# RSA SecurID Ready Implementation Guide

Last Modified: January 9, 2008

## Partner Information

| **Product Information** | |
|---|---|
| **Partner Name** | Cisco Systems, Inc. |
| **Web Site** | www.cisco.com |
| **Product Name** | Cisco Secure Access Control System (ACS) |
| **Version & Platform** | V4.1(4) 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:<br>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 |

# Solution Summary

| Partner Integration Overview | |
|---|---|
| **Authentication Methods Supported** | Native RSA SecurID Authentication |
| **List Library Version Used** | Version #5.0.3 |
| **RSA Authentication Manager Name Locking** | Yes |
| **RSA Authentication Manager Replica Support** | Full Replica Support |
| **Secondary RADIUS Server Support** | No |
| **Location of Node Secret on Agent** | In Registry |
| **RSA Authentication Agent Host Type** | Net OS |
| **RSA SecurID User Specification** | Designated Users, All Users, RSA SecurID as Default |
| **RSA SecurID Protection of Administrative Users** | No |
| **RSA Software Token and RSA SecurID 800 Automation** | No |
| **Use of Cached Domain Credentials** | No |

# Product Requirements

| Partner Product Requirements: Cisco Secure ACS | |
|---|---|
| **CPU** | x86 550MHz or faster |
| **Memory** | 256MB |
| **Storage** | 250MB of Hard Disk space. More disk space required for configurations also running a Database. |
| | |

| Operating System | |
|---|---|
| **Platform** | **Required Patches** |
| Microsoft Windows 2000 Server | Service Pack 4 or greater |
| Microsoft Windows 2000 Advanced Server | Service Pack 4 or greater |
| Microsoft Windows 2003 Server | All Service Levels Supported |
| Microsoft Windows 2003 Enterprise Server | All Service Levels Supported |
| | |

| Additional Software Requirements | |
|---|---|
| **Application** | **Additional Patches** |
| Microsoft Internet Explorer 6.0 | Service Pack 2<br>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: There was an issue with NEW-PIN mode with Cisco ACS 4.0 that was corrected with a fix from Cisco. Please contact Cisco to get this patch**

**ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip**

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

# Agent Host Configuration

To facilitate communication between the Cisco Secure ACS and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the Cisco Secure ACS within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the Cisco Secure ACS as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the Cisco Secure ACS will occur.

**Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

# Partner Authentication Agent Configuration

## Before You Begin

This section provides instructions for integrating the partners’ product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

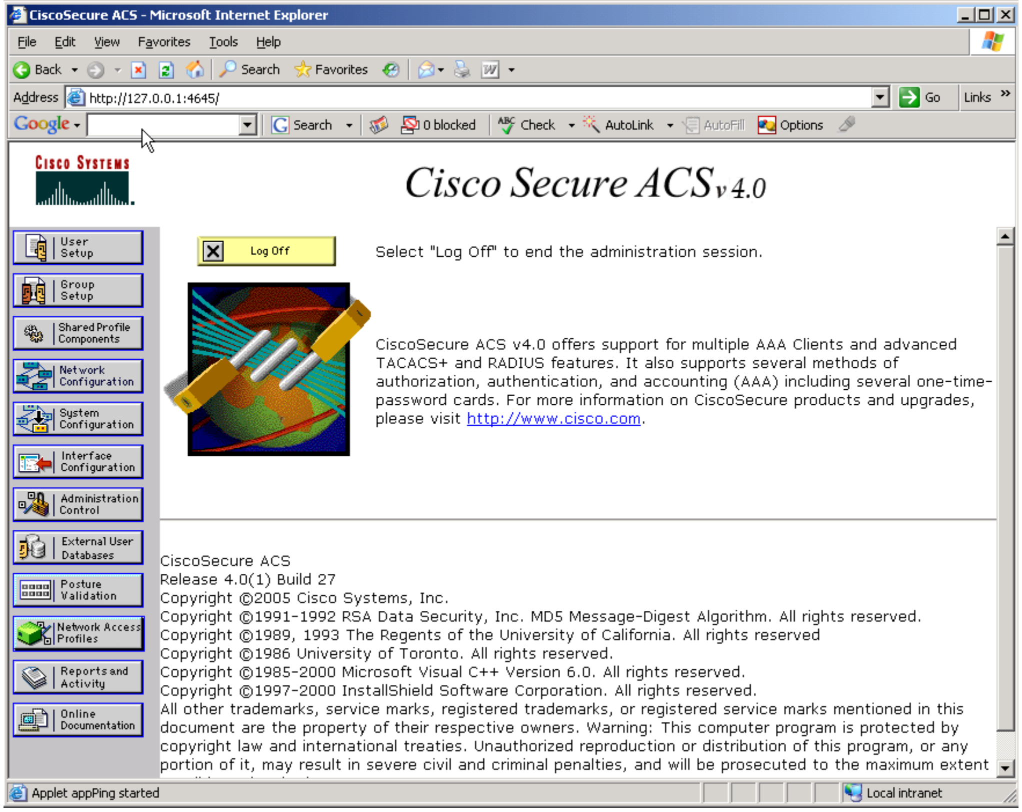
All vendor products/components must be installed and working prior to the integration.  Perform the necessary tests to confirm that this is true before proceeding.

