. This tunnel hides the address information and data from the NAT device, which allows database replication to proceed normally.

Note: If you have VPN tunnels with IPsec in place, you can add the ACS servers to the crypto access lists and achieve the same result.

To configure database replication with an intervening firewall (NAT configuration), complete these procedures:

1. Configure the Primary ACS Server
2. Configure the Secondary ACS Server
3. Configure Database Replication Through a NAT Device

Procedures

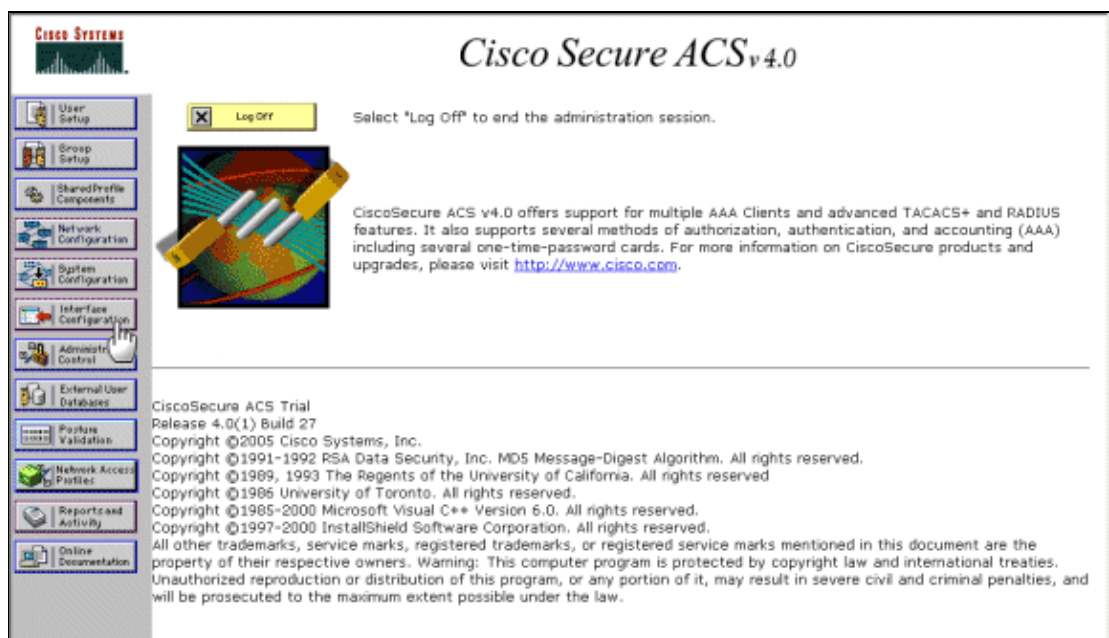
The procedures in this section describe how to configure database replication. You must complete these procedures as described in Scenario I or Scenario II.

Configure the Primary ACS Server

To configure the primary ACS server, complete these steps:

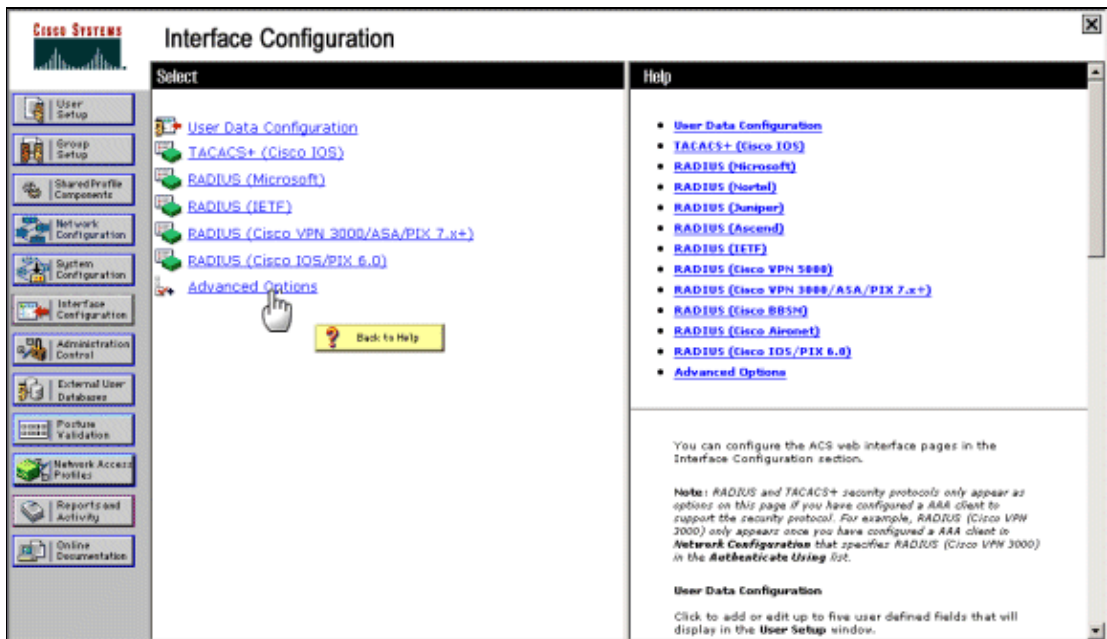
1. On the primary ACS server, open the Cisco Secure ACS user interface.

The Cisco Secure ACS interface appears.



