RSA SecurID Ready Implementation Guide

Last Modified: September 9, 2004

1. Partner Information

Partner Name	Cisco Systems, Inc.
Web Site	www.cisco.com
Product Name	Cisco Secure Access Control System (ACS)
Version & Platform	V3.3.1 for Windows
Product Description	Cisco Secure Access Control Server (ACS) for Windows provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control: Cisco Secure ACS is a main pillar of Cisco trust and identity networking security solutions. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework, allowing greater flexibility and mobility, increased security, and user productivity gains. With Cisco Secure ACS, you can manage and administer user access for Cisco IOS® routers, VPNs, firewalls, dialup and DSL connections, cable access solutions, storage, content, voice over IP (VoIP), Cisco wireless solutions, and Cisco Catalyst® switches using IEEE 802.1x access control.
Product Category	RADIUS Servers

2. Contact Information

	Sales Contact	**Support Contact**
E-mail	sales@cisco.com	tac@cisco.com
Phone	1 800 553 6387	1 800 553 2447
Web	www.cisco.com	www.cisco.com/public/support/tac/home.shtml

3. Solution Summary

Feature	Details
Authentication Methods Supported	Native RSA SecurID
RSA Authentication Agent Library Version	Version #5.0.2 [527]
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes/No (if yes list the number supported)
Location of Node Secret on Client	In Registry
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	Designated users, all users, RSA SecurID as default.
Support for Download of Offline Day Files	No
RSA SecurID Protection of Partner Product Administrators	No
RSA Software Token API Integration	No

4. Product Requirements

- ***Hardware requirements***

Component Name: Cisco Secure ACS	
CPU make/speed required	550 MHZ or faster
Memory	256 MB of RAM
HD space	250 MB of free disk space. If you are running your database on the same computer, more disk space is required.
Firmware level	

- ***Software requirements***

Component Name: Cisco Secure ACS	
Operating System	**Version (Patch-level)**
Windows	2000 Server SP4
Windows	2000 Advanced Server SP4
Windows	2003 Enterprise
Windows	2003 Standard Edition

Component Name: Cisco Secure ACS	
Web Browser	**Version (Patch-level)**
Microsoft Internet Explorer	6.0 SP2
	Sun Java Plug-in 1.4.2-04 or Microsoft Java Virtual Machine
Netscape Communicator	7.1
	Sun Java Plug-in 1.4.2-04

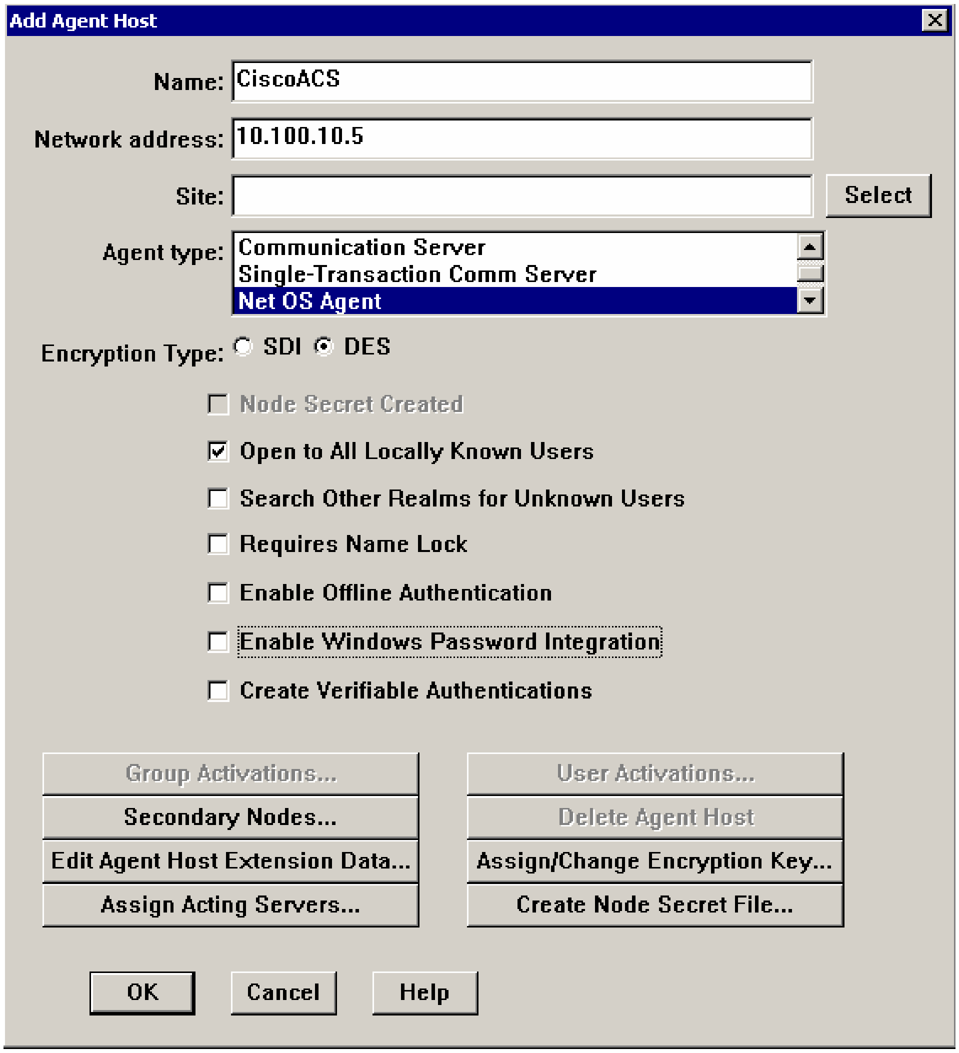
Note: Both Java and JavaScript must be enabled in browsers used to administer Cisco Secure ACS

5. RSA Authentication Manager configuration

Perform the following steps to set up the ***Cisco Secure ACS*** as an Agent Host within the RSA Authentication Manager's database.