## Documenting the Solution

### Activating RSA SecurID authentication:

Cisco Secure ACS supports RSA SecurID authentication of users.  To configure Cisco Secure ACS 4.0(1) to authenticate users with RSA Authentication Manger 6.1, follow these steps:

1. Install the **RSA Local Authentication Agent 6.1** 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.

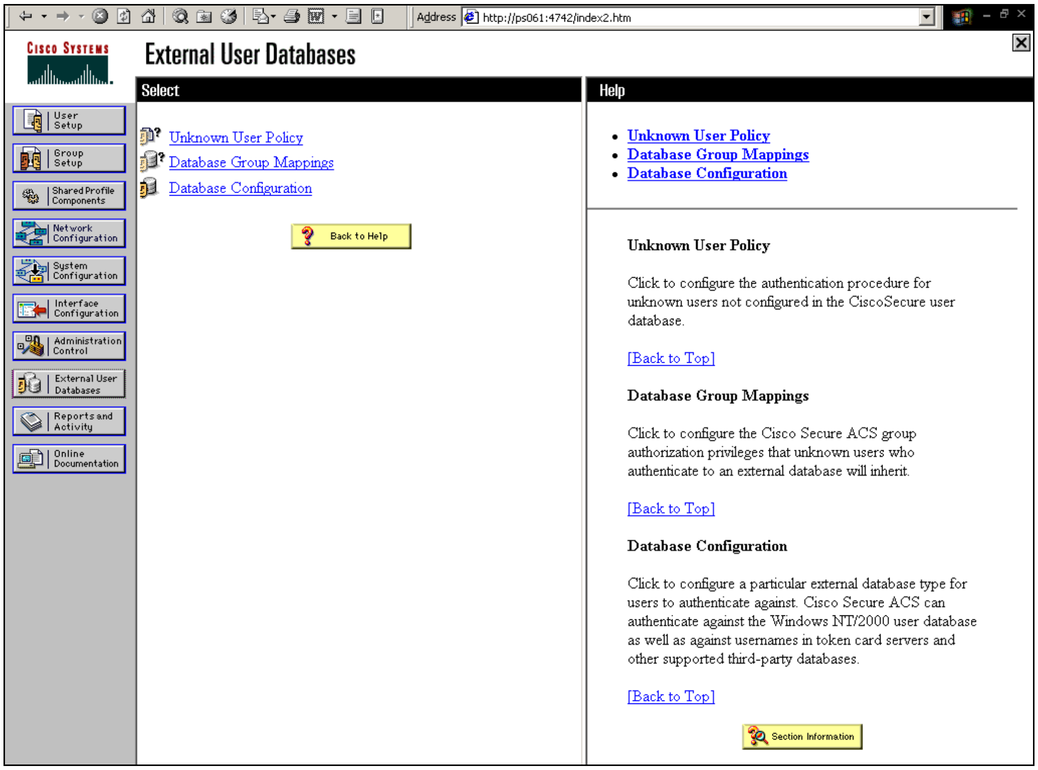


Select "Log Off" to end the administration session.

CiscoSecure ACS v4.0 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 4.0(1) Build 27
Copyright ©2005 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

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.