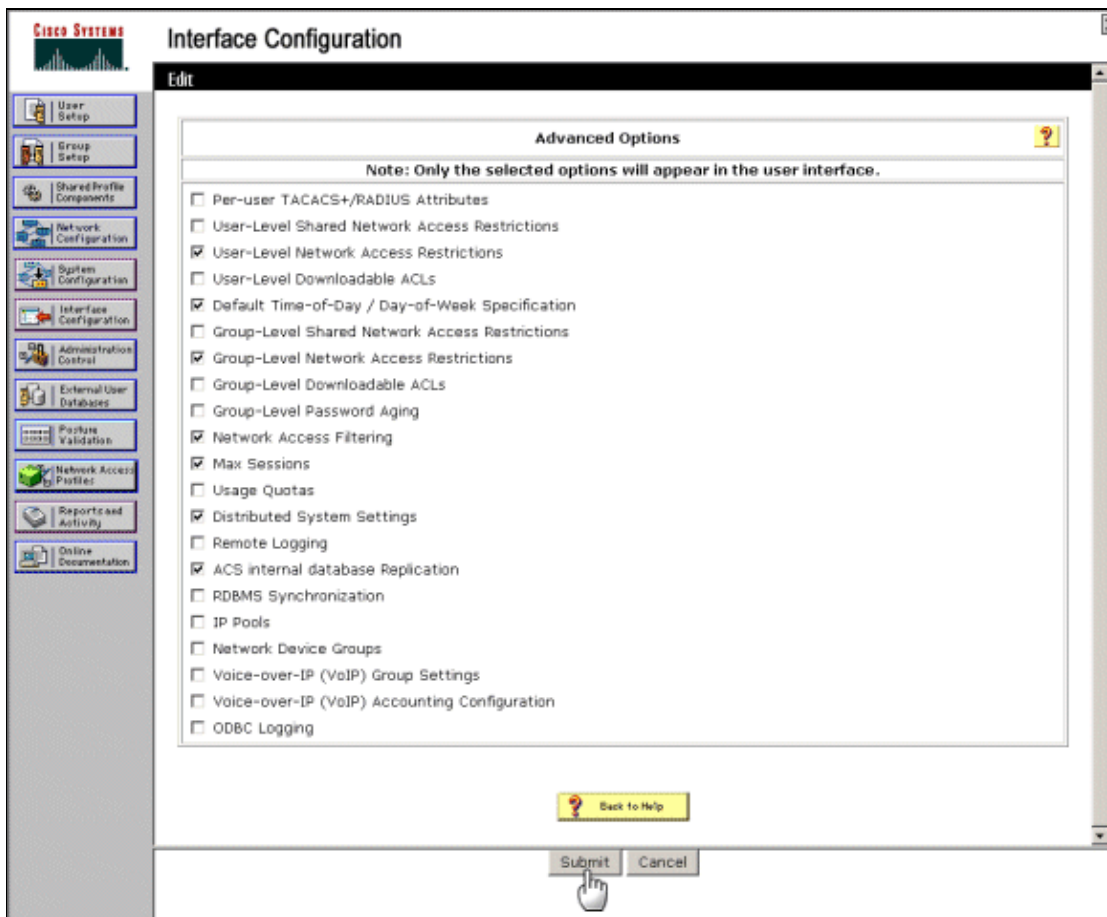
2. In the left pane, click the **Interface Configuration** button.

The Interface Configuration page appears.



3. Click the **Advanced Options** link.

The Advanced Options page appears.



4. On the Advanced Options page, check the **ACS internal database Replication** check box, and then click **Submit**.

5. In the left pane, click the **Network Configuration** button.

The Network Configuration page appears.

The screenshot shows the Cisco Network Configuration page. On the left is a navigation sidebar with buttons for User Setup, Snmp Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Report and Activity, and Online Documentation. The main content area is titled "Network Configuration" and has a "Select" header. It contains three tables:

- AAA Clients:** A table with columns "AAA Client Hostname", "AAA Client IP Address", and "Authenticate Using". It lists "firewall" (20.20.20.1, RADIUS), "router" (10.10.10.1, TACACS+), and "switch" (15.15.16.1, TACACS+).
- AAA Servers:** A table with columns "AAA Server Name", "AAA Server IP Address", and "AAA Server Type". It lists "AUSNMLAA01" (10.1.0.1, CiscoSecure ACS).
- Proxy Distribution Table:** A table with columns "Character String", "AAA Servers", "Strip", and "Account". It lists "(Default)" (AUSNMLAA01, No, Local).

Buttons for "Add Entry" and "Search" are present below each table. A "Back to Help" button is at the bottom.

6. In the AAA Servers area, click **Add Entry** in order to add a secondary ACS server.

The Add AAA Server page appears.

The screenshot shows the "Add AAA Server" form in the Cisco Network Configuration page. The form is titled "Add AAA Server" and has the following fields:

- AAA Server Name: AUSNMLAA02
- AAA Server IP Address: 10.2.0.1
- Key: guessn0t
- Log Update/Watchdog Packets from this remote AAA Server
- AAA Server Type: CiscoSecure ACS (dropdown)
- Traffic Type: inbound/outbound (dropdown)

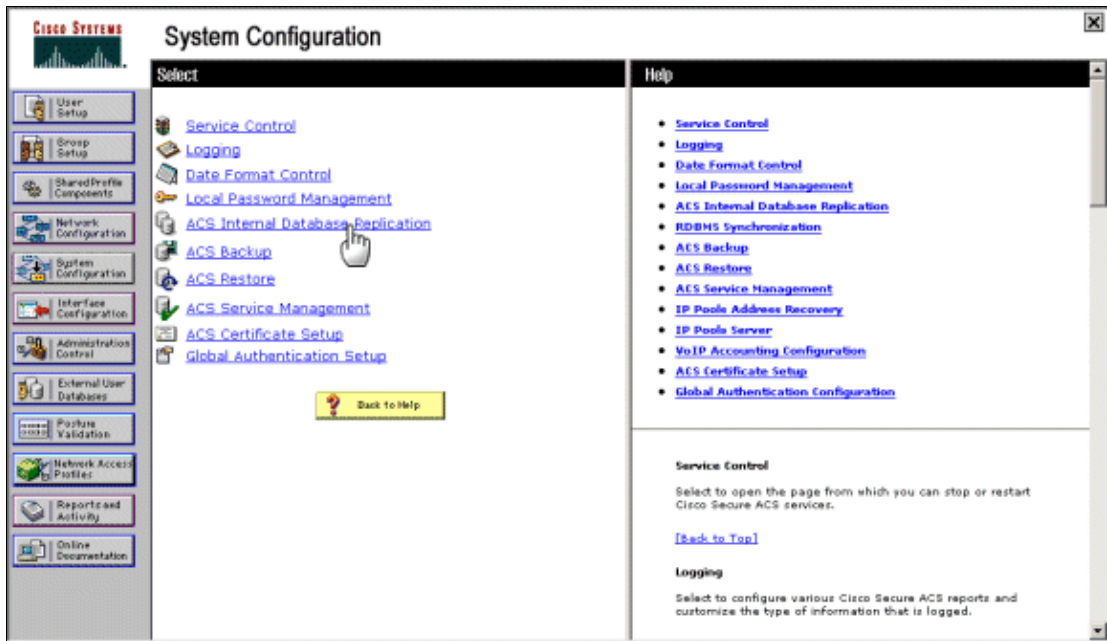
Buttons for "Submit", "Submit + Apply", and "Cancel" are at the bottom. A "Back to Help" button is also present. On the right, a "Help" section provides instructions for each field:

- AAA Server Name:** Type the name of the remote AAA server. [Back to Top]
- AAA Server IP Address:** Type the IP address assigned to the remote AAA server. [Back to Top]
- Key:** Type the shared secret that the remote AAA server and ACS use to encrypt the data. The key must be configured in the remote AAA server and in the local ACS identically, including case sensitivity. [Back to Top]
- Network Device Group:** From the list, click the Network Device Group (NDG) to which

7. Enter values for the secondary ACS server, and then click **Submit + Apply**.

8. In the left pane, click the **System Configuration** button.

The System Configuration page appears.



9. Click the **ACS Internal Database Replication** link.

The Database Replication Setup page appears.

CISCO SYSTEMS System Configuration

Edit

Database Replication Setup

CAUTION: Replication will **overwrite** the selected components on the replicated clients.
CiscoSecure ACS services will be halted momentarily during replication.

Replication Components ?

Component	Send	Receive
User and Group Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group Database only	<input type="checkbox"/>	<input type="checkbox"/>
Network Configuration Device 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"/>
EAP-FAST master keys and policies	<input type="checkbox"/>	<input type="checkbox"/>
Network Access Profiles	<input type="checkbox"/>	<input type="checkbox"/>

Outbound Replication ?

Scheduling

Manually
 Automatically triggered cascade
 Every minutes
 At specific times...

Partners

AAA Servers

Replication
 AUSNMLAAR02

Inbound Replication ?

Accept replication from

Replication settings ?

Replication timeout: minutes

10. In the Replication Components area, check the **Send** check box for the components that you want to replicate to the secondary ACS server.
11. In the Outbound Replication Scheduling area, click the **Manually** radio button.

Note: If you prefer, you can schedule outbound replication to occur at timed intervals.

12. In the Outbound Replication Partners area, select from the AAA Servers list the server that you added on the Add AAA Server page, and then click the right arrow button () in order to move the server

to the Replication list.

13. Leave the default values for the settings listed in the Inbound Replication and Replication Settings areas.
14. Click **Submit**.

Configure the Secondary ACS Server

To configure the secondary ACS server, complete these steps:

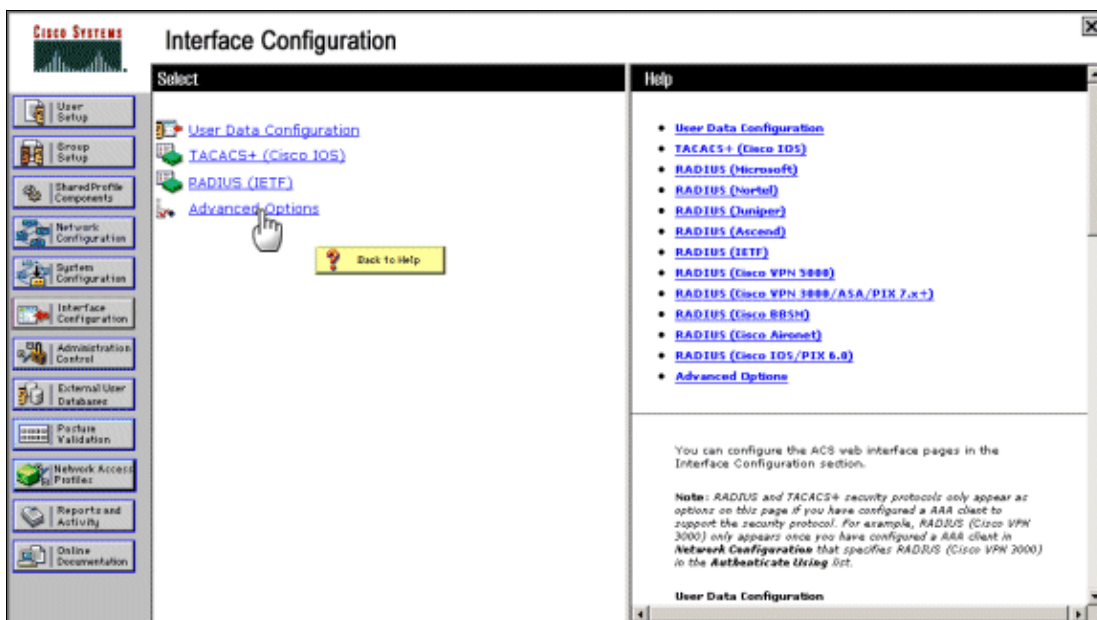
1. On the secondary server, open the Cisco Secure ACS user interface.

The Cisco Secure ACS interface appears.