- On the RSA Authentication Manager computer, go to **Start > Programs > RSA ACE Server**, and then **Database Administration - Host Mode**.

1. On the **Agent Host** menu, choose **Add Agent Host…**.



Add Agent Host

Name: CiscoACS

Network address: 10.100.10.5

Site:

Agent type: Communication Server / Single-Transaction Comm Server / Net OS Agent (selected)

Encryption Type: ○ SDI ● DES

□ Node Secret Created

☑ Open to All Locally Known Users

□ Search Other Realms for Unknown Users

□ Requires Name Lock

□ Enable Offline Authentication

□ Enable Windows Password Integration

□ Create Verifiable Authentications

- In **Name**, type the hostname of the Cisco Secure ACS.
- In **Network address**, type the IP address of the Cisco Secure ACS.
- For **Agent Type**, select ***Net OS Agent***.
- Under **Secondary Nodes**, define all hostname/IP addresses that resolve to the ***Cisco Secure ACS***. (IF NEEDED)

<u>**Note**</u>: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

6. Partner RSA Authentication Agent configuration

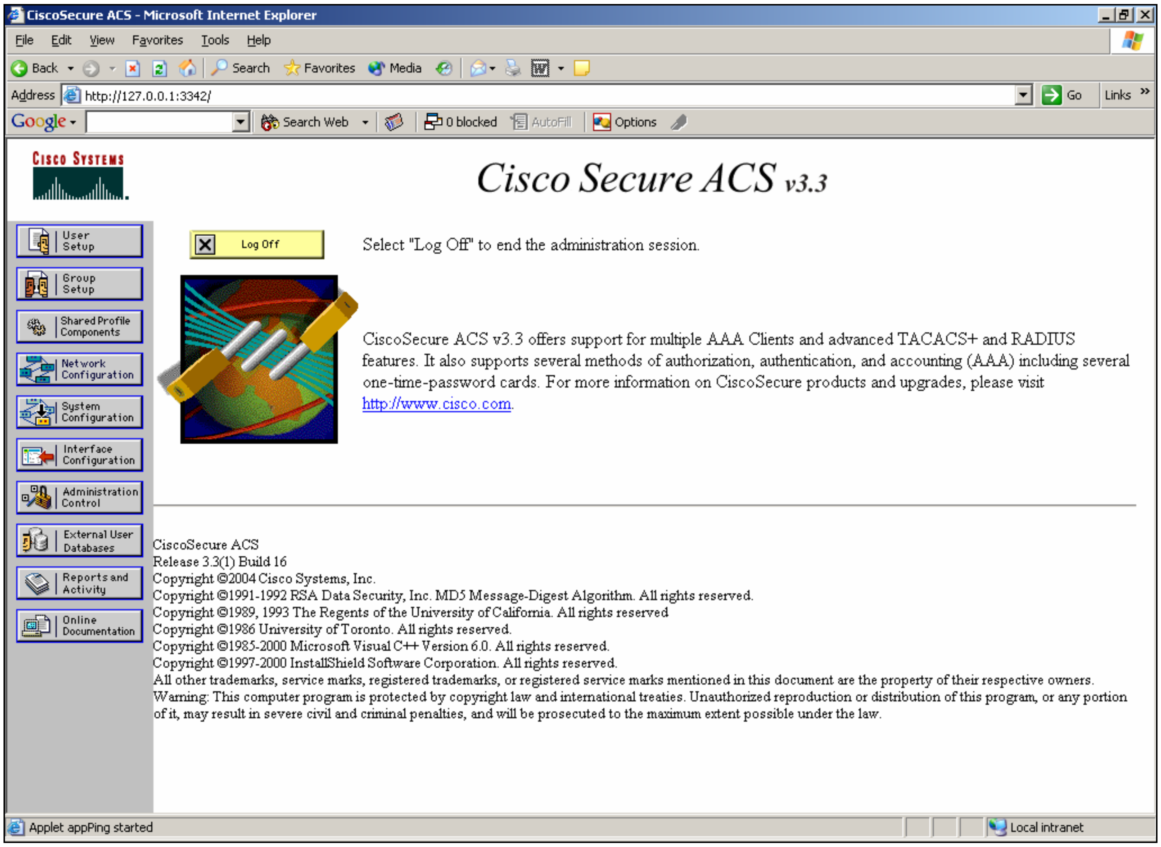
This section provides instructions for integrating the partners' product with RSA SecurID. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

- ## Activating SecurID authentication

Cisco Secure ACS supports SecurID authentication of users. To configure Cisco Secure ACS 3.3.1 to authenticate users with Authentication Manger 6.0, follow these steps:

1. Install the Authentication Agent 5.5 for Windows on the same system as the Cisco Secure ACS server. Verify connectivity by running the Test Authentication function of the Authentication Agent.

