CHAPTER 5

Managing Authentication

This chapter explains these subjects and tasks:

SDI Token (SoftID) Integration

Cisco AnyConnect VPN Client, Release 2.1 and higher, integrates support for RSA SecurID client software running on Windows XP. This support allows IT administrators to make strong authentication a convenient part of doing business. RSA SecurID software authenticators reduce the number of items a user has to manage for safe and secure access to corporate assets. RSA SecurID Software Tokens residing on a remote device generate a random, one-time-use passcode that changes every 60 seconds. The term SDI stands for Security Dynamics, Inc. technology, which refers to this one-time password generation technology that uses hardware and software tokens.

Note The AnyConnect client is compatible with RSA SecurID software versions 1.1 and higher. At the time of this release, RSA SecurID Software Token client software does not support Windows Vista and 64-bit systems. In addition, the AnyConnect client does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the AnyConnect client uses the default selected via the RSA SecurID Software Token GUI.

Comparing Native SDI with RADIUS SDI

The network administrator can configure the secure gateway to allow SDI authentication in either of the following modes:

- *Native SDI* refers to the native ability in the secure gateway to communicate directly with the SDI server for handling SDI authentication.
- *RADIUS SDI* refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

In Release 2.1 and higher, except for one case, described later, Native SDI and RADIUS SDI appear identical to the remote user. Because the SDI messages are configurable on the SDI server, the message text (see on page 5-9) on the security appliance must match the message text on the SDI server. Otherwise, the prompts displayed to the remote client user might not be appropriate for the action required during authentication. The AnyConnect client might fail to respond and authentication might fail.

RADIUS SDI challenges, with minor exceptions, essentially mirror native SDI exchanges. Since both ultimately communicate with the SDI server, the information needed from the client and the order in which that information is requested is the same. Except where noted, the remainder of this section deals with native SDI.

When a remote user using RADIUS SDI authentication connects to the security appliance with the AnyConnect VPN client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

For more information about configuring the ASA to ensure AnyConnect client compatibility, see Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client, page 5-6.

Using SDI Authentication

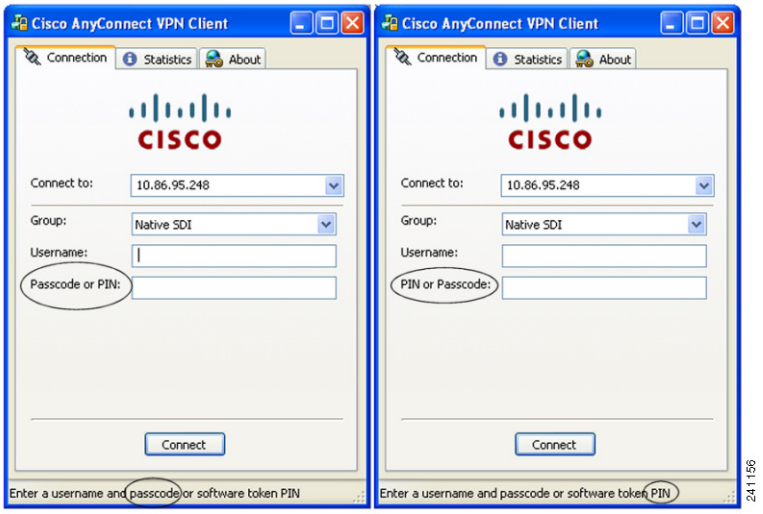
The login (challenge) dialog box matches the type of authentication configured for the tunnel group to which the user belongs. The input fields of the login dialog box clearly indicate what kind of input is required for authentication. Users who rely on username/password authentication see a dialog box like that in Figure 5-1.

Figure 5-1 Username/Password Authentication Login Dialog Box

For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect client software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, RSA Authentication Manager validates the passcode and allows the user to gain access.