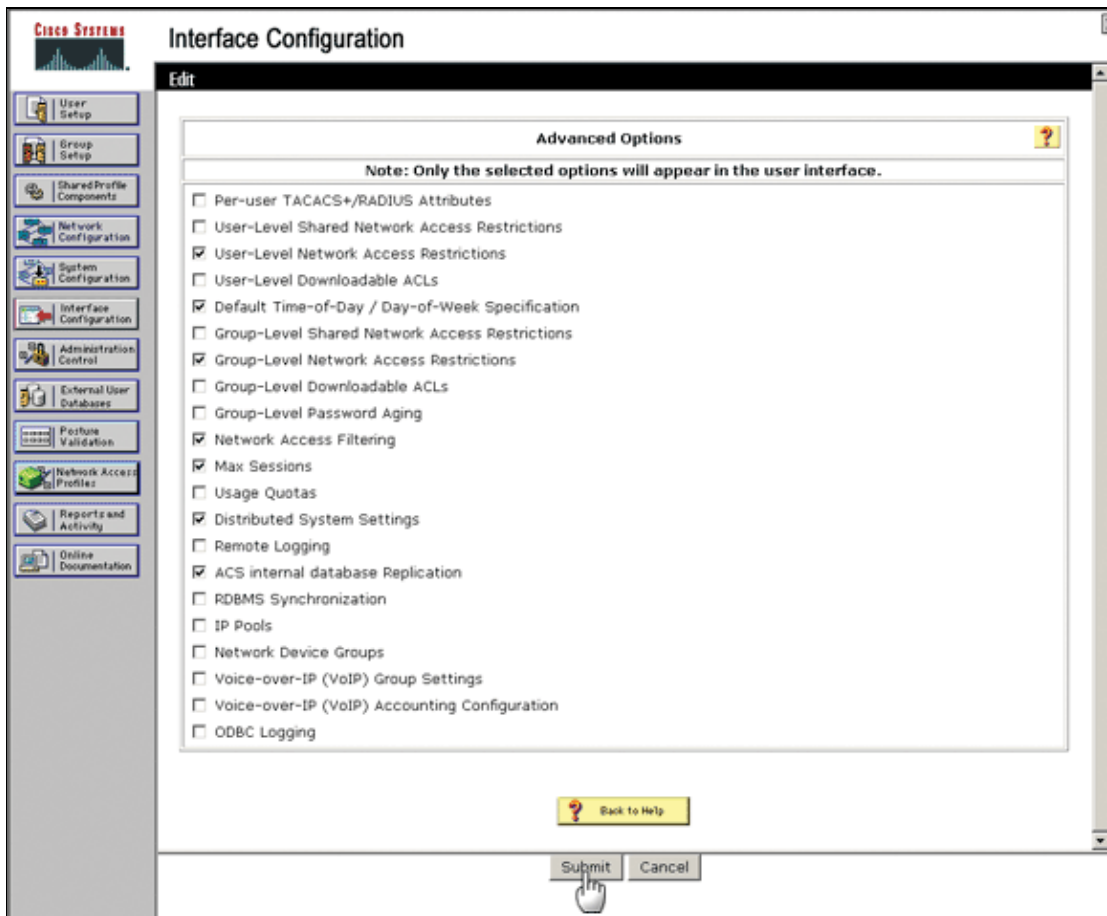
2. In the left pane, click the **Interface Configuration** button.

The Interface Configuration page appears.



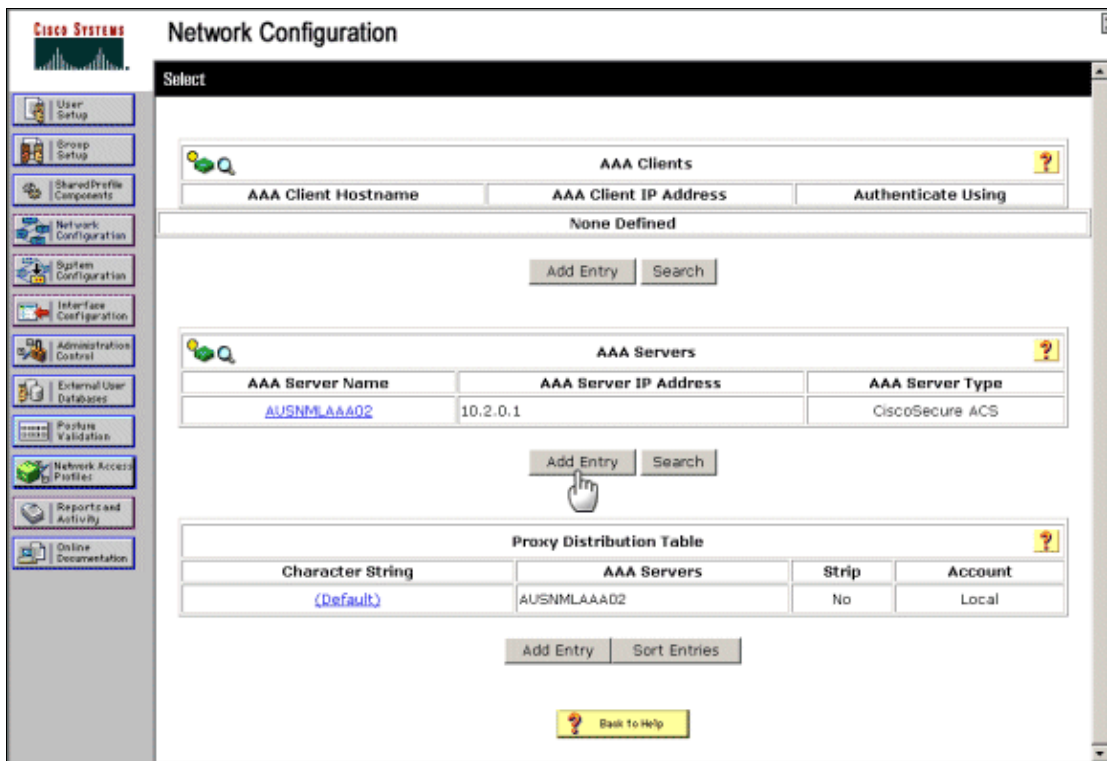
3. Click the **Advanced Options** link.

The Advanced Options page appears.