2. In the navigation bar, click, External User Databases

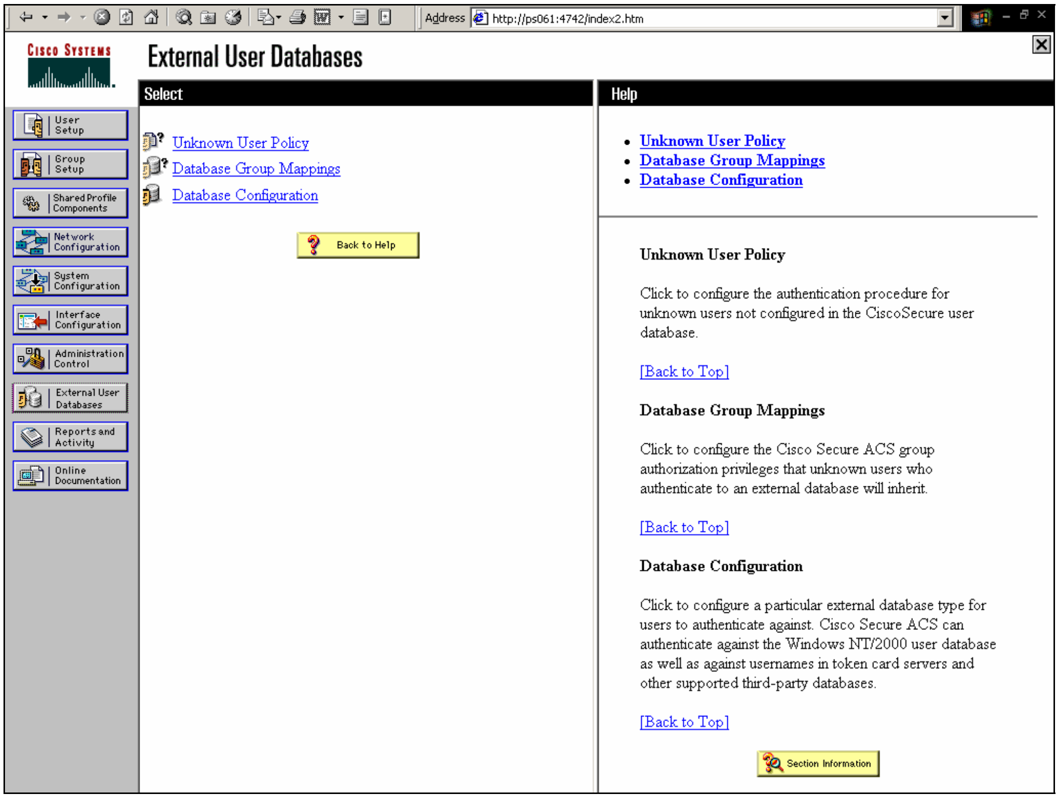


Select "Log Off" to end the administration session.

CiscoSecure ACS v3.3 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

CiscoSecure ACS
Release 3.3(1) Build 16
Copyright ©2004 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3. Click **Database Configuration**.



External User Databases

Select

Unknown User Policy

Database Group Mappings

Database Configuration

Help

- Unknown User Policy
- Database Group Mappings
- Database Configuration

Unknown User Policy

Click to configure the authentication procedure for unknown users not configured in the CiscoSecure user database.

[Back to Top]

Database Group Mappings

Click to configure the Cisco Secure ACS group authorization privileges that unknown users who authenticate to an external database will inherit.

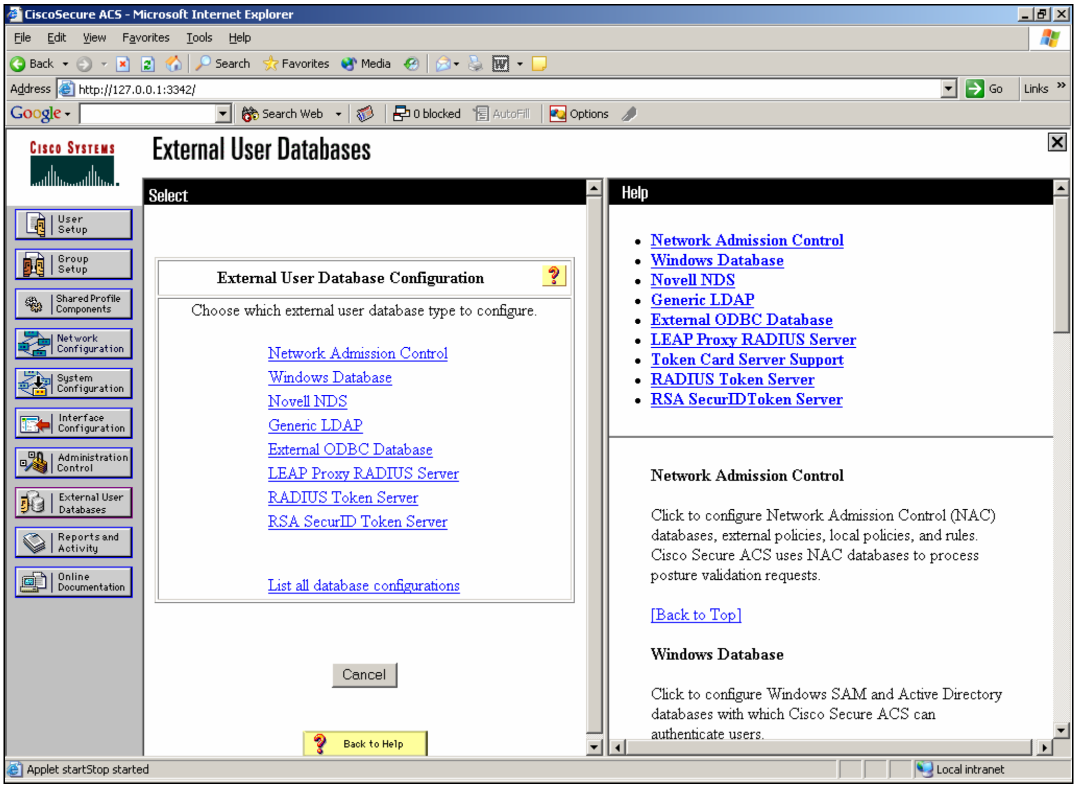
[Back to Top]