Users who use RSA SecurID hardware or software tokens see input fields indicating whether the user should enter a passcode or a PIN, and the status line at the bottom of the dialog box provides further information about the requirements. The user enters a software token PIN or passcode directly into the AnyConnect user interface. See Figure 5-2 on page 5-3.

Figure 5-2 PIN and Passcode Dialog Boxes



The appearance of the initial login dialog box depends on the secure gateway settings: the user can access the secure gateway either through the main login page, the main index URL, or through a tunnel-group login page, a tunnel group URL (URL/tunnel-group). To access the secure gateway via the main login page, the “Allow user to select connection” check box must be set in the secure gateway SSL VPN Connection Profiles. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down box in which the user selects a tunnel group; the tunnel-group login page does not, since the tunnel-group is specified in the URL.

In the case of a main login page (with a drop-down tunnel-group list), the authentication type of the default tunnel group determines the initial setting for the password input field label. For example, if the default tunnel group uses SDI authentication, the field label is “Passcode”; but if the default tunnel group uses NTLM authentication, the field label is “Password”. In Release 2.1 and higher, the field label is not dynamically updated with the user selection of a different tunnel group. For a tunnel-group login page, the field label matches the tunnel-group requirements.

The client supports input of RSA SecurID Software Token PINs in the password input field. If the RSA SecurID Software Token software is installed and the tunnel-group authentication type is SDI, the field label is “Passcode” and the status bar states “Enter a username and passcode or software token PIN.” If a PIN is used, subsequent consecutive logins for the same tunnel group and username have the field label “PIN”. The client retrieves the passcode from the RSA SecurID Software Token DLL using the entered PIN. With each successful authentication, the client saves the tunnel group, the username, and authentication type, and the saved tunnel group becomes the new default tunnel group.

The AnyConnect client accepts passcodes for any SDI authentication. Even when the password input label is “PIN”, the user may still enter a passcode as instructed by the status bar. The client sends the passcode to the secure gateway as is. If a passcode is used, subsequent consecutive logins for the same tunnel group and username have the field label “Passcode”.

Categories of SDI Authentication Exchanges

All SDI authentication exchanges fall into one of the following categories:

- Normal SDI Authentication Login
- Normal login challenge
- New user mode
- New PIN mode
- Clear PIN mode
- Next Token Code mode

Normal SDI Authentication Login

A normal login challenge is always the first challenge. The SDI authentication user must provide a user name and token passcode (or PIN, in the case of a software token) in the username and passcode or PIN fields, respectively. The client returns the information to the secure gateway (central-site device), and the secure gateway verifies the authentication with the authentication server (SDI or SDI via RADIUS proxy).

If the authentication server accepts the authentication request, the secure gateway sends a success page back to the client, and the authentication exchange is complete.

If the passcode is not accepted, the authentication fails, and the secure gateway sends a new login challenge page, along with an error message. If the passcode failure threshold on the SDI server has been reached, then the SDI server places the token into next token code mode. See “Next Passcode” and “Next Token Code” Challenges, page 5-6.

New User, Clear PIN, and New PIN Modes

The PIN can be cleared only on the SDI server and only by the network administrator.

In the New User, Clear PIN, and New PIN modes, the AnyConnect client caches the user-created PIN or system-assigned PIN for later use in the “next passcode” login challenge.

Clear PIN mode and New User mode are identical from the point of view of the remote user and are both treated the same by the secure gateway. In both cases, the remote user either must enter a new PIN or be assigned a new PIN by the SDI server. The only difference is in the user response to the initial challenge.

For New PIN mode, the existing PIN is used to generate the passcode, as it would be in any normal challenge. For Clear PIN mode, no PIN is used at all for hardware tokens, with the user entering just a token code. A PIN Of eight consecutive zeros, “00000000”, is used to generate a passcode for RSA software tokens. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Adding a new user to an SDI server has the same result as clearing the PIN of an existing user. In both cases, the user must either provide a new PIN or be assigned a new PIN by the SDI server. In these modes, for hardware tokens, the user enters just a token code from the RSA device. In either case, the SDI server administrator must inform the user of what, if any, PIN value to use.