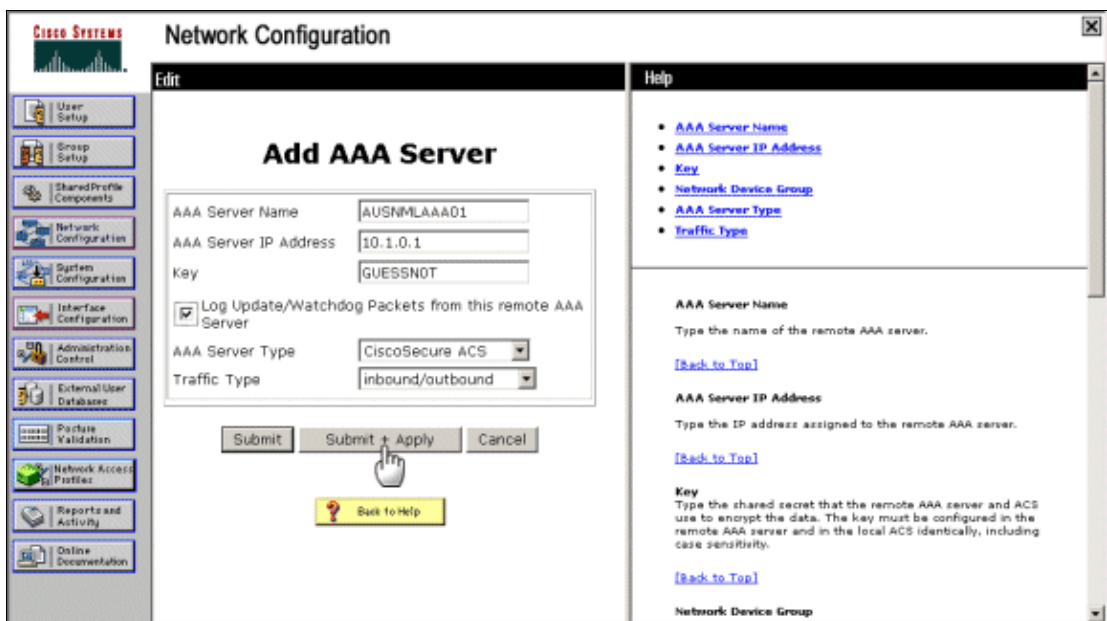
4. On the Advanced Options page, check the **ACS internal database Replication** check box, and then click **Submit**.
5. In the left pane, click the **Network Configuration** button.

The Network Configuration page appears.



6. In the AAA Servers area, click **Add Entry** in order to add a primary ACS server.

The Add AAA Server page appears.

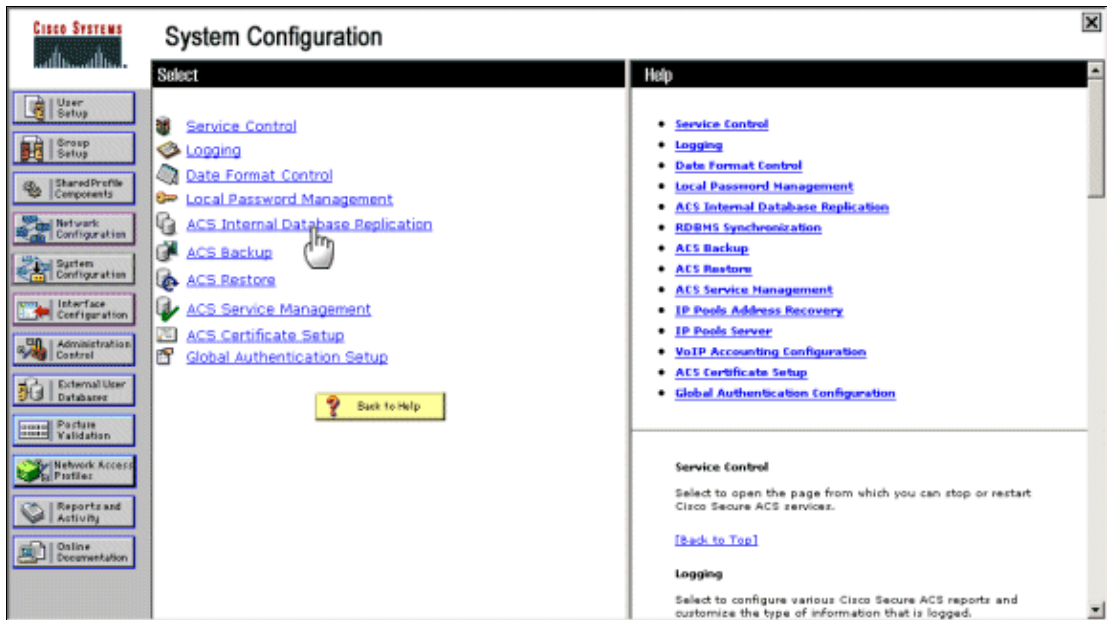


7. Enter values for the primary ACS server, and then click **Submit + Apply**.

Note: The key for the primary and secondary server must be the same.

8. In the left pane, click the **System Configuration** button.

The System Configuration page appears.



9. On the System Configuration page, click the **ACS Internal Database Replication** link.

The Database Replication Setup page appears.

CISCO SYSTEMS System Configuration

Database Replication Setup

CAUTION: Replication will **overwrite** the selected components on the replicated clients.
CiscoSecure ACS services will be halted momentarily during replication.

Replication Components

Component	Send	Receive
User and Group Database	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group Database only	<input type="checkbox"/>	<input type="checkbox"/>
Network Configuration Device 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"/>
EAP-FAST master keys and policies	<input type="checkbox"/>	<input type="checkbox"/>
Network Access Profiles	<input type="checkbox"/>	<input type="checkbox"/>

Outbound Replication

Scheduling

Manually
 Automatically triggered cascade
 Every 60 minutes
 At specific times...

Partners

AAA Servers: AUSNMLAAA01, AUSNMLAAA02

Replication: (empty)

Inbound Replication

Accept replication from: AUSNMLAAA01

Replication settings

Replication timeout: 5 minutes

[Back to Help](#)

- In the Replication Components area, check the **Receive** check box for the components that you want to replicate to the primary ACS server.

Note: The components you check for the primary server must match the components you check for the secondary server.

- In the Outbound Replication Scheduling area, click the **Manually** radio button.

Note: In the Outbound Replication Partners area, leave the Replication list blank. Because the secondary server receives database components, you do not need to add a primary server to the Replication list.

12. In the Inbound Replication area, choose the primary AAA server from the Accept replication from drop-down menu.
13. In the Replication Settings area, leave the default setting for this value.
14. Click **Submit**.