Database Configuration

Click to configure a particular external database type for users to authenticate against. Cisco Secure ACS can authenticate against the Windows NT/2000 user database as well as against usernames in token card servers and other supported third-party databases.

[Back to Top]

4. Click **RSA SecurID Token Server.**



External User Databases

Select

External User Database Configuration

Choose which external user database type to configure.

Network Admission Control

Windows Database

Novell NDS

Generic LDAP

External ODBC Database

LEAP Proxy RADIUS Server

RADIUS Token Server

RSA SecurID Token Server

List all database configurations

Help

- Network Admission Control
- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- RSA SecurIDToken Server

Network Admission Control

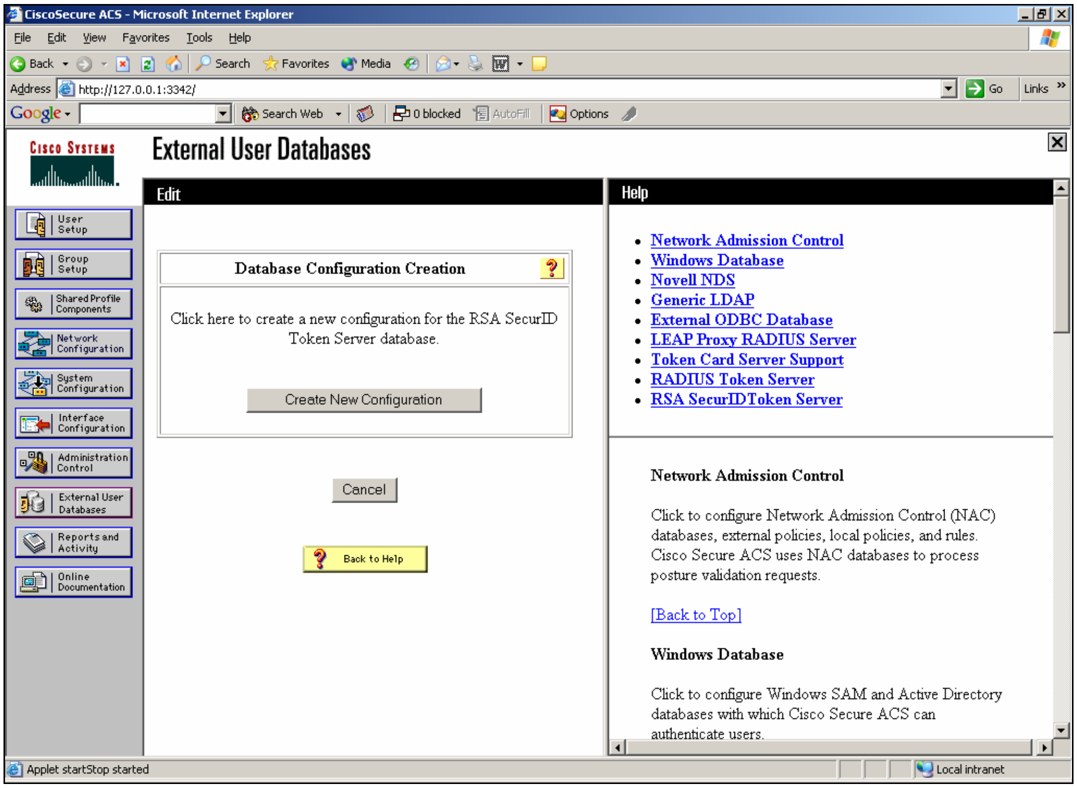
Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process posture validation requests.

[Back to Top]

Windows Database

Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.

5. Click **Create New Configuration.**



External User Databases

Database Configuration Creation

Click here to create a new configuration for the RSA SecurID Token Server database.

- Network Admission Control
- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- RSA SecurIDToken Server