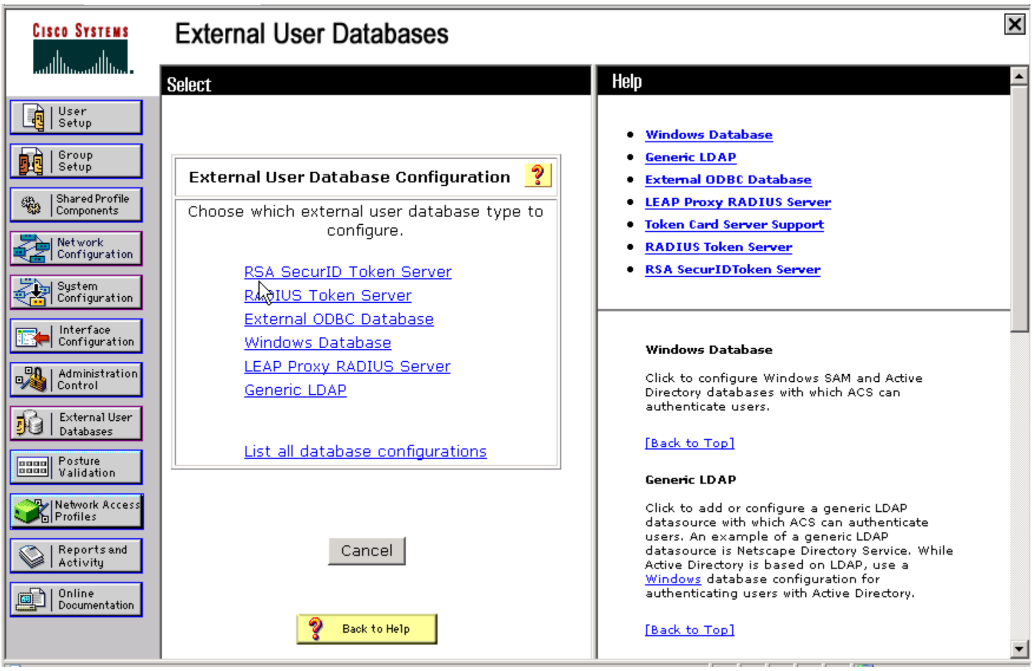
[Back to Top]

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.

RSA SecurID Token Server

RADIUS Token Server

External ODBC Database

Windows Database

LEAP Proxy RADIUS Server

Generic LDAP

List all database configurations

Help

- Windows Database
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- RSA SecurIDToken Server

Windows Database

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

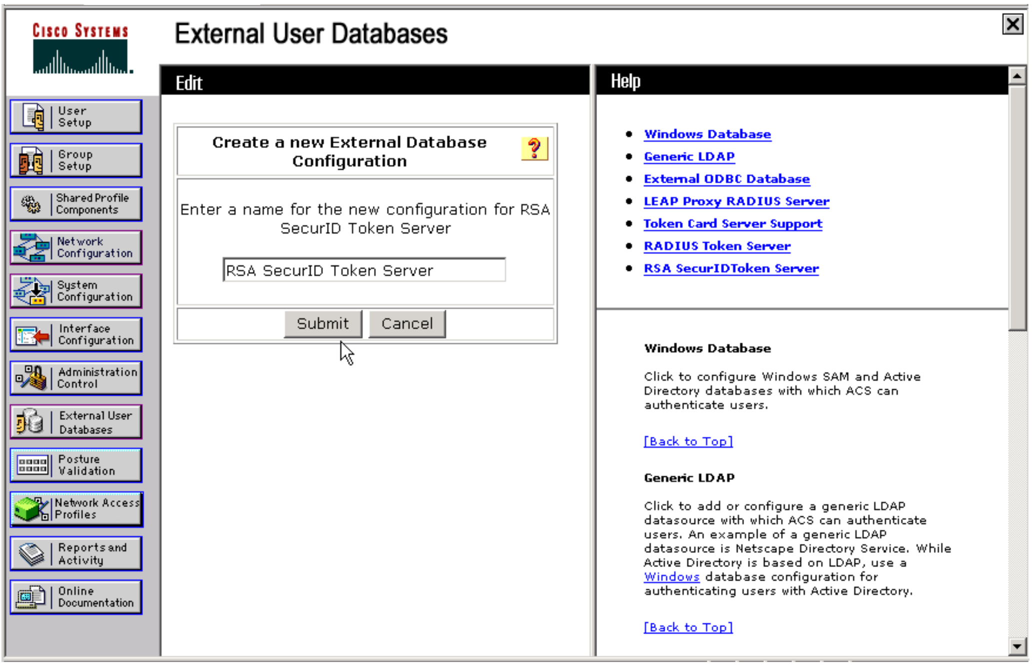
[Back to Top]

Generic LDAP

Click to add or configure a generic LDAP datasource with which ACS can authenticate users. An example of a generic LDAP datasource is Netscape Directory Service. While Active Directory is based on LDAP, use a Windows database configuration for authenticating users with Active Directory.

