

Configuring Cisco Secure ACS for Windows NT with ACE Server Authentication

Document ID: 20713

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure ACS to Communicate with ACE

Configure an ACS User for ACE Authentication

Test the ACS Communication with ACE and a Network Device for Telnet

Test the ACS Communication with ACE and a Network Device for Dial (Optional)

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

Cisco Secure Access Control Software (ACS) for Windows can be integrated with RSA's ACE Server, also known as the Security Dynamics Incorporated (SDI) server. Requests that come in from devices in the network via TACACS+ or RADIUS can be processed by ACS directly, or ACS can hand off to the ACE server. If the request is handed off to the ACE server, the ACE server responds to ACS, and ACS responds to the network device. Users passed off to ACE can be enumerated, input with the Cisco Secure ACS command-line utility (CSUtil), or placed in the 'unknown user' category.

Note: For more information on CSUtil, refer to the Cisco Secure Command-Line Database Utility documentation.

This document is not intended to cover installation of the ACE server or client. Refer to the ACE documentation for the version of code that you run for further information. Versions of ACE tested with ACS are listed in the ACS release notes for the various ACS versions.

You can install ACS with ACE in these configurations:

- The ACE server, ACE client and ACS on the same box.
- The ACE server on one box and the ACE client with ACS on another box.
- The ACE server, without the ACE client, and ACS on the same box.

Prerequisites

Requirements

Ensure that you perform these steps before you configure the Cisco Secure ACS with ACE server authentication.

1. Install the ACE server with the use of the ACE directions.

2. Install the ACE client with the use of the ACE directions.

Note: If the ACS and ACE servers are on the same box, installation of the ACE client is optional, but useful for testing and troubleshooting.

3. Test the ACE client to the ACE server connectivity with a test user.

4. Install and test ACS to a Cisco device with a non-ACE Telnet (test) user.

5. Install and test ACS to a Cisco device with a non-ACE dial (test) user. This is optional unless the goal is to ultimately have ACE dial users.

Components Used

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

- ACE Server Version 5.0.01[061]
- ACE Agent Version 5.0
- Cisco Secure ACS for Windows 3.0.1

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.

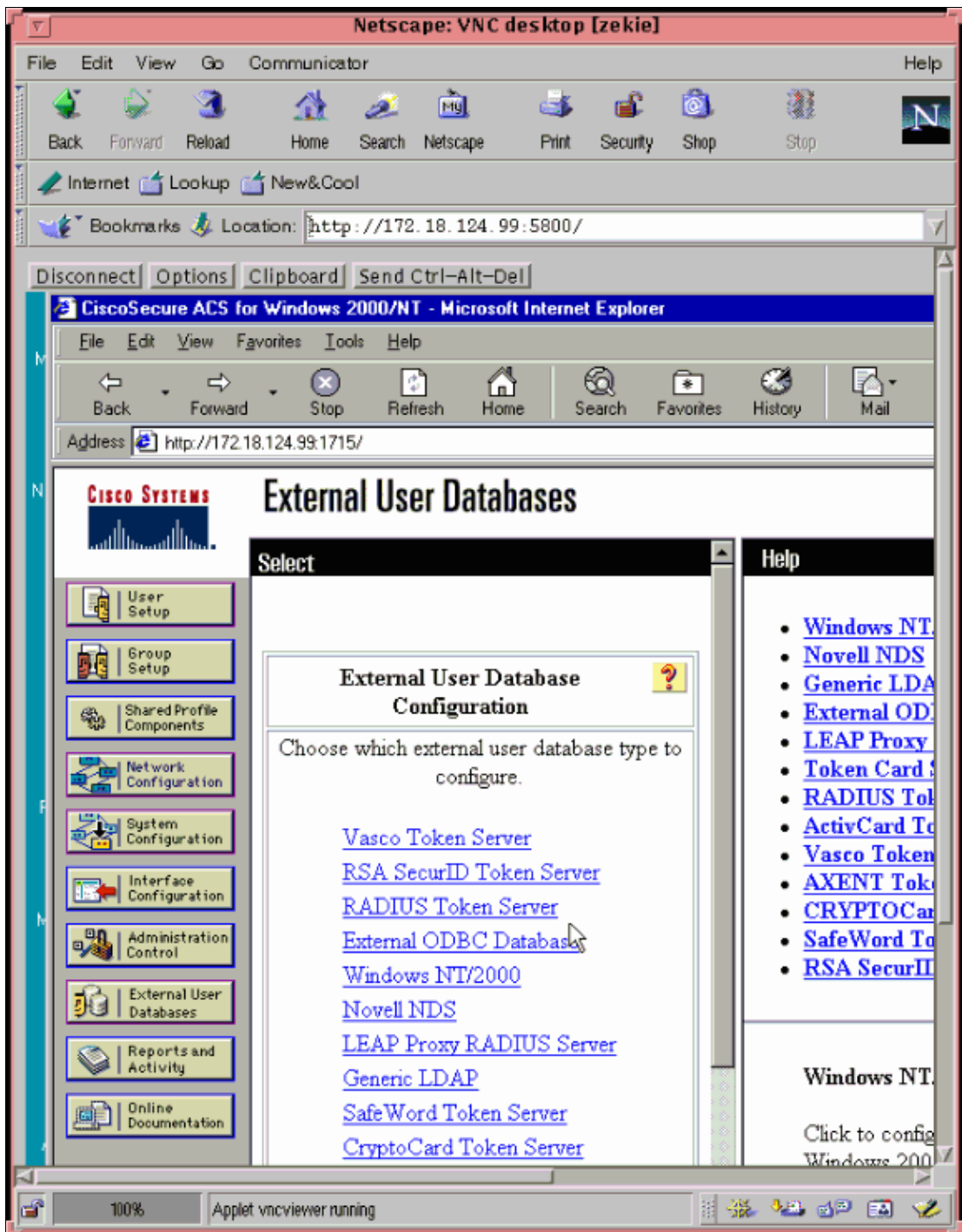
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