Network Admission Control

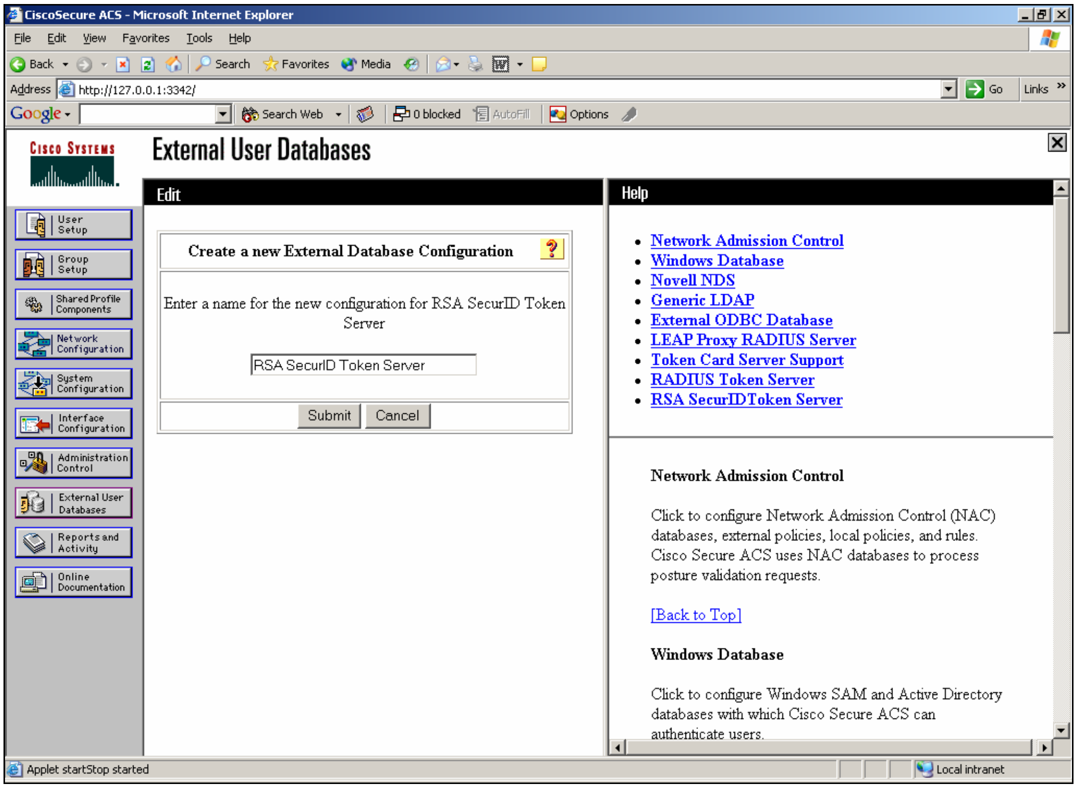
Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process posture validation requests.

[Back to Top]

Windows Database

Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.

6. Enter a name, then click **Submit.**



External User Databases

Create a new External Database Configuration

Enter a name for the new configuration for RSA SecurID Token Server

RSA SecurID Token Server

- Network Admission Control
- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- RSA SecurIDToken Server

Network Admission Control

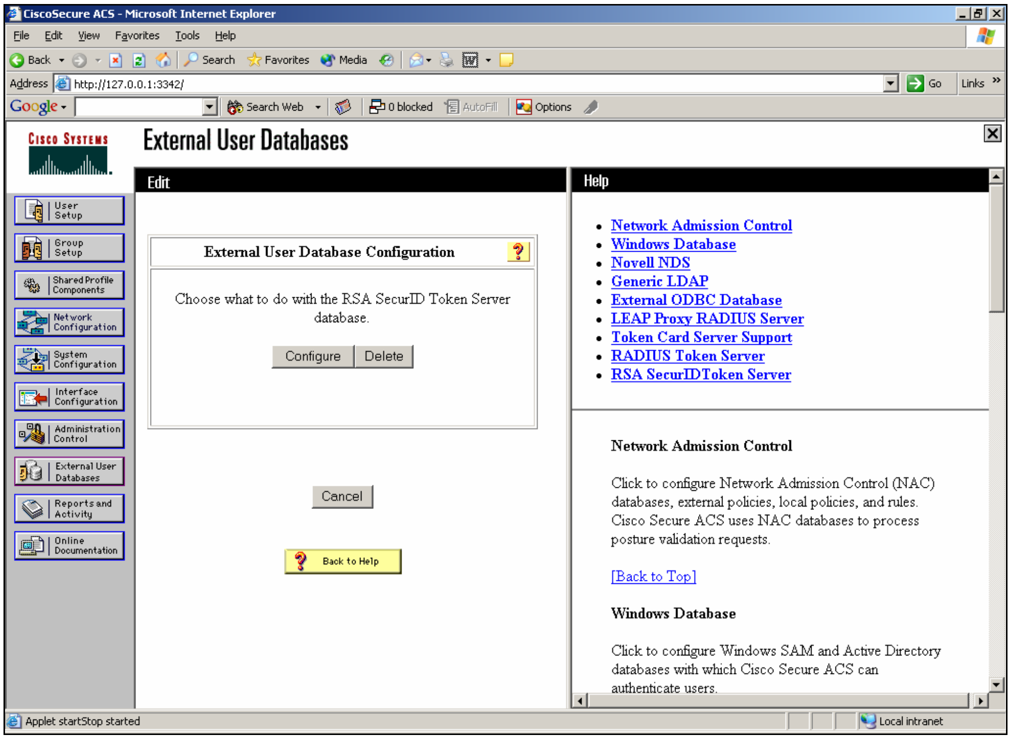
Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process posture validation requests.

[Back to Top]

Windows Database

Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.

7. Click **Configure**.



External User Databases

Edit

External User Database Configuration

Choose what to do with the RSA SecurID Token Server database.