Getting a New PIN

If there is no current PIN, the SDI server requires that one of the following conditions be met, depending on how the system is configured:

- The user can choose whether to create a PIN or have the system assign it.
- The user must create a new PIN.
- The system must assign a new PIN to the user.

By default, the system simply assigns a PIN. If the SDI server is configured to allow the remote user to choose whether to create a PIN or have the system assign a PIN, the login screen presents a drop-down menu showing the options. The status line provides a prompt message. In either case, the user must remember the new PIN for future login authentications.

Creating a New PIN

If the user chooses to create a new PIN and clicks Continue, the AnyConnect client presents a dialog box on which to enter that PIN (Figure 5-3 on page 5-5). The PIN must be a number from 4 to 8 digits long.

Figure 5-3 Creating a New PIN

For a user-created PIN, after entering and confirming the new PIN, the user clicks Continue. Because the PIN is a type of password, anything the user enters into these input fields is displayed as asterisks. With RADIUS proxy, the PIN confirmation is a separate challenge, subsequent to the original dialog box. The client sends the new PIN to the secure gateway, and the secure gateway continues with a “next passcode” challenge.

For a system-assigned PIN, if the SDI server accepts the passcode that the user enters on the login page, then the secure gateway sends the client the system-assigned PIN. The user must click Continue. The client sends a response back to the secure gateway, indicating that the user has seen the new PIN, and the system continues with a "next passcode' challenge.

In both cases, the user must remember the PIN for subsequent login authentications.

"Next Passcode" and "Next Token Code" Challenges

For a "next passcode" challenge, the client uses the PIN value cached during the creation or assignment of a new PIN to retrieve the next passcode from the RSA SecurID Software Token DLL and return it to the secure gateway without prompting the user. Similarly, in the case of a "next Token Code" challenge for a software token, the client retrieves the next Token Code from the RSA SecurID Software Token DLL.

Ensuring RADIUS/SDI Proxy Compatibility with the AnyConnect Client

This section describes procedures to ensure that the AnyConnect client using RSA SecureID Software tokens can properly respond to user prompts delivered to the client through a RADIUS server proxying to an SDI server or servers. This section contains the following topics:

- AnyConnect Client and RADIUS/SDI Server Interaction
- Configuring the Security Appliance to Support RADIUS/SDI Messages

AnyConnect Client and RADIUS/SDI Server Interaction

When a remote user connects to the security appliance with the AnyConnect client and attempts to authenticate using an RSA SecurID token, the security appliance communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

During authentication, the RADIUS server presents access challenge messages to the security appliance. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the security appliance is communicating directly with an SDI server from when communicating through the RADIUS proxy. Therefore, in order to appear as a native SDI server to the AnyConnect client, the security appliance must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the security appliance must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The AnyConnect client might fail to respond and authentication might fail.