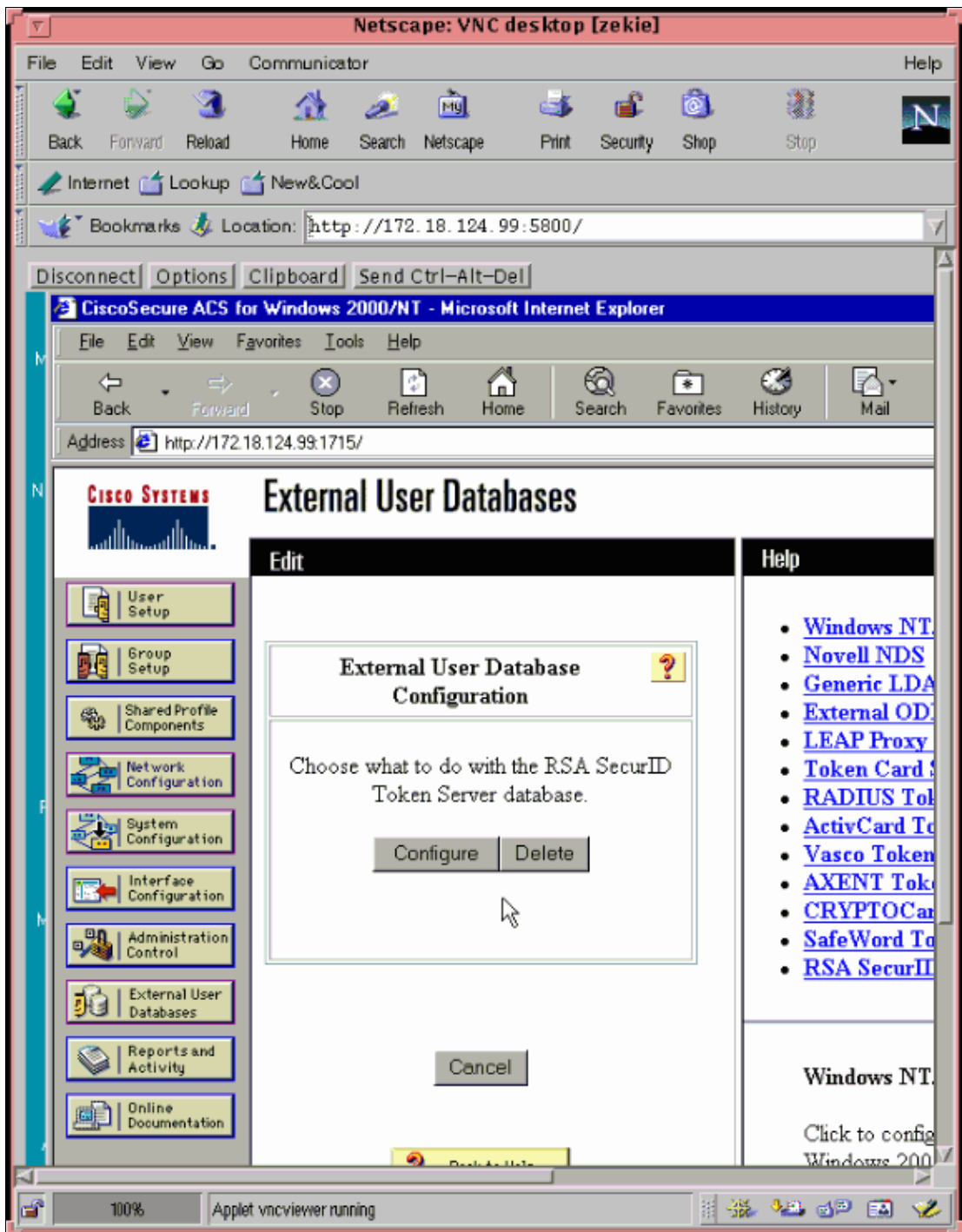
Configure ACS to Communicate with ACE

Complete these steps.

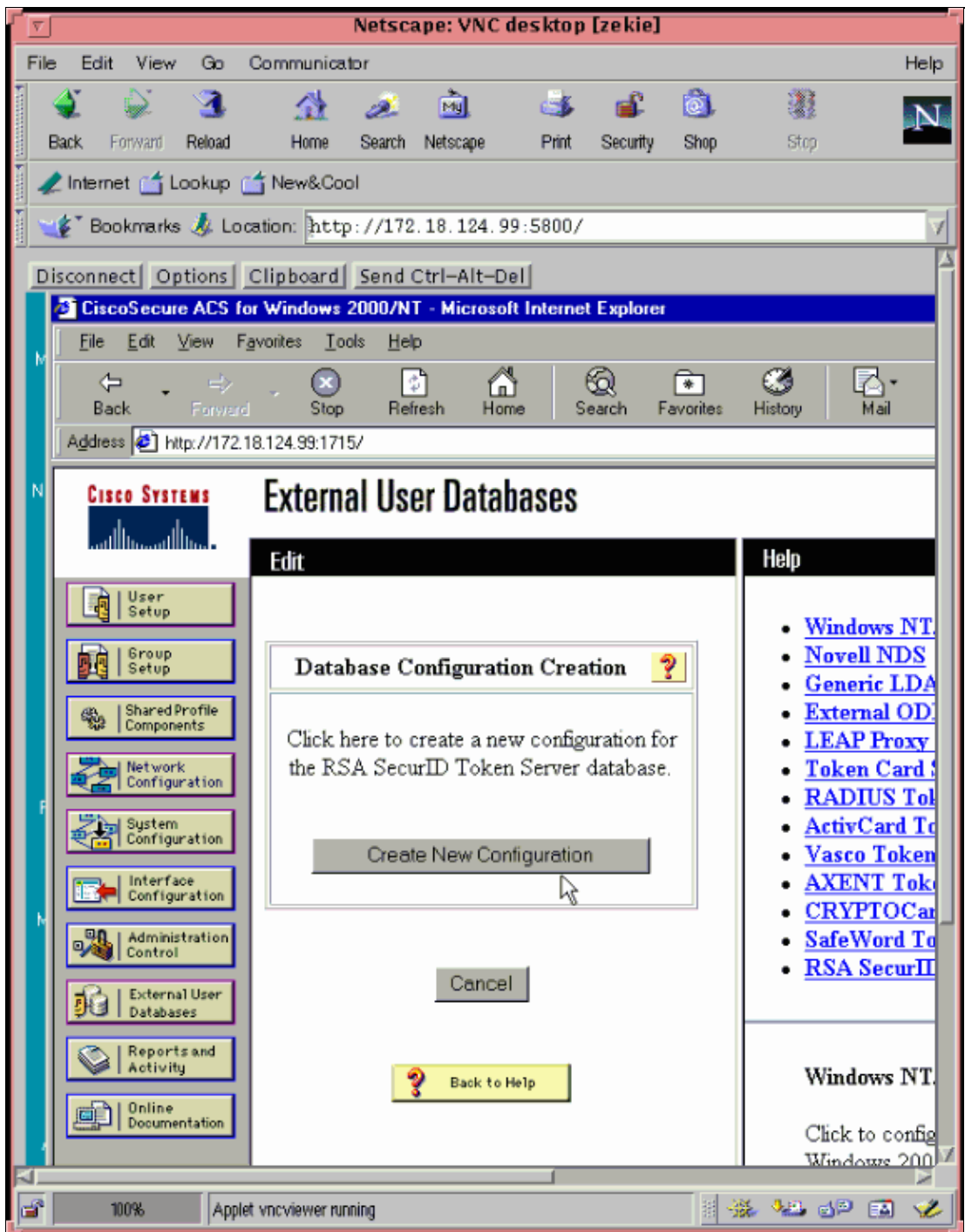
1. From the Cisco Secure ACS for Windows 2000/NT web site, select **External User Databases**.
2. From the External User Database configuration list, choose **RSA SecurID Token Server**.