[Back to Top]

5. Click **Create New Configuration**.



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

**Windows Database**

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

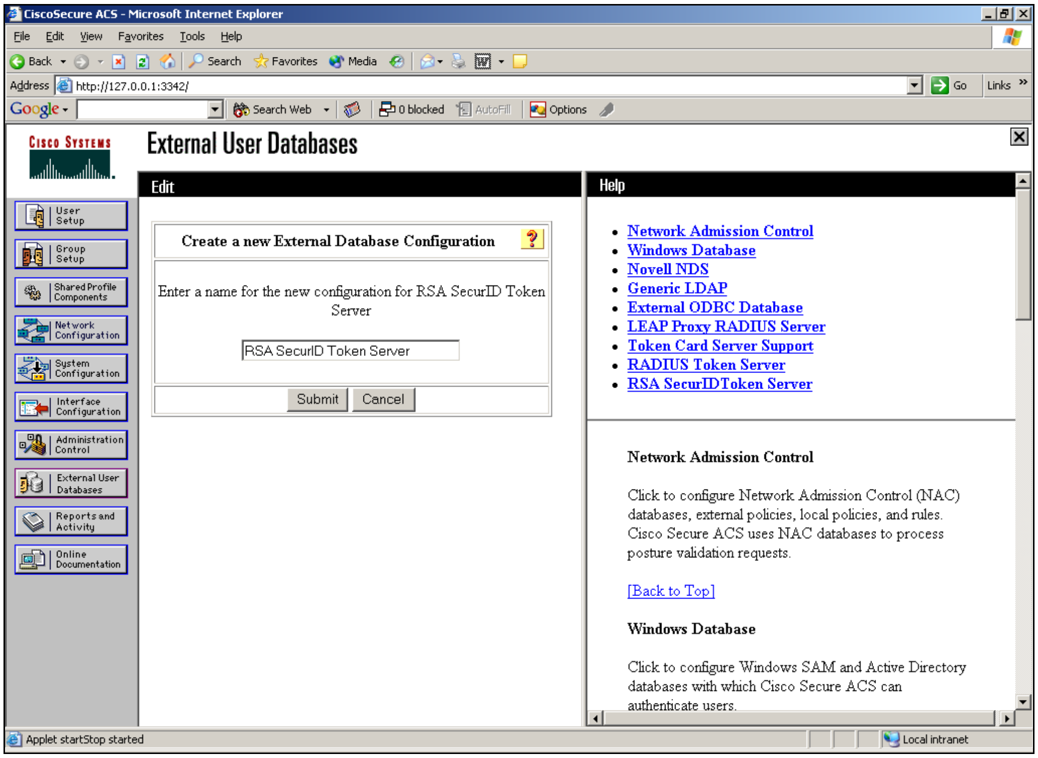
[Back to Top]

**Generic LDAP**

Click to add or configure a generic LDAP datasource with which ACS can authenticate users. An example of a generic LDAP datasource is Netscape Directory Service. While Active Directory is based on LDAP, use a Windows database configuration for authenticating users with Active Directory.

[Back to Top]

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



CiscoSecure ACS - Microsoft Internet Explorer

Address http://127.0.0.1:3342/

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**

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.