Configure Delete

Cancel

Back to Help

Help

- Network Admission Control
- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- RSA SecurIDToken Server

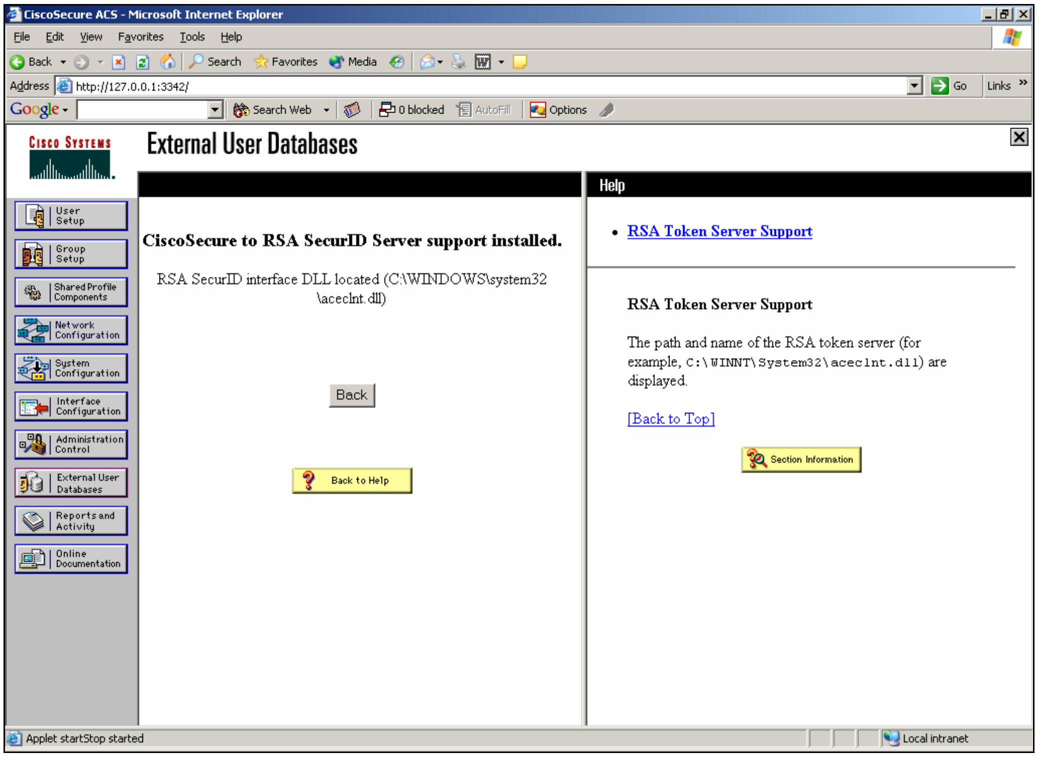
Network Admission Control

Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process posture validation requests.

[Back to Top]

Windows Database

Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.



External User Databases

CiscoSecure to RSA SecurID Server support installed.

RSA SecurID interface DLL located (C:\WINDOWS\system32\aceclnt.dll)

Back

Back to Help

Help

- RSA Token Server Support

RSA Token Server Support

The path and name of the RSA token server (for example, `C:\WINNT\System32\aceclnt.dll`) are displayed.

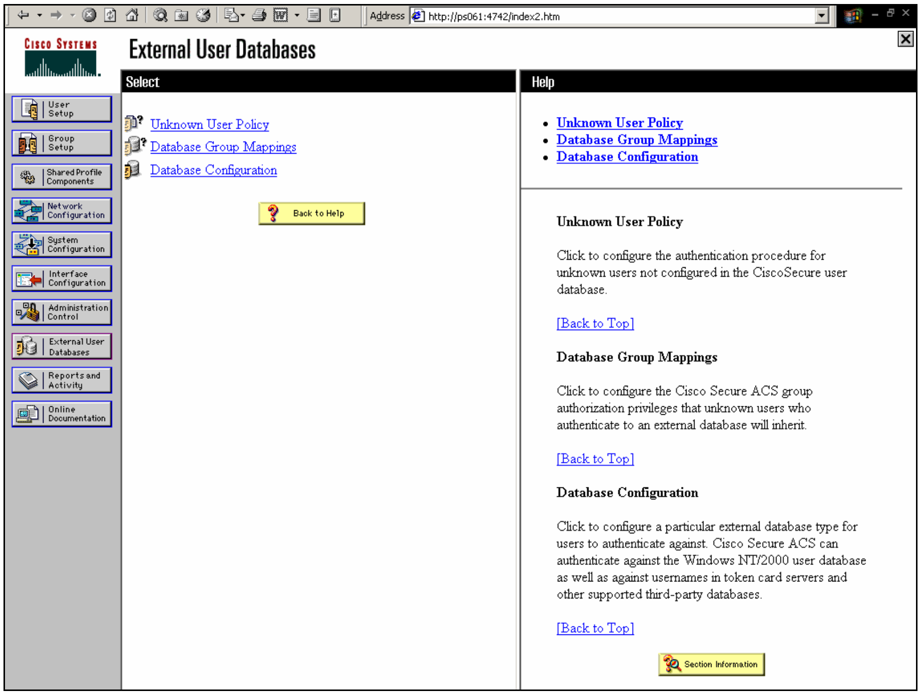
[Back to Top]

Section Information

Note: *Cisco Secure ACS displays the name of the token server and the path to the authenticator DLL. This information confirms that Cisco Secure ACS can contact the RSA agent. You can add the RSA SecurID external user database to your Unknown User Policy or assign specific user accounts to use this database for authentication.*

- **Adding/Configuring SecurID authentication to your Unknown User Policy**

1. Click External User Databases



External User Databases

Unknown User Policy
Database Group Mappings
Database Configuration

- Unknown User Policy
- Database Group Mappings
- Database Configuration

Unknown User Policy

Click to configure the authentication procedure for unknown users not configured in the CiscoSecure user database.

[Back to Top]

Database Group Mappings

Click to configure the Cisco Secure ACS group authorization privileges that unknown users who authenticate to an external database will inherit.