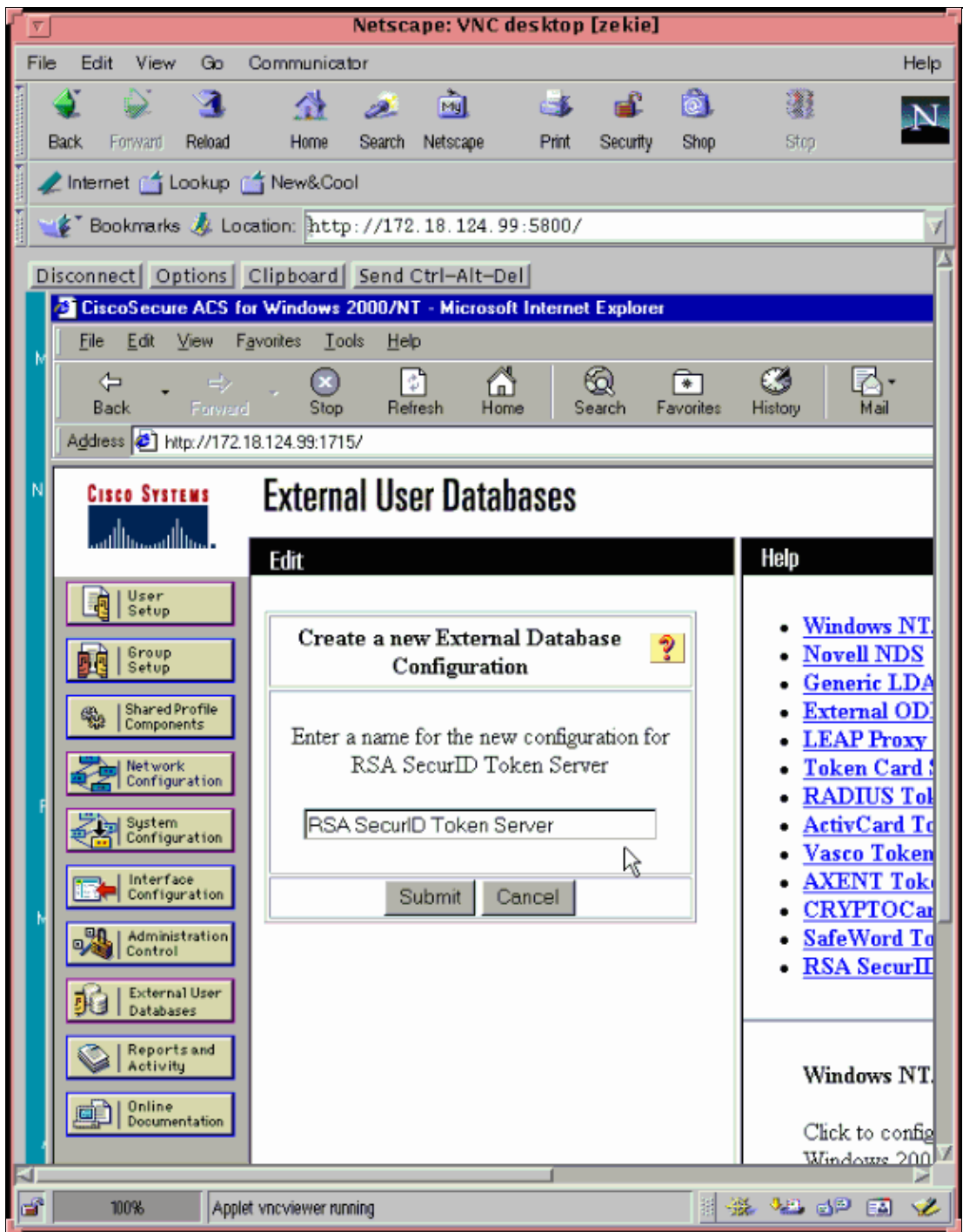
3. Choose **Configure** when prompted to choose what to do with the RSA SecurID Token Server database.