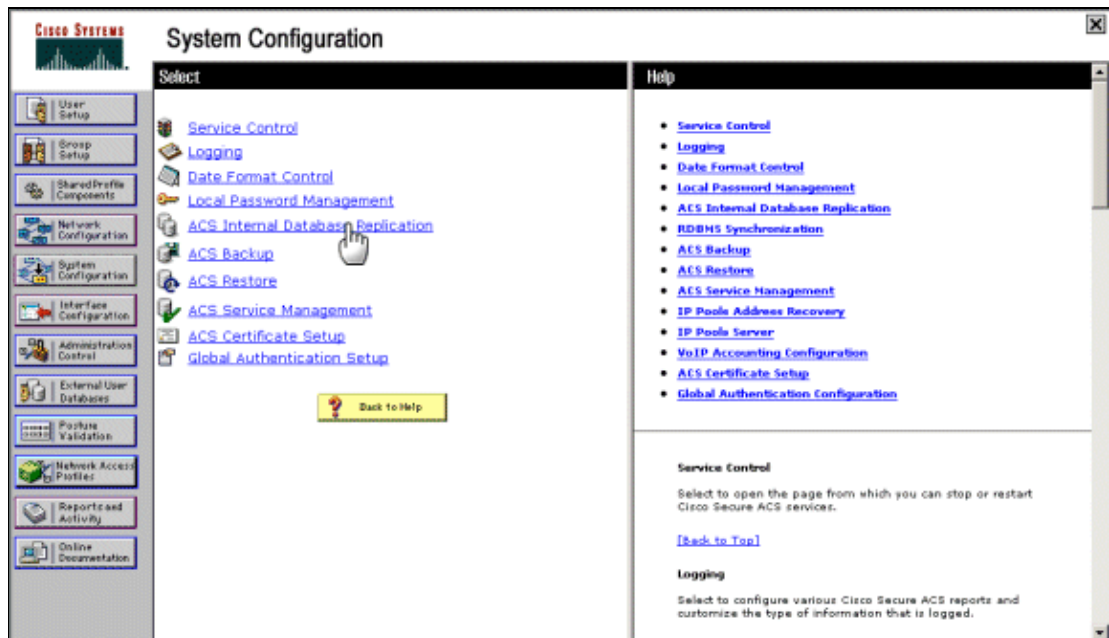
Invoke Database Replication Through Secure ACS

This procedure applies only to Scenario I.

To invoke database replication through Cisco Secure ACS, complete these steps:

1. On the primary ACS server, click the **System Configuration** button located in the left pane.

The System Configuration page appears.



2. Click the **ACS Internal Database Replication** link.

The Database Replication Setup page appears.

CISCO SYSTEMS System Configuration

Database Replication Setup

CAUTION: Replication will **overwrite** the selected components on the replicated clients.
CiscoSecure ACS services will be halted momentarily during replication.

Replication Components

Component	Send	Receive
User and Group Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group Database only	<input type="checkbox"/>	<input type="checkbox"/>
Network Configuration Device 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"/>
EAP-FAST master keys and policies	<input type="checkbox"/>	<input type="checkbox"/>
Network Access Profiles	<input type="checkbox"/>	<input type="checkbox"/>

Outbound Replication

Scheduling

Manually
 Automatically triggered cascade
 Every minutes
 At specific times...

	00:00	06:00	12:00	18:00	24:00
Mon					
Tue					
Wed					
Thu					
Fri					
Sat					
Sun					

Partners

AAA Servers	Replication
	AUSNMLAAR02

Inbound Replication

Accept replication from

Replication settings

Replication timeout: minutes

3. Click the **Replicate Now** button.
4. Verify the configuration. For details about how to verify your configuration, see Verify the Configuration.

Configure Database Replication Through a NAT Device

This procedure applies only to Scenario II.

To configure database replication through a NAT device, complete these steps:

1. Configure the GRE tunnel on routers *Ausnml-3825-01* and *Ausnml-7204-05*.
2. Perform replication as normal.

These tables provide sample GRE tunnel configurations:

AUSNML-3825-01	AUSNML-7204-05
<pre>show run Building configuration... Current configuration : 1218 bytes ! ! ! ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname AUSNML-3825-01 ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$dLun\$g726j7YEccX.qw9YNA8I1. enable password cisco ! no aaa new-model ! resource policy ! ip cef ! voice-card 0 no dspfarm !--- GRE tunnel configuration interface Tunnel0 ip address 172.16.16.1 255.255.255.0 ip mtu 1438 tunnel source GigabitEthernet0/0 tunnel destination 192.168.1.65 ! interface GigabitEthernet0/0 ip address 192.168.200.1 255.255.255.0 duplex auto speed auto media-type rj45 no mop enabled ! interface GigabitEthernet0/1 ip address 192.168.25.1 255.255.255.0 duplex auto speed auto media-type rj45</pre>	<pre>show run Building configuration... Current configuration : 1222 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname AUSNML-7204-05 ! ip subnet-zero ip cef ! call rsvp-sync !--- GRE tunnel configuration interface Tunnel0 ip address 172.30.30.1 255.255.255.0 ip mtu 1438 tunnel source FastEthernet0/0 tunnel destination 192.168.200.1 ! interface FastEthernet0/0 ip address 10.0.0.2 255.255.255.0 duplex half ! interface ATM2/0 no ip address shutdown no atm ilmi-keepalive ! interface Ethernet3/0 ip address 10.1.0.2 255.255.255.0 duplex half ! interface Ethernet3/1 ip address 10.2.0.2 255.255.255.0 duplex half ! interface Ethernet3/2 no ip address shutdown duplex half ! interface Ethernet3/3 no ip address</pre>