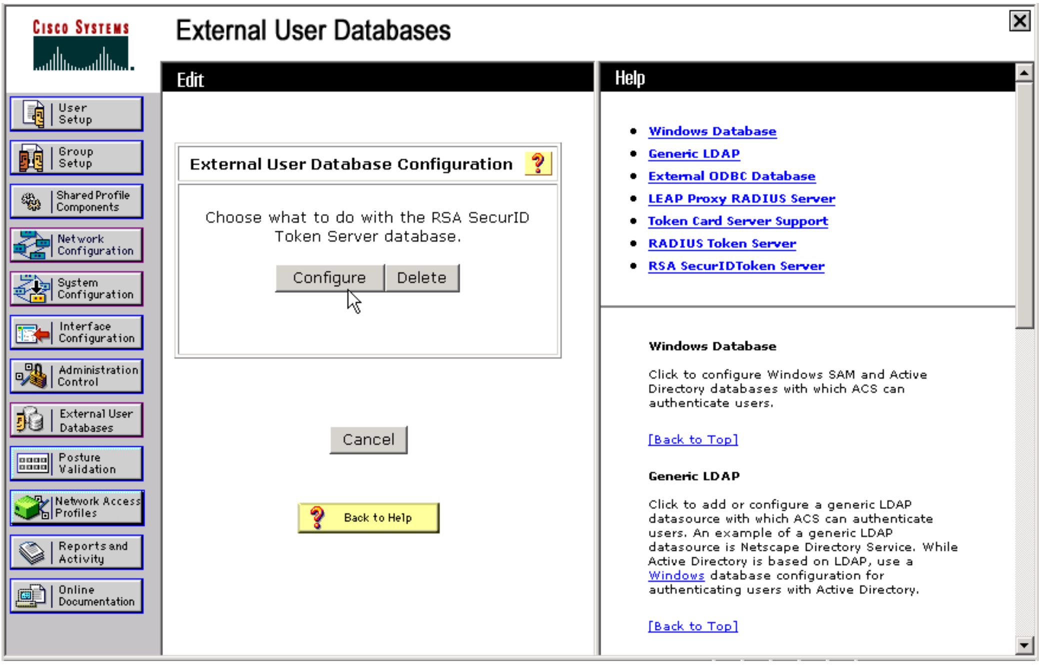
[Back to Top]

**Windows Database**

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

Applet startStop started

7. Click **Configure**.



External User Databases

External User Database Configuration

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

- Windows Database
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- RSA SecurIDToken Server

**Windows Database**

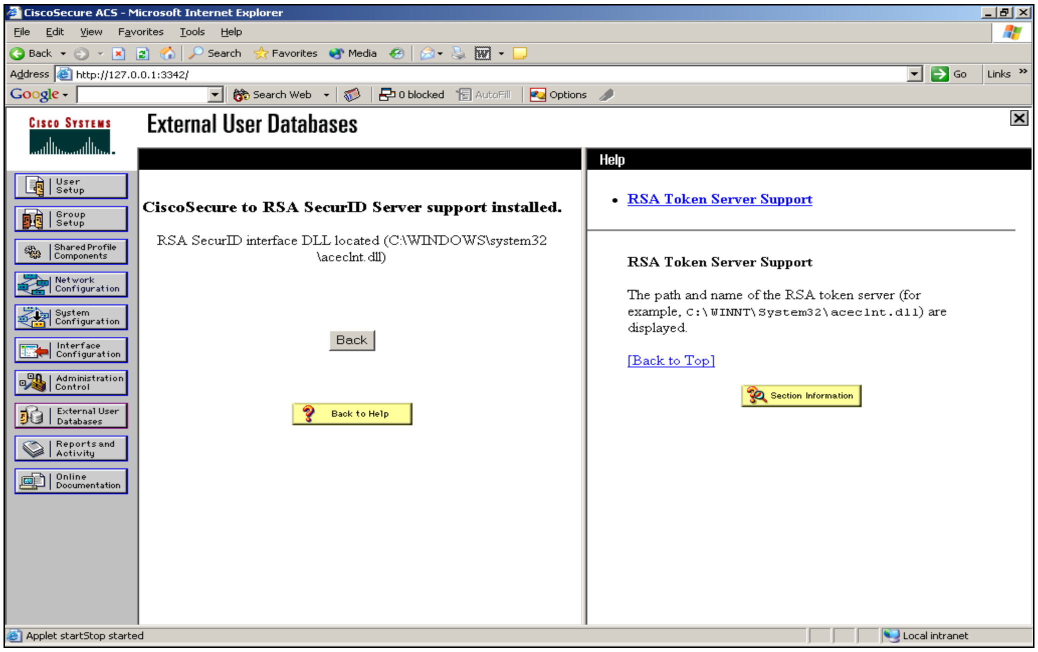
Click to configure Windows SAM and Active Directory databases with which ACS can authenticate users.

[Back to Top]

**Generic LDAP**

Click to add or configure a generic LDAP datasource with which ACS can authenticate users. An example of a generic LDAP datasource is Netscape Directory Service. While Active Directory is based on LDAP, use a Windows database configuration for authenticating users with Active Directory.