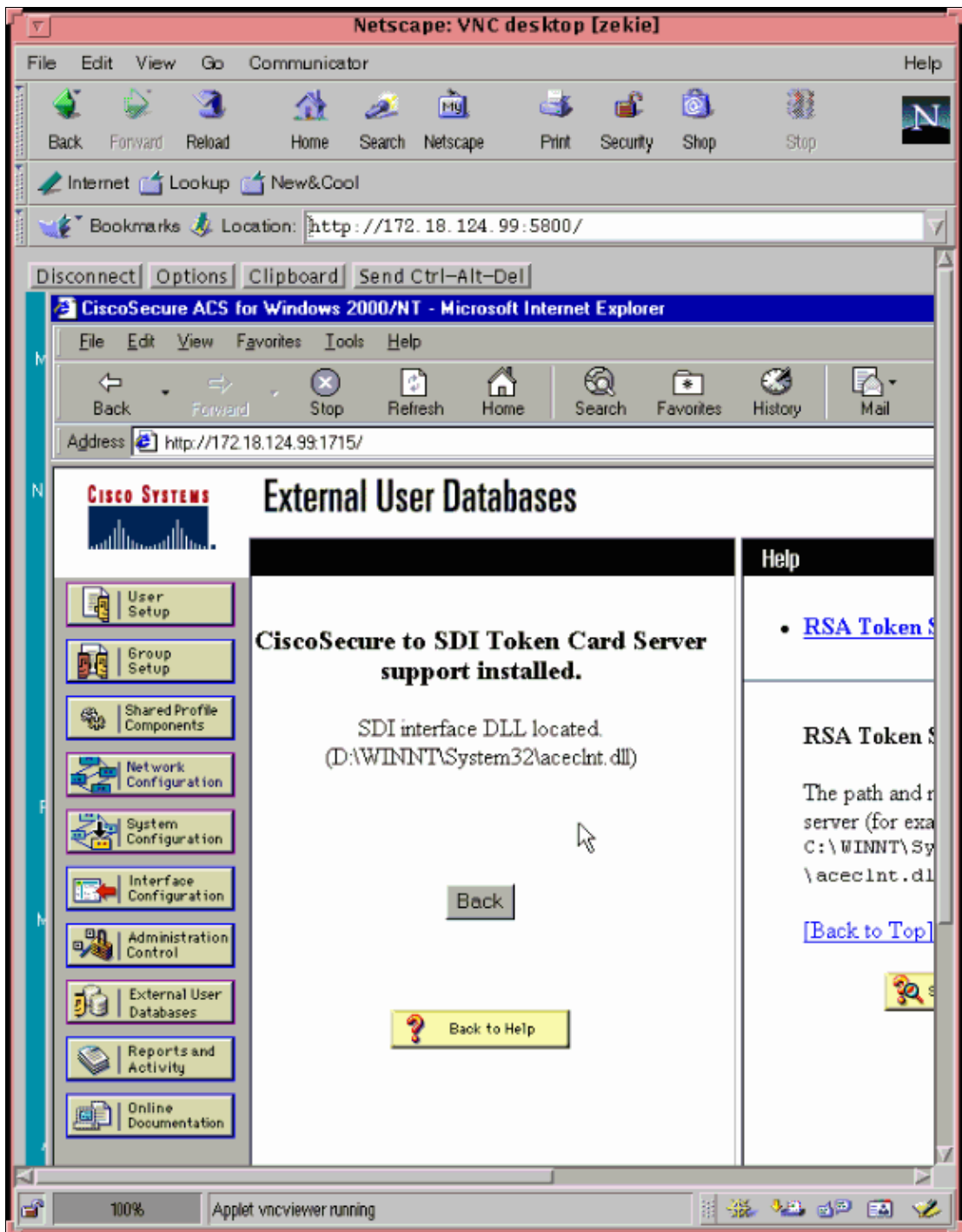
4. Click **Create New Configuration**.