<pre> ! ip route 0.0.0.0 0.0.0.0 192.168.200.2 ip route 10.1.0.1 255.255.255.255 Tunnel0 !---- Route ACS database traffic ! ip http server no ip http secure-server ! control-plane ! ! ! line con 0 stopbits 1 line aux 0 line vty 0 4 exec-timeout 0 0 password cisco login transport input telnet ! scheduler allocate 20000 1000 ! end AUSNML-3825-01# </pre>	<pre> shutdown duplex half ! ip classless ip route 0.0.0.0 0.0.0.0 10.0.0.1 ip route 192.168.25.2 255.255.255.255 Tunnel0 !---- Route ACS database traffic no ip http server ip pim bidir-enable ! dial-peer cor custom ! gatekeeper shutdown ! line con 0 line aux 0 line vty 0 4 password cisco123 login ! end AUSNML-7204-05# </pre>
---	--

This table provides the firewall configuration that is relevant to this scenario:

ausnml-pix-515e
<pre> show run : Saved PIX Version 6.3(5) hostname ausnml-pix-515e domain-name cisco.com fixup protocol dns maximum-length 512 fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol http 80 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol sip 5060 fixup protocol sip udp 5060 fixup protocol skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol tftp 69 names !---- Permit GRE tunnel protocol access-list 101 permit gre host 192.168.200.1 host 192.168.1.65 no pager mtu outside 1500 mtu inside 1500 ip address outside 192.168.1.214 255.255.255.252 ip address inside 10.0.0.1 255.255.255.0 global (outside) 1 192.168.1.67-192.168.1.127 netmask 255.255.255.192 </pre>

```

global (outside) 1 192.168.1.130-192.168.1.190 netmask 255.255.255.192
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- Static endpoint translation for tunnel and others

static (inside,outside) 192.168.1.65 10.0.0.2 netmask 255.255.255.255 0 0
static (inside,outside) 192.168.1.66 10.1.0.1 netmask 255.255.255.255 0 0
static (inside,outside) 192.168.1.129 10.2.0.1 netmask 255.255.255.255 0 0

access-group 101 in interface outside

!--- Static route to Perimeter router

route outside 0.0.0.0 0.0.0.0 192.168.1.213 1

!--- Route to ACS Servers

route inside 10.1.0.0 255.255.255.0 10.0.0.2 1
route inside 10.2.0.0 255.255.255.0 10.0.0.2 1
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 10.1.0.1 255.255.255.255 inside
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
vpdn username wvshaw password ***** store-local
terminal width 80
Cryptochecksum:f23dd725f24bb68e8ce8710f0d7bb58f
: end
ausnml-pix-515e(config)#

```

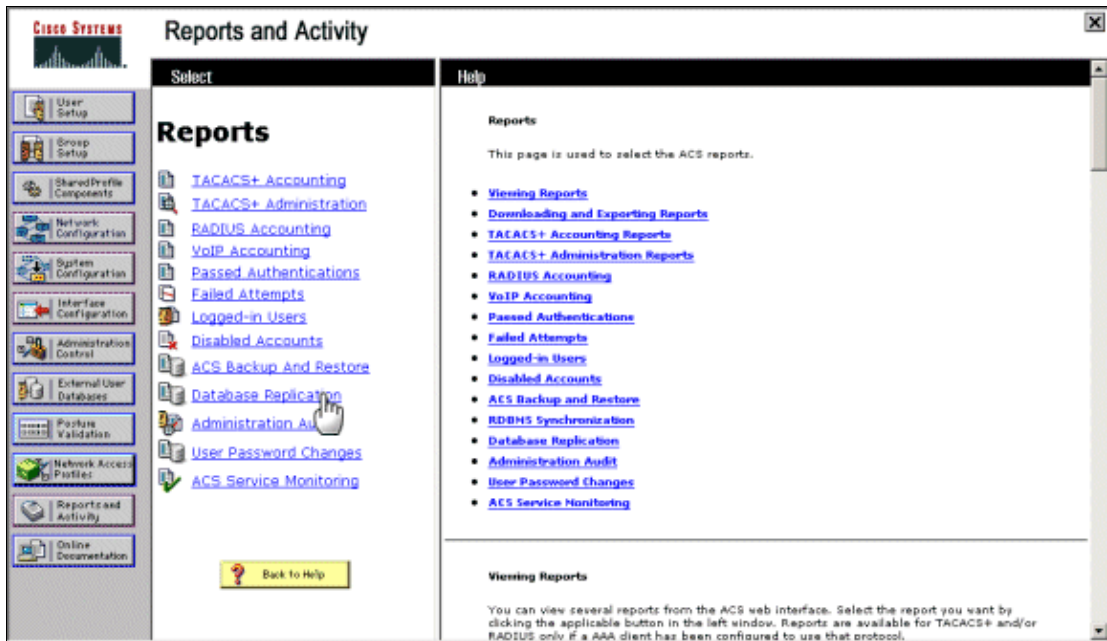
Verify the Configuration

This section describes how to verify the configuration.

To verify that you successfully configured database replication, complete these steps:

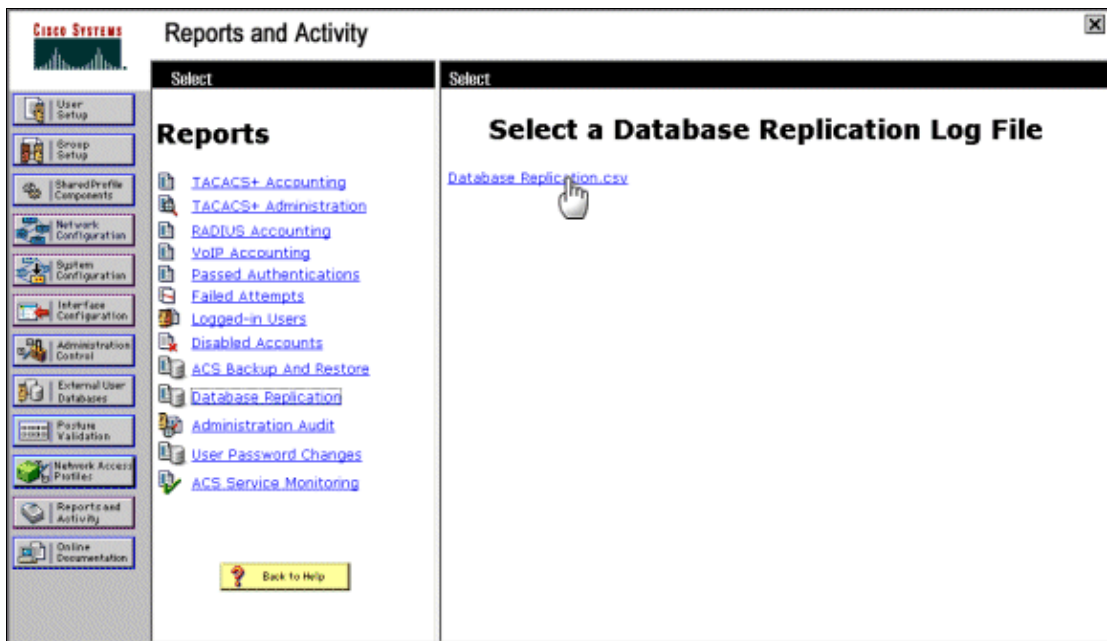
1. On the primary ACS Server, click the **Reports and Activity** button located in the left pane.

