CHAPTER 10

Managing VPN Authentication

This chapter explains how to manage VPN authentication for users using the Cisco AnyConnect Secure Mobility client, and includes these subjects and tasks:

Server Certificate Verification

The following verifications are applied to received server certificates:

- SSL and IPSec connections from the AnyConnect client to the secure gateway being performed using the FQDN of the secure gateway will no longer make a secondary server certificate verification with the FQDN's resolved IP address for name verification, if the initial verification using the FQDN fails.
- SSL and IPSec connections from the AnyConnect client to the secure gateway require server certificates to contain Key Usage attributes of Digital Signature and Key Encipherment.
- SSL connections from the AnyConnect client to the secure gateway require server certificates to contain an Enhanced Key Usage attribute of Server Authentication.
- IPSec connections from the AnyConnect client to the secure gateway require server certificates to contain an Enhanced Key Usage attribute of Server Authentication or IKE Intermediate.

Note Note that server certificates not containing a Key Usage will be considered invalid for all Key Usages, and similarly server certificates not containing an Enhanced Key Usage will be considered invalid for all Enhanced Key Usages.

- In this release of AnyConnect, IPSec connections from the AnyConnect client to the secure gateway now perform name verification on server certificates. The following rules will be applied for the purposes of both IPSec and SSL name verification:
  - If a Subject Alternative Name extension is present with relevant attributes, name verification will be performed solely against the Subject Alternative Name. Relevant attributes include DNS Name attributes for all certificates, and additionally include IP address attributes if the connection is being performed to an IP address.
  - If a Subject Alternative Name extension is not present, or is present but contains no relevant attributes, name verification will be performed against any Common Name attributes found in the Subject of the certificate.
  - If a certificate uses a wildcard for the purposes of name verification, the wildcard must be in the first (left-most) subdomain only, and additionally must be the last (right-most) character in the subdomain. Any wildcard entry not in compliance will be ignored for the purposes of name verification.

Configuring Certificate-only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password.

You can configure certificate-only authentication in connection profiles. To enable this setting, follow this procedure:

Step 1 Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. Select a connection profile and click **Edit**. The Edit AnyConnect Connection Profile window opens.

Step 2 If it is not already, click the **Basic** node of the navigation tree on the left pane of the window. In the right pane of the window, in the **Authentication** area, enable the method **Certificate**.

Step 3 Click **OK**.

Step 4 (Optional) You can specify which certificates, if any, you want to use for SSL authentication on each interface. If you do not specify a certificate for a particular interface, the fallback certificate will be used.

To do this, go to **Configuration > Remote Access VPN > AnyConnect Connection Profiles**. In the **Access Interfaces** area in the right pane, select the interface for which you want to specify a certificate, and then click **Device Certificate**.

Step 5 In the Specify Device Certificate dialog, click the **Device Certificate** field to choose a certificate or click **Manage** to add a certificate you want to use for authentication connections to the interface you have chosen.

Step 6 Click **OK** and apply your changes.

Note

- To configure in which certificate store the AnyConnect client searches for the authentication certificate, see the"Configuring a Certificate Store" section on page 3-42. You will also find information on configuring certificate restrictions for Linux and Mac OS X operating systems.

- The certificate used to authenticate the client to the secure gateway must be valid and trusted (signed by a CA). A self-signed client certificate will not be accepted.

AnyConnect Smart Card Support

AnyConnect supports smart cards in the following environments:

- Microsoft CAPI 1.0 and CAPI 2.0 on Windows XP, 7 & Vista
- Keychain via Tokend on Mac OS X, 10.4 and higher

Note AnyConnect does not support Smart cards on Linux or PKCS #11 devices

Avoiding SHA 2 Certificate Validation Failure

The AnyConnect client relies on the Windows Cryptographic Service Provider (CSP) of the certificate for hashing and signing of data required during the IKEv2 authentication phase of the IPsec/IKEv2 VPN connection. If the CSP does not support SHA 2 algorithms, and the ASA is configured for the pseudo-random function (PRF) SHA256, SHA384, or SHA512, and the connection profile (tunnel-group) is configured for certificate, or certificate *and* AAA authentication, certificate authentication fails. The user receives the message *Certificate Validation Failure*.

This failure occurs for Windows only, for certificates that belong to CSPs that do not support SHA 2-type algorithms. Other supported OSs do not experience this problem.

To avoid this problem you can configure the PRF in the IKEv2 policy on the ASA to **md5** or **sha** (SHA 1).