5. When prompted, enter a name for the new configuration, then click **Submit**.

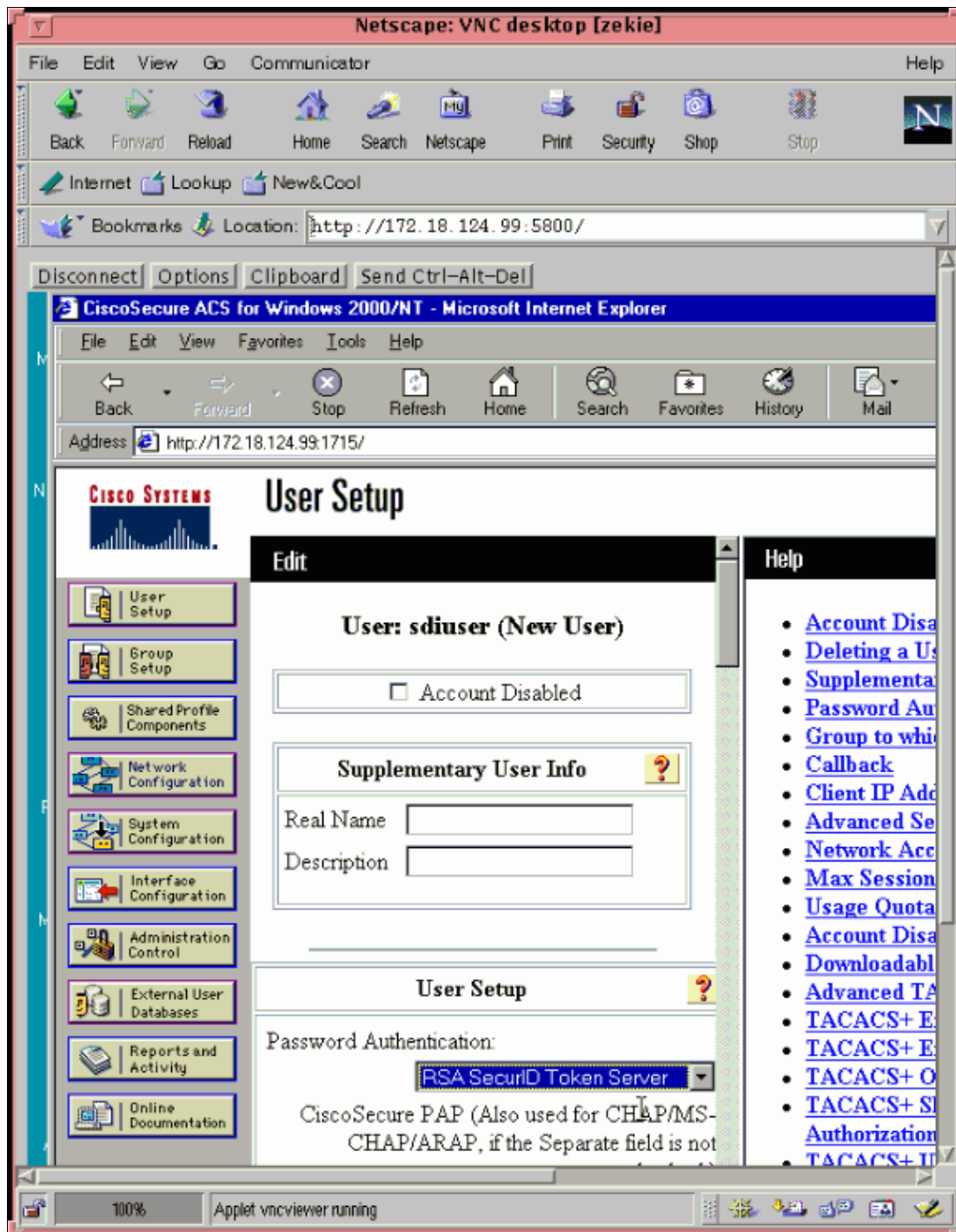


The system finds the ACE dynamic link library (DLL) and displays the message "Cisco Secure to SDI Token Card Server support installed".