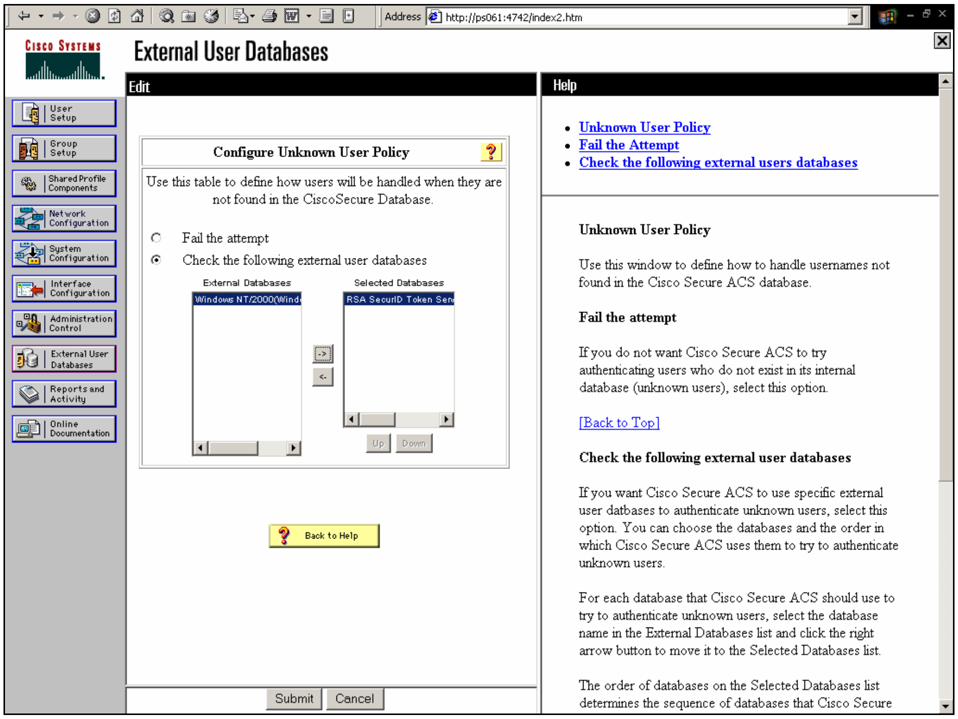
[Back to Top]

Database Configuration

Click to configure a particular external database type for users to authenticate against. Cisco Secure ACS can authenticate against the Windows NT/2000 user database as well as against usernames in token card servers and other supported third-party databases.

[Back to Top]

2. Click **Unknown User Policy**. Select ‘**Check the following external user databases**’ , highlight ‘**RSA SecurID Token Server**’ and move it to the ‘**Selected Databases**’ box. Click ‘**Submit**’.



External User Databases

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the CiscoSecure Database.

○ Fail the attempt
● Check the following external user databases

External Databases	Selected Databases
Windows NT/2000(Windo	RSA SecurID Token Serv

- Unknown User Policy
- Fail the Attempt
- Check the following external users databases

Unknown User Policy

Use this window to define how to handle usernames not found in the Cisco Secure ACS database.

Fail the attempt

If you do not want Cisco Secure ACS to try authenticating users who do not exist in its internal database (unknown users), select this option.

[Back to Top]

Check the following external user databases

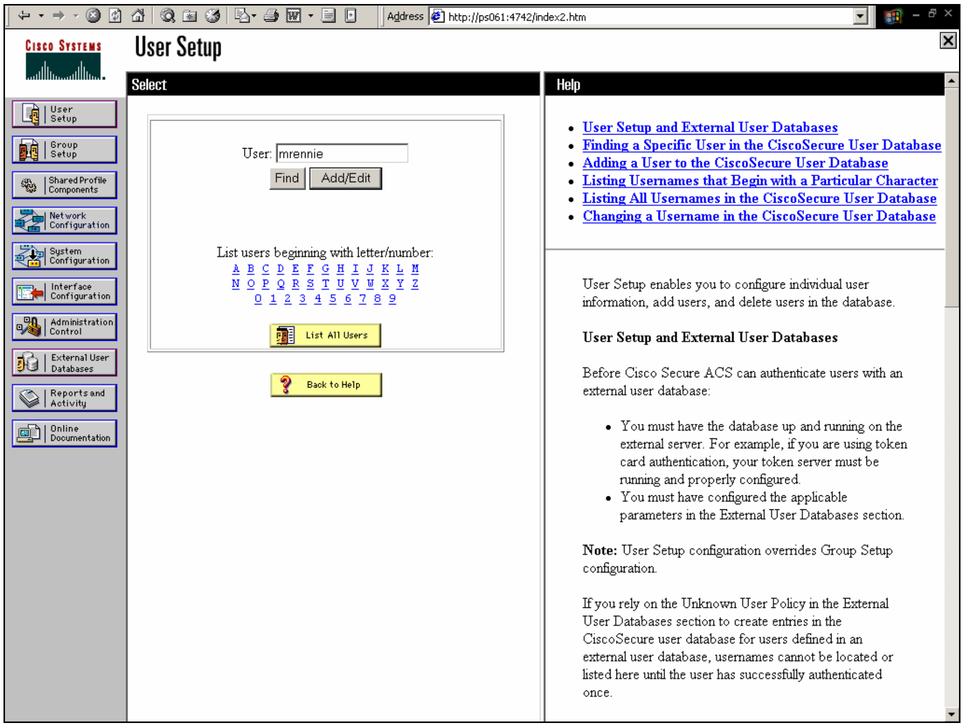
If you want Cisco Secure ACS to use specific external user datbases to authenticate unknown users, select this option. You can choose the databases and the order in which Cisco Secure ACS uses them to try to authenticate unknown users.