Alternatively, you can modify the certificate CSP value for native CSPs that we know work:

- For Windows XP—Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
- For Windows 7 and Vista—Microsoft Enhanced RSA and AES Cryptographic Provider

Caution Do not apply this workaround to SmartCards certificates. The CSP names must not be changed. Instead, contact the SmartCard provider for an updated CSP that supports SHA 2 algorithms.

Caution Performing the following workaround actions could corrupt the user certificate if you perform them incorrectly. Use extra caution when specifying changes to the certificate.

You can use the Microsoft Certutil.exe utility to modify the certificate CSP values. Certutil is a command-line utility for managing a Windows CA, and is available in the Microsoft Windows Server 2003 Administration Tools Pack. You can download the Tools Pack at this URL:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

Follow this procedure to run Certutil.exe and change the Certificate CSP values:

Step 1 Open a command window on the endpoint computer.

Step 2 View the certificates in the user store along with their current CSP value using the following command:

```
certutil -store -user My
```

The following example shows the certificate contents displayed by this command:

```
================ Certificate 0 ================
Serial Number: 3b3be91200020000854b
Issuer: CN=cert-issuer, OU=Boston Sales, O=Example Company, L=San Jose,
S=CA, C=US, E=csmith@example.com
NotBefore: 2/16/2011 10:18 AM
NotAfter: 5/20/2024 8:34 AM
Subject: CN=Carol Smith, OU=Sales Department, O=Example Company, L=San Jose, S=C
A, C=US, E=csmith@example.com
Non-root Certificate
Template:
Cert Hash(sha1): 86 27 37 1b e6 77 5f aa 8e ad e6 20 a3 14 73 b4 ee 7f 89 26
  Key Container = {F62E9BE8-B32F-4700-9199-67CCC86455FB}
  Unique container name: 46ab1403b52c6305cb226edd5276360f_c50140b9-ffef-4600-ada
6-d09eb97a30f1
  Provider = Microsoft Enhanced RSA and AES Cryptographic Provider
Signature test passed
```

Step 3 Identify the <CN> attribute in the certificate. In the example, the CN is *Carol Smith*. You need this information for the next step.

Step 4 Modify the certificate CSP using the following command. The example below uses the subject <CN> value to select the certificate to modify. You can also use other attributes.

On Windows Vista and Windows 7, use this command:

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider" -f -repairstore
-user My <CN> carol smith
```

On Windows XP, use this command:

```
certutil -csp "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)" -f
-repairstore -user My <CN> carol smith
```

Step 5 Repeat step 2 and verify the new CSP value appears for the certificate.

SDI Token (SoftID) Integration

AnyConnect integrates support for RSA SecurID client software versions 1.1 and later running on Windows 7 x86 (32-bit) and x64 (64-bit), Vista x86 and x64, and XP x86.

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.

The RSASecureIDIntegration profile setting has three possible values:

- Automatic—The client first attempts one method, and if it fails, the other method is tried. The default is to treat the user input as a token passcode (HardwareToken), and if that fails, treat it as a software token pin (SoftwareToken). When authentication is successful, the successful method is set

as the new SDI Token Type and cached in the user preferences file. For the next authentication attempt, the SDI Token Type defines which method is attempted first. Generally, the token used for the current authentication attempt is the same token used in the last successful authentication attempt. However, when the username or group selection is changed, it reverts to attempting the default method first, as shown in the input field label.

Note The SDI Token Type only has meaning for the automatic setting. You can ignore logs of the SKI Token Type when the authentication mode is not automatic. HardwareToken as the default avoids triggering next token mode.

- SoftwareToken—The client always interprets the user input as a software token PIN, and the input field label is “PIN:”.
- HardwareToken—The client always interprets the user input as a token passcode, and the input field label is “Passcode:”.

Note AnyConnect does not support token selection from multiple tokens imported into the RSA Software Token client software. Instead, the 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 releases 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 10-13) on the ASA 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. AnyConnect 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 ASA with AnyConnect and attempts to authenticate using an RSA SecurID token, the ASA communicates with the RADIUS server, which in turn, communicates with the SDI server about the authentication.

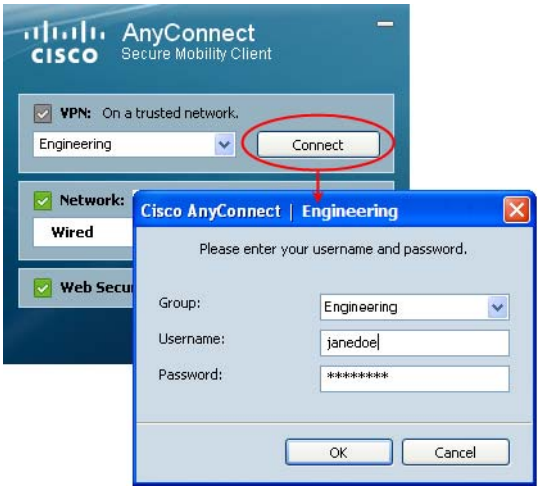
For more information about configuring the ASA to ensure AnyConnect compatibility, see the “Ensuring RADIUS/SDI Proxy Compatibility with AnyConnect” section on page 10-10.

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.

Typically, users make an AnyConnect connection by clicking the AnyConnect icon in the tools tray, selecting the connection profile with which they wish to connect, and then entering the appropriate credentials in the authentication dialog box. Users who rely on username/password authentication see a dialog box like that in Figure 10-1.

Figure 10-1 Username/Password Authentication Login Dialog Box



For SDI authentication, the remote user enters a PIN (Personal Identification Number) into the AnyConnect software interface and receives an RSA SecurID passcode. After the user enters the passcode into the secured application, the 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, a PIN, or a passcode 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 10-2, Figure 10-3, and Figure 10-4.

Figure 10-2 Passcode or Pin Dialog Box

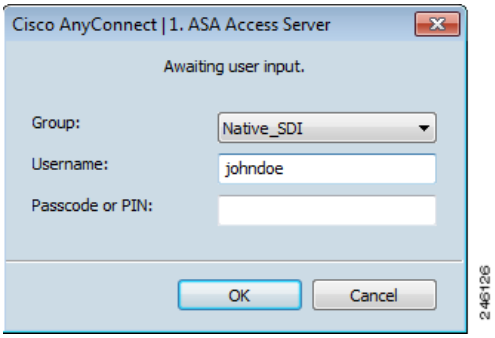


Figure 10-3 PIN Dialog Box

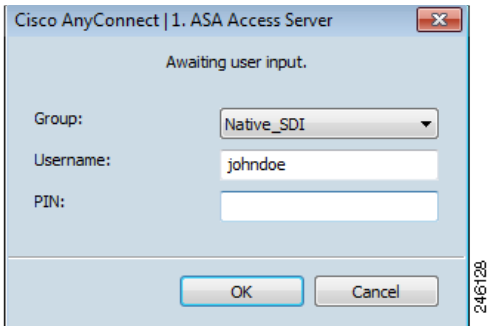
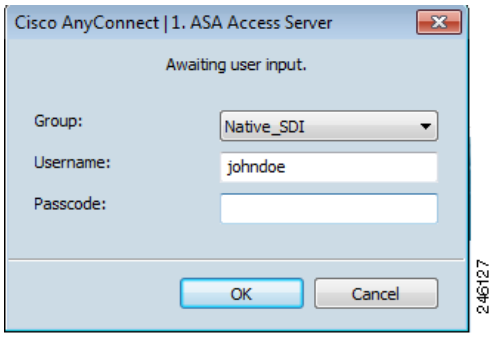


Figure 10-4 Passcode Dialog Box