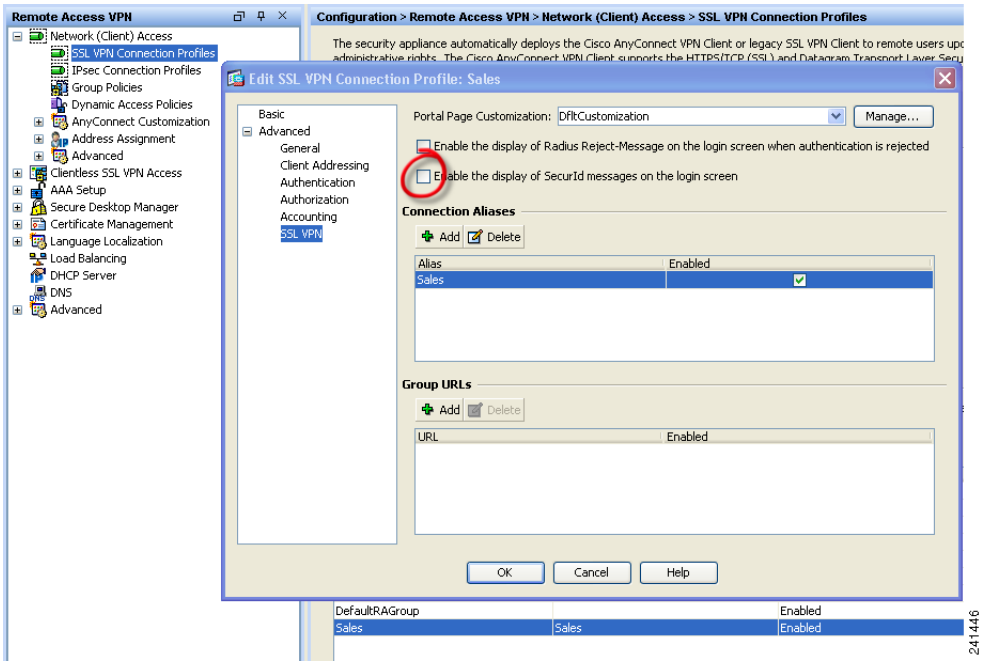
Configuring the Security Appliance to Support RADIUS/SDI Messages

The following section describes the steps to configure the security appliance to interpret SDI-specific RADIUS reply messages and prompt the AnyConnect user for the appropriate action.

Configure a connection profile (tunnel group) to forward RADIUS reply messages in a manner that simulates direct communication with an SDI server. Users authenticating to the SDI server must connect over this connection profile.

Step 1 Go to Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles. The Edit SSL VPN Connection Profile window displays (Figure 5-4).