Configure an ACS User for ACE Authentication

Since your ACE database already has an ACE named `sdiuser`, also name the ACS user '`sdiuser`' and tell ACS to use RSA SecurID Token Server for the Password Authentication. Put the user in an ACS group that has working users to inherit authorization permissions. For example:



Test the ACS Communication with ACE and a Network Device for Telnet

Confirm that you are able to Telnet to the network device without ACE, but with the use of ACS. Next, Telnet to the device with the new ACS/ACE user. If this is unsuccessful, refer to the Troubleshoot section of this document.

Test the ACS Communication with ACE and a Network Device for Dial (Optional)

After you confirm that you are able to Telnet to the network device with ACS/ACE and dial to the network device with ACS, test the router configuration with ACS/ACE for dial.

The router configuration needs to contain some variation of one of these commands:

```
aaa authentication ppp default

!--- Under the dial interface:

async mode

!--- Under the dial interface:

ppp authentication
```

Consider this information for authentication with ACE:

- If the **async mode interactive** command is configured with the **aaa authentication ppp default** *<method / group tacacs / group radius>* command, the router does a login authentication, then attempts a Point-to-Point (PPP) authentication re-using the same token. The second authentication fails because of the attempt to re-use the token too quickly.
- If the **async mode dedicated** command is configured, there is no facility for users to see the new Pin messages if the ACE server asks for a new Pin. You can decrease the chances of this happening when you deselect **Allowed to create a PIN and Required to create a PIN** in the ACE user interface.
- Challenge Handshake Authentication Protocol (CHAP) cannot be used with the ACE tokens alone because of the requirement CHAP RFC (1994) that states:

- ◆ CHAP requires that the secret be available in plaintext form. Irreversibly encrypted password databases commonly available cannot be used.

This precludes use of the ACE tokens for straight CHAP unless there is a separate CHAP password. For instance:

```
username: username*token
password: chap_password
```

Password Authentication Protocol (PAP) is a better choice here.

For these reasons, ensure that the router configuration has:

```
aaa authentication ppp default if-needed tacacs+|radius

!--- Under the dial interface:

async mode interactive

!--- Under the dial interface:

ppp authentication pap
```

Make sure that non-ACE ACS dial users still work after you make any configuration changes, then test with ACS ACE dial users. ACS ACE dial users need to be able to connect in these ways:

- Bring up Dial-up Networking (DUN) and connect to the device screen. In order to do this, type in the username in the Username field and the token (code+card) in the Password field.
- Bring up DUN and connect to the device screen. In order to do this, type **username*token(code+card)** in the Username field and leave the Password field blank.
- Configure DUN to bring up a terminal window after you dial and type in the username and token (code+card) when prompted by the router. The configuration of the **autocommand ppp default**

command on the line needs to start the PPP session afterwards.

If this does not work, see the Troubleshoot section of this document.

Verify

See the Test the ACS Communication with ACE and a Network Device for Dial (Optional) section of this document for verification information.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

The ACE log displays the message "Passcode accepted", but the user still fails.

- Check the ACS Failed Attempts log to determine the cause of the problem. The failure can be due to authorization issues.

The ACE log displays the message "Access Denied, passcode incorrect".

- This is an ACE problem with the passcode. During this time, the ACS Failed Attempts log shows either the message "External DB auth failed" or "External DB user invalid or bad password".

The ACE log displays the message "User not in database".

- Check the ACE database. During this time, the ACS Failed Attempts log shows either the message "External DB auth failed" or "External DB user invalid or bad password".

The ACE log displays the message "User not on agent host".

- This is an ACE configuration problem. In order to solve this problem, configure the user on the agent host.

The ACS log displays the message "External database not operational".

- If the ACE log does not show any attempts, confirm operation with the ACE client test authentication and check to be sure that the ACE/server authentication engine run.

The ACS log displays the message "CS user unknown" or "Cached token rejected/expired" with nothing in the ACE log.

- If the network device sends a CHAP request and the ACS does not have an enumerated ACE user with a separate CHAP password, ACS does not send the user to ACE because token-only authentication requires PAP.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands.

- **debug tacacs** Displays information associated with TACACS+.

- **debug radius** Displays information associated with RADIUS.
- **debug aaa authentication** Displays information on authentication, authorization, and accounting (AAA) and TACACS+ authentication.
- **debug aaa authorization** Displays information on AAA and TACACS+ authorization.
- **debug ppp negotiation** Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.

Related Information

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

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 02, 2006

Document ID: 20713