[Back to Top]



External User Databases

**CiscoSecure to RSA SecurID Server support installed.**

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

- RSA Token Server Support

**RSA Token Server Support**

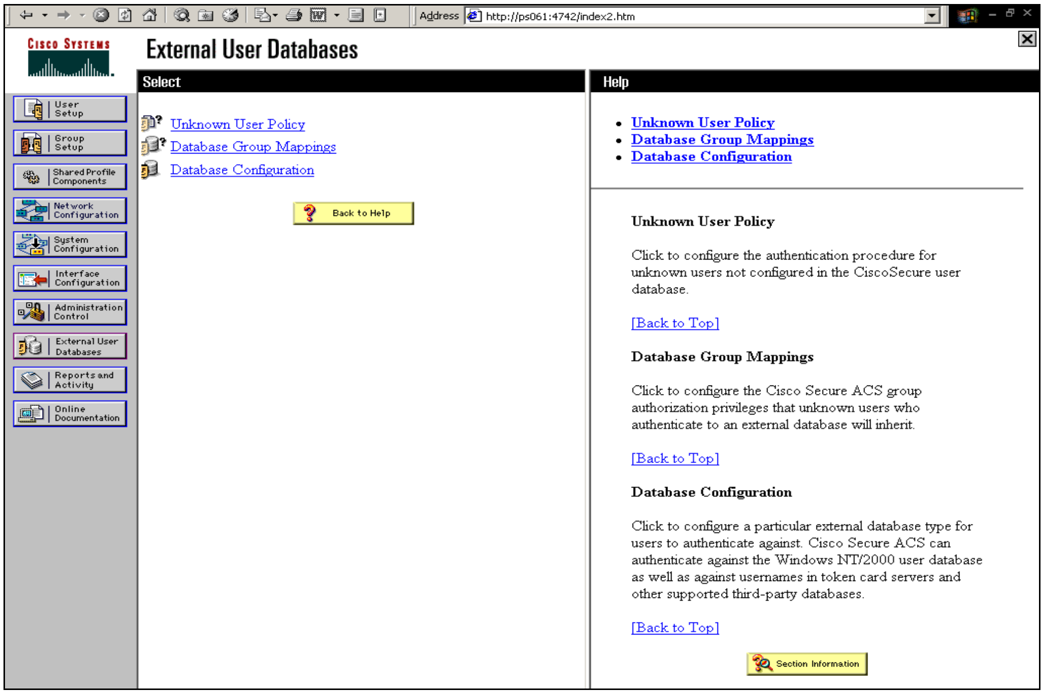
The path and name of the RSA token server (for example, C:\WINNT\System32\aceclnt.dll) are displayed.

[Back to Top]

**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 Authentication 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 RSA SecurID Authentication to your Unknown User Policy:

1. Click External User Databases.



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.

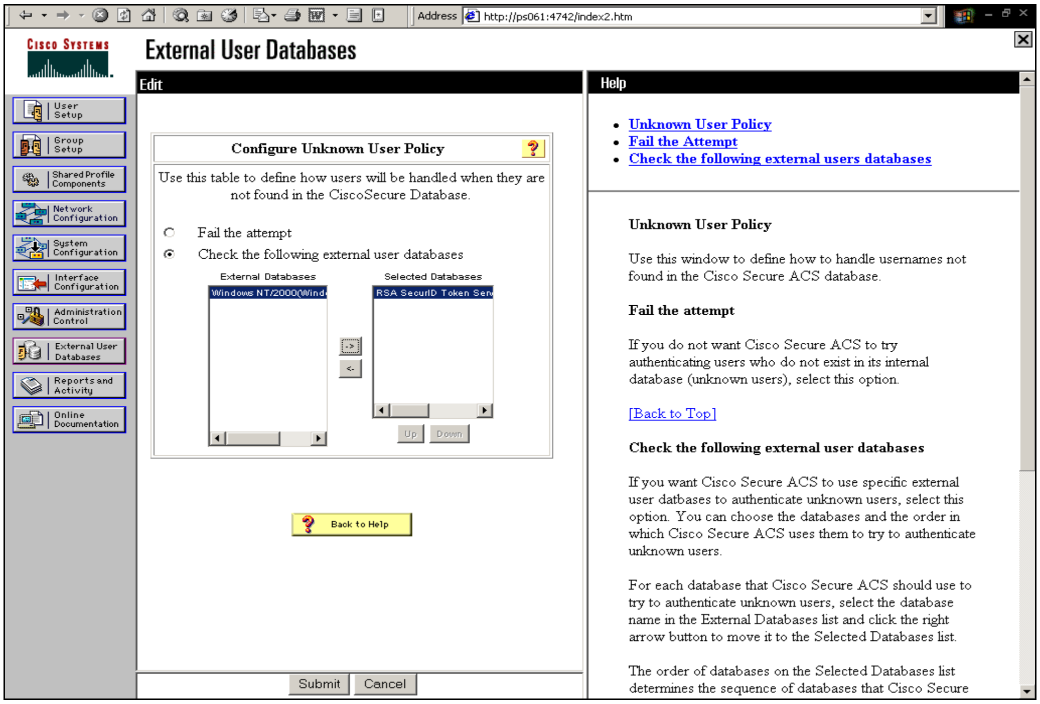
[Back to Top]