Figure 5-4 Edit SSL VPN Connection Profile Screen

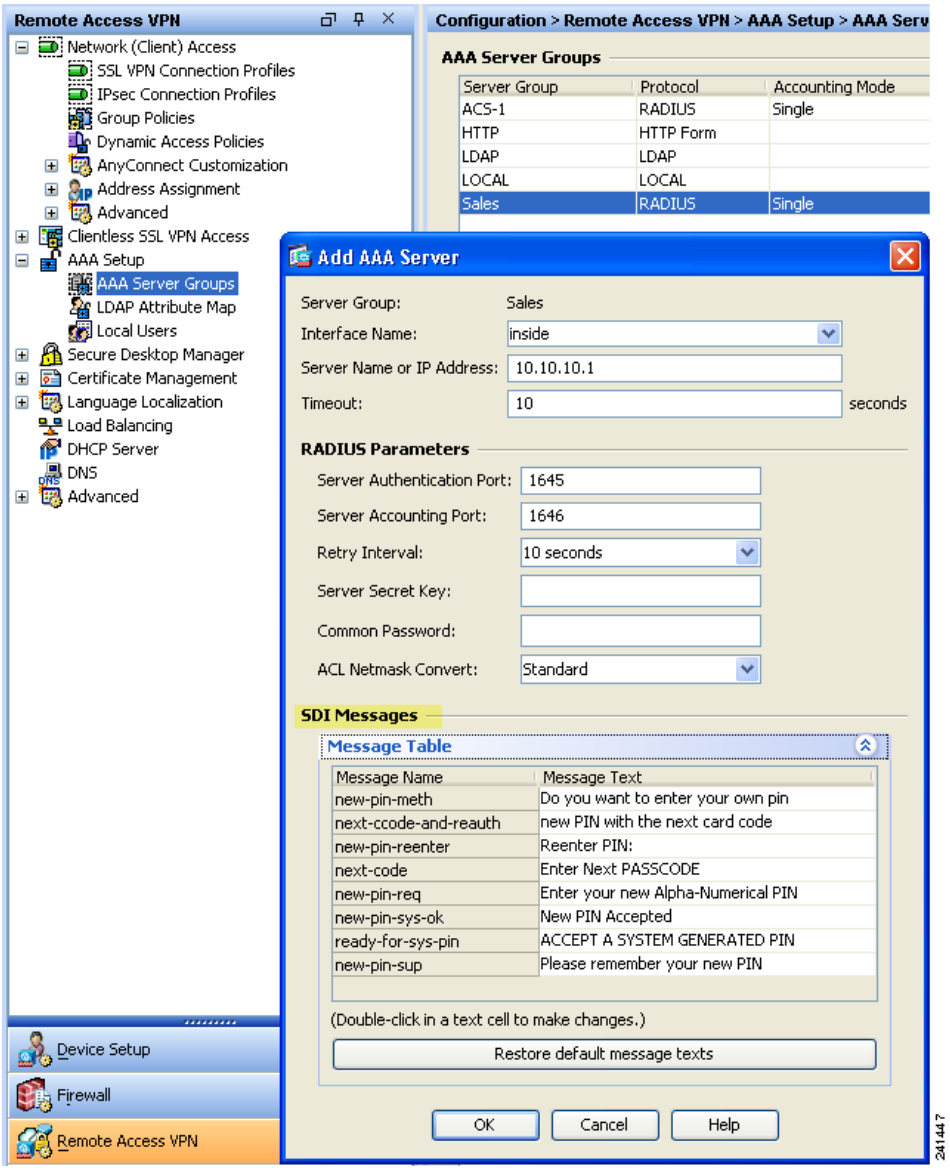


Step 2 Check **Enable the display of SecurID messages on the login screen**.

Step 3 Choose Configuration > Remote Access VPN > AAA Server Groups.

The Add AAA Server window opens (Figure 5-5).

Figure 5-5 Configuring RADIUS SDI Messages



Step 4 In the SDI Messages area, click Message Table to expand the table and view the messages. Double-click a message text field to edit the message. Configure the RADIUS reply message text on the security appliance to match (in whole or in part) the message text sent by the RADIUS server.

The default message text used by the security appliance is the default message text used by Cisco Secure Access Control Server (ACS). If you are using Cisco Secure ACS, and it is using the default message text, you do not need to configure the message text on the security appliance. Otherwise, configure the messages to ensure the message text matches.

Table 5-1 shows the message code, the default RADIUS reply message text, and the function of each message. Because the security appliance searches for strings in the order in which they appear in the table, you must ensure that the string you use for the message text is not a subset of another string.

For example, “new PIN” is a subset of the default message text for both new-pin-sup and next-ccode-and-reauth. If you configure new-pin-sup as “new PIN”, when the security appliance receives “new PIN with the next card code” from the RADIUS server, it will match the text to the new-pin-sup code instead of the next-ccode-and-reauth code.

Table 5-1 SDI Opcodes, Default Message Text, and Message Function

Message Code	Default RADIUS Reply Message Text	Function
next-code	Enter Next PASSCODE	Indicates the user must enter the NEXT tokencode without the PIN.
new-pin-sup	Please remember your new PIN	Indicates the new system PIN has been supplied and displays that PIN for the user.
new-pin-meth	Do you want to enter your own pin	Requests from the user which new PIN method to use to create a new PIN.
new-pin-req	Enter your new Alpha-Numerical PIN	Indicates a user-generated PIN and requests that the user enter the PIN.
new-pin-reenter	Reenter PIN:	Used internally by the security appliance for user-supplied PIN confirmation. The client confirms the PIN without prompting the user.
new-pin-sys-ok	New PIN Accepted	Indicates the user-supplied PIN was accepted.
next-ccode-and-reauth	new PIN with the next card code	Follows a PIN operation and indicates the user must wait for the next tokencode and to enter both the new PIN and next tokencode to authenticate.
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN	Used internally by the security appliance to indicate the user is ready for the system-generated PIN.