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, a tunnel-group login page, or 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 Network (Client) Access AnyConnect Connection Profiles page. In either case, the secure gateway sends the client a login page. The main login page contains a drop-down list 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 list of connection profiles or tunnel groups), 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 later, 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.

AnyConnect 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 the ““Next Passcode” and “Next Token Code” Challenges” section on page 10-10.

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, AnyConnect 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 list 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** (Figure 10-5), AnyConnect presents a dialog box on which to enter that PIN (Figure 10-6). The PIN must be a number from 4 to 8 digits long.

Figure 10-5 User Choose to Create a PIN

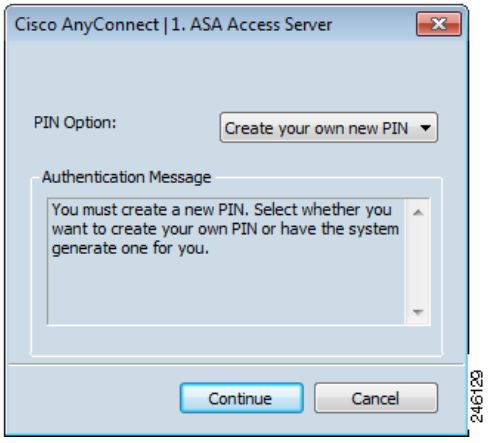
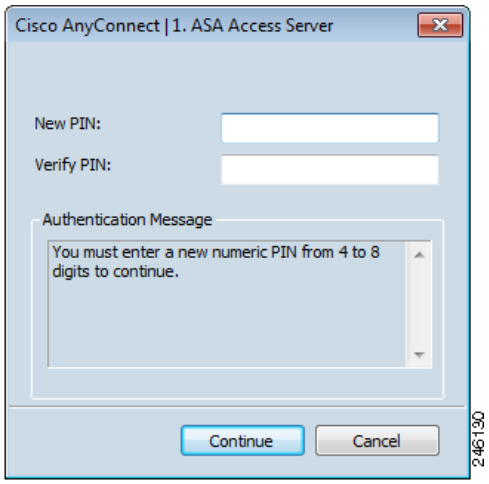


Figure 10-6 Creating a New PIN



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 AnyConnect

This section describes procedures to ensure that AnyConnect 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 and RADIUS/SDI Server Interaction
- Configuring the Security Appliance to Support RADIUS/SDI Messages

AnyConnect and RADIUS/SDI Server Interaction

When a remote user connects to the ASA with AnyConnect and attempts to authenticate using an RSA SecurID token, the ASA 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 ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA 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 AnyConnect, the ASA must interpret the messages from the RADIUS server.

Also, because the SDI messages are configurable on the SDI server, the message text on the ASA 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. AnyConnect 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 ASA 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 > AnyConnect Connection Profiles**.

Step 2 Select the connection profile you want to configure to interpret SDI-specific RADIUS reply messages and click **Edit**.

Step 3 In the **Edit AnyConnect Connection Profile** window, expand the Advanced node in the navigation pane on the left and select **Group Alias / Group URL.**

Step 4 Check **Enable the display of SecurID messages on the login screen**.

Step 5 Click **OK**.

Step 6 Choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**.

Step 7 Click **Add** to Add a AAA Server group.

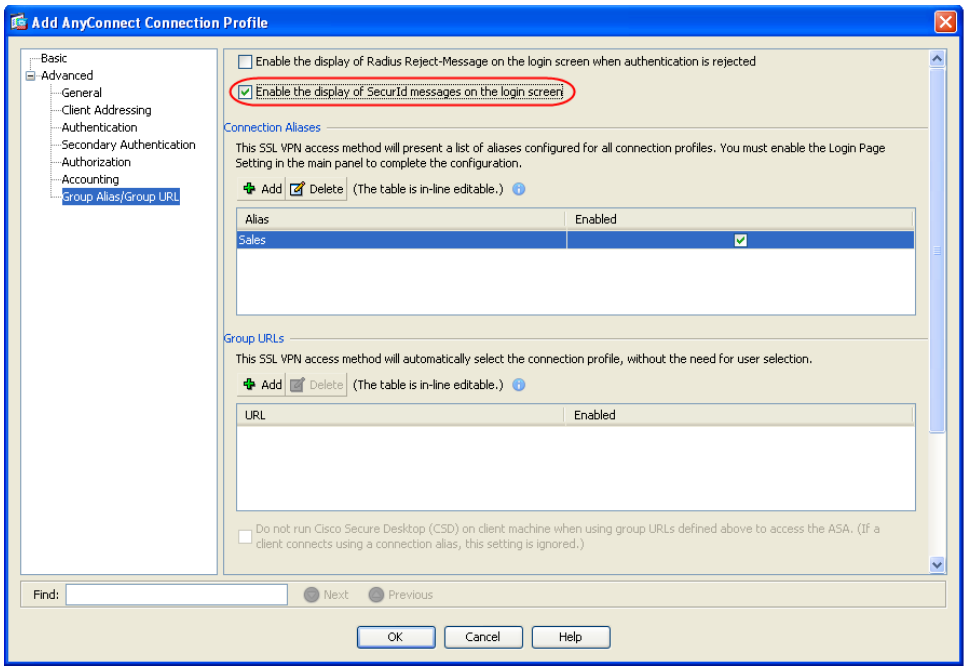
Step 8 Configure the AAA server group in the Edit AAA Server Group dialog and click **OK**.

Step 9 In the **AAA Server Groups** area, select the AAA server group you just created and then click **Add** in the **Servers in the Selected Group** area.

Step 10 In the SDI Messages area, expand the **Message Table** area. Double-click a message text field to edit the message. Configure the RADIUS reply message text on the ASA to match (in whole or in part) the message text sent by the RADIUS server.

Step 11 Click **OK**. Click **Apply**. Click **Save**.

Figure 10-7 Add/Edit AnyConnect Connection Profile Screen



The default message text used by the ASA 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 ASA. Otherwise, configure the messages to ensure the message text matches.

Table 10-1 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 10-1 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 ASA 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 ASA to indicate the user is ready for the system-generated PIN.