**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]

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

Edit

**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(Wind | RSA SecurID Token Serv |

Help

- 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**

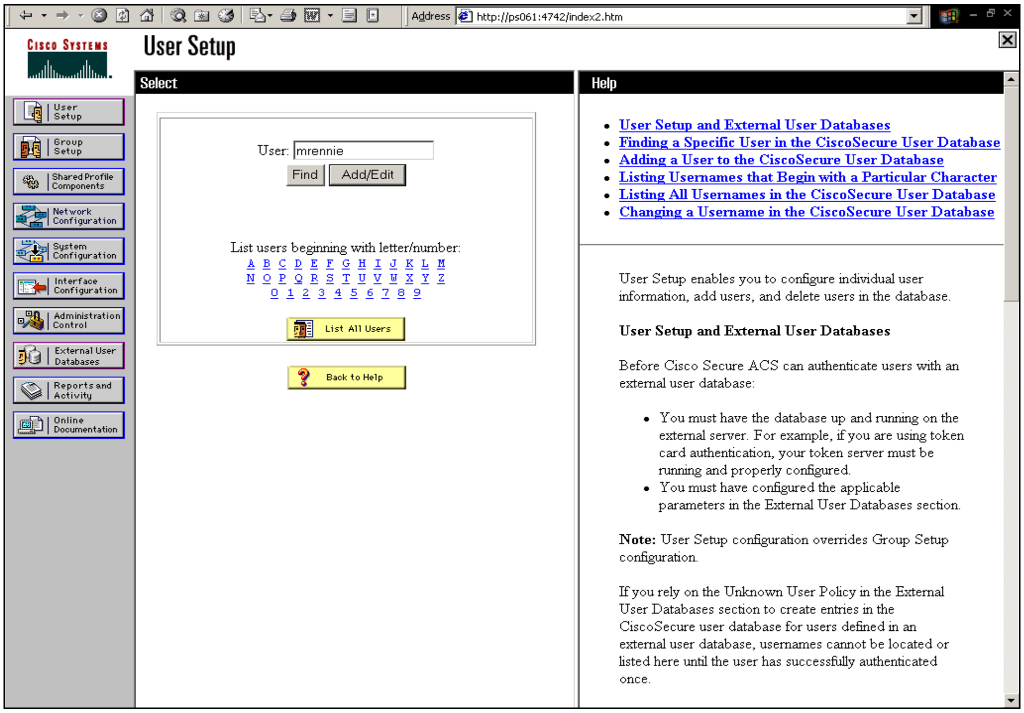
If you want Cisco Secure ACS to use specific external user datbases to authenticate unknown users, select this option. You can choose the databases and the order in which Cisco Secure ACS uses them to try to authenticate unknown users.

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 RSA 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:

- 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**

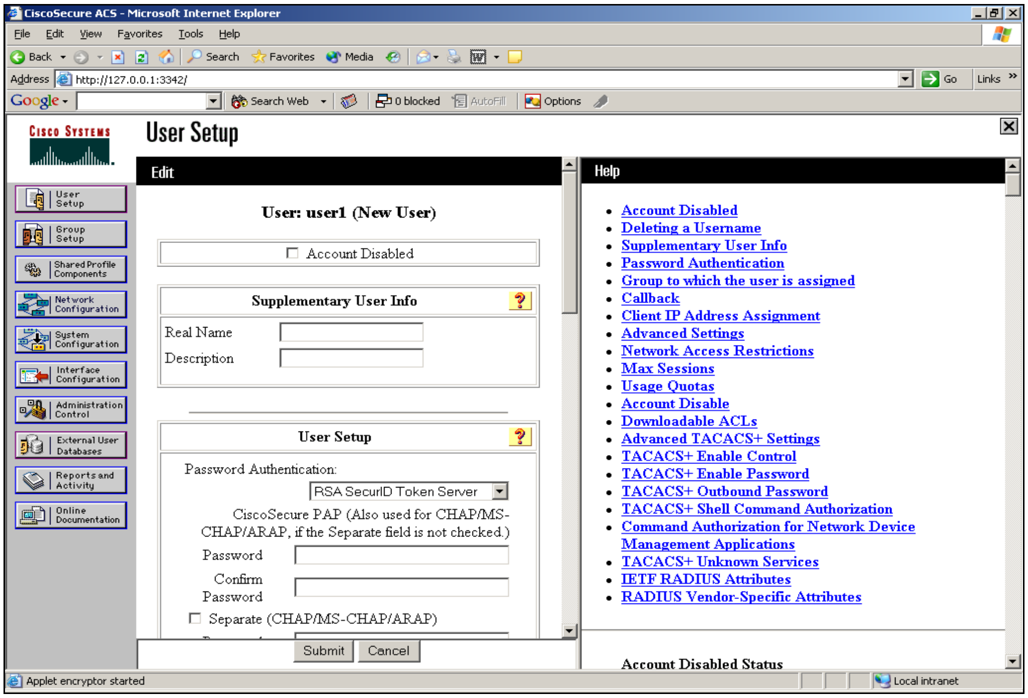
Before Cisco Secure ACS can authenticate users with an external user database:

- 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**. Click **Submit**.



**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**

# Certification Checklist

Date Tested: January 9, 2008

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | 6.1.2 | Windows 2003 |
| **RSA Authentication Agent** | 6.1 | Windows 2003 |
| **Cisco Secure ACS** | 4.1(4) Build 13 | Windows 2003 |
| | | |

| Mandatory Functionality | | | |
|---|---|---|---|
| **RSA Native Protocol** | | **RADIUS Protocol** | |
| **New PIN Mode** | | | |
| Force Authentication After New PIN | ✓ | Force Authentication After New PIN | N/A |
| System Generated PIN | ✓ | System Generated PIN | N/A |
| User Defined (4-8 Alphanumeric) | ✓ | User Defined (4-8 Alphanumeric) | N/A |
| User Defined (5-7 Numeric) | ✓ | User Defined (5-7 Numeric) | N/A |
| User Selectable | ✓ | User Selectable | N/A |
| Deny 4 and 8 Digit PIN | ✓ | Deny 4 and 8 Digit PIN | N/A |
| Deny Alphanumeric PIN | ✓ | Deny Alphanumeric PIN | N/A |
| **PASSCODE** | | | |
| 16 Digit PASSCODE | ✓ | 16 Digit PASSCODE | N/A |
| 4 Digit Password | ✓ | 4 Digit Password | N/A |
| **Next Tokencode Mode** | | | |
| Next Tokencode Mode | ✓ | Next Tokencode Mode | N/A |
| **Load Balancing / Reliability Testing** | | | |
| Failover (3-10 Replicas) | ✓ | Failover | N/A |
| Name Locking Enabled | ✓ | Name Locking Enabled | |
| No RSA Authentication Manager | ✓ | No RSA Authentication Manager | N/A |
| **Additional Functionality** | | | |
| **RSA Software Token API Functionality** | | | |
| System Generated PIN | N/A | System Generated PIN | N/A |
| User Defined (8 Digit Numeric) | N/A | User Defined (8 Digit Numeric) | N/A |
| User Selectable | N/A | User Selectable | N/A |
| Next Tokencode Mode | N/A | Next Tokencode Mode | N/A |
| **RSA SecurID 800 Token Automation** | | | |
| System Generated PIN | N/A | System Generated PIN | N/A |
| User Defined (8 Digit Numeric) | N/A | User Defined (8 Digit Numeric) | N/A |
| User Selectable | N/A | User Selectable | N/A |
| Next Tokencode Mode | N/A | Next Tokencode Mode | N/A |
| **Domain Credential Functionality** | | | |
| Determine Cached Credential State | N/A | Determine Cached Credential State | |
| Set Domain Credential | N/A | Set Domain Credential | |
| Retrieve Domain Credential | N/A | Retrieve Domain Credential | |

PAR/CMY

✓ = Pass ✗ = Fail N/A = Non-Available Function

## Known Issues

1. Force Authentication after New PIN in **System Generated Mode** does not occur. Force Authentication after New PIN in **User Defined Mode** functions as designed.