For each database that Cisco Secure ACS should use to try to authenticate unknown users, select the database name in the External Databases list and click the right arrow button to move it to the Selected Databases list.

The order of databases on the Selected Databases list determines the sequence of databases that Cisco Secure

- ## Adding/Configuring SecurID authentication for specific user accounts

1. Click User Setup from the main ACS Admin GUI. Type in the user name and click 'Add'.



User: mrennie

List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

- User Setup and External User Databases
- Finding a Specific User in the CiscoSecure User Database
- Adding a User to the CiscoSecure User Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the CiscoSecure User Database
- Changing a Username in the CiscoSecure User Database

User Setup enables you to configure individual user information, add users, and delete users in the database.

User Setup and External User Databases

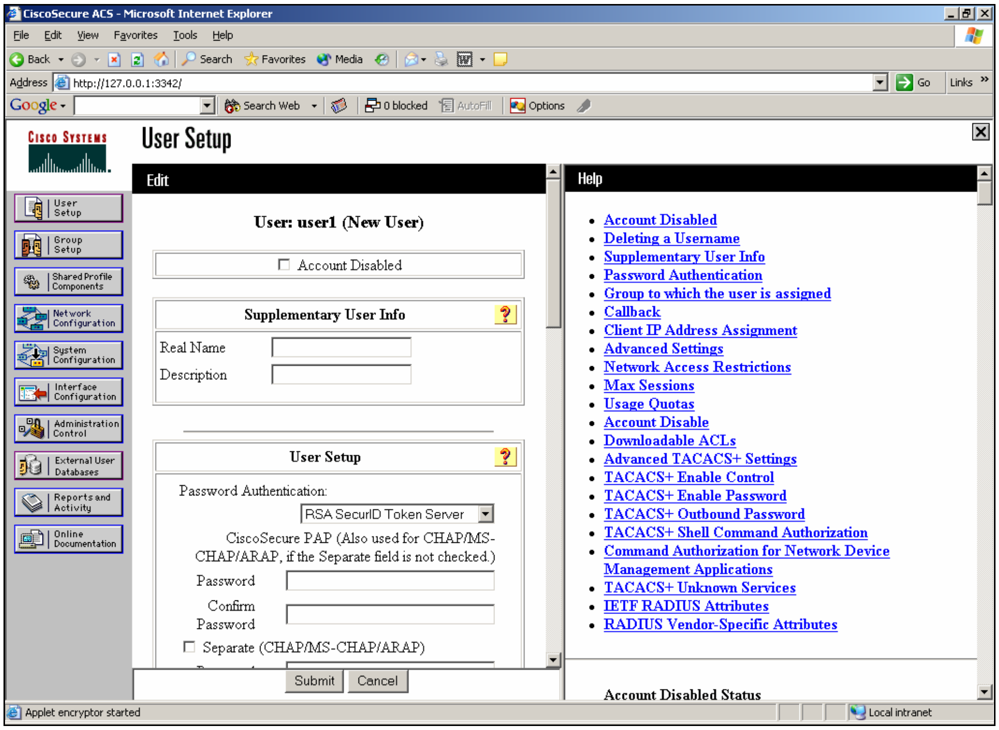
Before Cisco Secure ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

Note: User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the CiscoSecure user database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

2. Under User Setup…**Password Authentication**, choose **RSA SecurID Token Server**.



User: user1 (New User)

☐ Account Disabled

Supplementary User Info

Real Name
Description

User Setup

Password Authentication: RSA SecurID Token Server

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

☐ Separate (CHAP/MS-CHAP/ARAP)

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

7. Certification Checklist

Date Tested: September 10, 2004

Tested Certification Environment		
Product	**Platform (OS)**	**Product Version**
RSA Authentication Manager	WIN2K SP4	6.0
RSA Authentication Agent	WIN2K SP4	5.5
RSA Software Token	WIN2K SP4	3.0.3 [008]
Cisco Secure ACS	WIN2K SP4	3.3.1

Test		RSA Native Protocol	RADIUS Protocol
1st time auth. (node secret creation)		P	▨
New PIN mode:			
System-generated			
	Non-PINPAD token	P	
	PINPAD token	P	
User-defined (4-8 alphanumeric)			
	Non-PINPAD token	P	
	Password	P	
User-defined (5-7 numeric)			
	Non-PINPAD token	P	
	PINPAD token	P	
	Software token	P	
	Deny 4 digit PIN	P	
	Deny Alphanumeric	P	
User-selectable			
	Non-PINPAD token	P	
	PINPAD token	P	
PASSCODE			
	16 Digit PASSCODE	P	
	4 Digit Password	P	
	"Pin-less" TokenCode	P	
Next Tokencode mode			
	Non-PINPAD token	P	
	PINPAD token	P	
Software Token API Authentication			
	New PIN mode	N/A	
	8 Digit PIN with 8 Digit TokenCode	N/A	
Failover		P	
User Lock Test (RSA Name Lock Function)		P	▨
No RSA Authentication Manager		P	

SWA

Pass, Fail or N/A (N/A=Non-available function)

8. Known Issues

-

Appendix

-