The Reports and Activity page appears.



2. Click the **Database Replication** link.

The Select a Database Replication Log File area appears.



3. From the Select a Database Replication Log File area, click **Database Replication.csv**.

In the log file, successful database replication looks similar to this image.

Select			
Database Replication.csv Refresh Download			
Regular Expression		Start Date & Time	End Date
<input type="text"/>		<input type="text" value="mm/dd/yyyy, hh:mm:ss"/>	<input type="text" value="mm/dd/yyyy"/>
<input type="button" value="Apply Filter"/>		<input type="button" value="Clear Filter"/>	
Filtering is not applied.			
Date ↓	Time	Status	Message
09/01/2006	11:54:58	INFO	Outbound replication cycle completed
09/01/2006	11:54:58	INFO	Replication to ACS 'AUSNMLAAA02' was successful
09/01/2006	11:54:42	INFO	Outbound replication cycle starting...

In addition, the log file on the secondary ACS server should contain no errors, similar to this image.

Select			
Database Replication.csv Refresh Download			
Regular Expression		Start Date & Time	End Date
<input type="text"/>		<input type="text" value="mm/dd/yyyy, hh:mm:ss"/>	<input type="text" value="mm/dd/yyyy"/>
<input type="button" value="Apply Filter"/>		<input type="button" value="Clear Filter"/>	
Filtering is not applied.			
Date ↓	Time	Status	Message
09/01/2006	11:52:51	INFO	Inbound database replication from ACS 'AUSNMLAAA01' completed
09/01/2006	11:52:38	INFO	Inbound database replication from ACS 'AUSNMLAAA01' started

Troubleshoot the Configuration

Use this section to troubleshoot your configuration.

Replication Problem

The setup has one primary and one secondary server. The primary server receives the error message as shown.

```
Primary(hostname): ACS 'hostname' has denied replication request
Secondary(hostname): Inbound database replication from ACS 'hostname' denied
```

Solution

- Remove the entry for the primary ACS server in the secondary ACS server since the ACS does not support two-way replication. Also, make sure that the received components options in secondary ACS are different from the send components options in the primary ACS.
- Make sure that the shared secret key is the same in both primary and secondary.

Note: Load sharing is not supported in ACS and works only as failover. If the primary fails, the secondary takes over.

Secondary ACS Server does not Restart the Service

After the DB replication between the primary ACS and the secondary ACS machines with *dual processor*, ACS services are not started within 30 minutes after rebooting secondary ACS machine.

Solution

You can fix this by rebooting the Secondary ACS only after 30 minutes if there is DB replication.

Procedures

To troubleshoot your configuration, complete one or more of these procedures:

- To ensure that database replication has completed successfully, view the Database Replication report on the primary and secondary ACS servers as described in Verify the Configuration.
- View the Windows Event logs for possible error messages.

Tips

- **Primary server must have all secondary servers listed** If you use a cascade of one primary server that sends data to a secondary server, which in turn sends to another server, you must configure all servers on the primary server. This requirement must be performed even if the primary server does not directly replicate to the server.
- **Access-list for TCP port 2000** If your primary server is outside a firewall, you must ensure that the destination TCP port 2000 is permitted through that firewall. The primary server uses a random source port and a destination port of 2000 for database replication.
- **Access-list for GRE or IPsec on firewall** Access-lists that permit GRE or IPsec are necessary if your traffic must traverse a firewall.
- **Database replication key** The key of the primary ACS server is very important to successful database replication. The key value must match exactly wherever the primary ACS server is defined.
- **ACS Error – Database file cannot be read into memory** This error occurs when the disk space on the server is exhausted. In order to resolve this error, free additional disk space on the server.
- **Error Message on External Database** Either the primary or secondary ACS server does not authenticate with the external database, such as LDAP, but the other works fine. Also, you receive the error authentication code, `External DB not operational`, which is located in the **Reports and Activity > Failed Attempts** dialog box of the ACS. In order to resolve this issue, choose **External Databases > Unknown User Policy**, and verify you have the LDAP database at the top and not the Windows database.
- **Base Image** Ensure that the primary and secondary ACS servers use the same base image version.
- **ACS Error – Cannot replicate to <Server Name> – server not responding** This error message appears in the replication report log when Database replication fails. This error is caused when **Skinny Inspection** is enabled as both Skinny protocol and Database replication in ACS uses same TCP port 2000. In order to resolve the issue, disable Skinny Inspection as shown below:

```
hostname# configure terminal
hostname(config)# policy-map global-policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# no inspect skinny
```

- **ACS Error – acs1 ERROR Inbound database replication** If you receive this error, verify that the IP addresses are correct.

```
acs1 ERROR Inbound database replication from ACS 'csacs1' denied -
shared secret mismatch
```

Related Information

- **ACS Internal Database Replication**
 - **Cisco Secure Access Control Server for Windows Release Notes**
 - **Cisco Secure ACS for Windows Compatibility**
 - **Supported and Interoperable Devices for Cisco Secure ACS for Windows 4.0**
 - **Technical Support & Documentation – Cisco Systems**
-

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

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 28, 2009

Document ID: 71320
