Two-Factor Authentication

This document describes SonicWALL's implementation of two-factor authentication for SonicWALL SSL-VPN appliances. This document contains the following sections:

Feature Overview

This section provides an introduction to two-factor authenticating. This section contains the following subsections:

What is Two-Factor Authentication?

Two-factor authentication is an authentication method that requires two independent pieces of information to establish identity and privileges. Two-factor authentication is stronger and more rigorous than traditional password authentication that only requires one factor (the user's password).

SonicWALL's implementation of two-factor authentication partners with two of the leaders in advanced user authentication: RSA and VASCO.

Benefits

Two-factor authentication offers the following benefits:

- Greatly enhances security by requiring two independent pieces of information for authentication.
- Reduces the risk posed by weak user passwords that are easily cracked.
- Minimizes the time administrators spend training and supporting users by providing a strong authentication process that is simple, intuitive, and automated.

How Does Two-Factor Authentication Work?

Two-factor authentication requires the use of a third-party authentication service. The authentication service consists of two components:

- An authentication server on which the administrator configures user names, assigns token, and manages authentication-related tasks.
- Tokens that the administrator gives to users which display temporary token codes.

Table 1 lists the currently-supported third-party authentication services.

Table 1 Supported Two-Factor Authentication Services

Company	Authentication Server	Token Service
RSA	RSA Authentication Manager	RSA SecurID tokens
VASCO	VACMAN Middleware	Digipass tokens

With two-factor authentication, users must enter a valid temporary passcode to gain access. A passcode consists of the following:

- The user's personal identification number (PIN)
- A temporary token code

Users receive the temporary token codes from their RSA or VASCO token cards. The token cards display a new temporary token code every minute. When the RSA or VASCO server authenticates the user, it verifies that the token code timestamp is current. If the PIN is correct and the token code is correct and current, the user is authenticated.

Because user authentication requires these two factors, the RSA SecurID and VASCO DIGIPASS solution offers stronger security than traditional passwords (single-factor authentication).

Platforms

Two-Factor Authentication is available on the SonicWALL SSL-VPN 2000 and 4000 platforms running firmware version 2.0.

Using Two-Factor Authentication

This section contains the following subsections:

Administrator Prerequisites

Two-factor authentication requires the use of a third-party authentication service. If you are using RSA, you must have the RSA Authentication Manager and RSA SecurID tokens. If you are using VASCO, you must have the VASCO VACMAN Middleware and Digipass tokens.

Administrator Configuration Tasks

The following sections describe how to configure two-factor authentication.

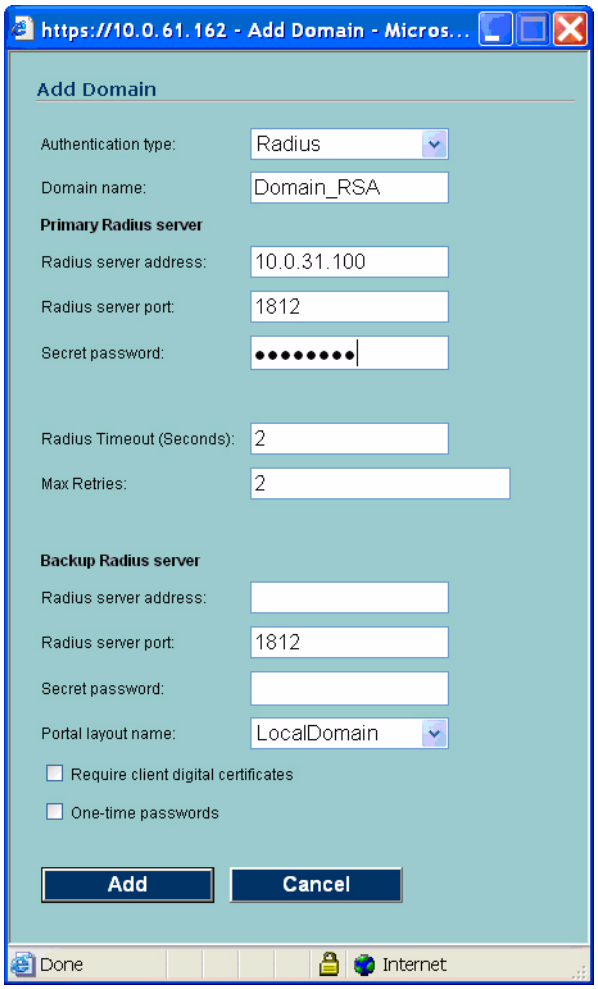
Configuring the SSL-VPN Appliance

Note Because two-factor authentication depends on time synchronization, it is import that the internal clocks for the SSL-VPN appliance and the third-party authentication server are set correctly. On the SSL-VPN appliance, set the time on the **System > Time** page.

To configure a SonicWALL SSL-VPN appliance for two-factor authentication, perform the following steps:

Step 1 On the SSL-VPN appliance, navigate to the **Portal > Domain** page.

Step 2 Click on the **Add domain** button.



Step 3 In the authentication type pulldown menu, select **Radius**.

Step 4 Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL-VPN appliance portal.

Step 5 Enter the IP address of the RADIUS server in the **Radius Server Address** field.

Step 6 Enter the Radius server port in the **Radius server port** field.

Step 7 Enter a number (in seconds) for Radius timeout in the **Radius Timeout (Seconds)** field.

Step 8 Enter the maximum number of retries in the **Max Retries** field.

Step 9 Enter the authentication secret in the **Secret Password** field.

Step 10 Click the name of the layout in the **Portal Layout Name** pull-down menu.

Step 11 Optionally check the box next to **Require client digital certificates** to require the use of client certificates for login. By checking this box, you require the client to present a client certificate for strong mutual authentication.

Step 12 Click **Add** to update the configuration. The domain will be added to the **Domain Settings** table.

Note The SonicWALL SSL-VPN appliance will attempt to authenticate against the specified RADIUS server using PAP authentication. It is generally required that the RADIUS server be configured to accept RADIUS client connections from the SonicWALL SSL-VPN appliance. Typically, these connections will appear to come from the SonicWALL SSL-VPN's X0 interface IP address. Refer to your RADIUS server documentation for configuration instructions.

Configuring the RSA Authentication Manager

The following sections describe how to configure the RSA Authentication Manager version 6.1 to perform two-factor authentication with your SonicWALL SSL-VPN appliance:

- "Adding an Agent Host Record for the SonicWALL SSL-VPN Appliance" on page 6
- "Adding the SonicWALL SSL-VPN as a RADIUS Client" on page 8
- "Setting the Time and Date" on page 8
- "Importing Tokens and Adding Users" on page 9

Note This configuration procedure is specific to RSA Authenticaiton Manager version 6.1. If you are using a different version of RSA Authentication Manager, the procedure will be slightly different.

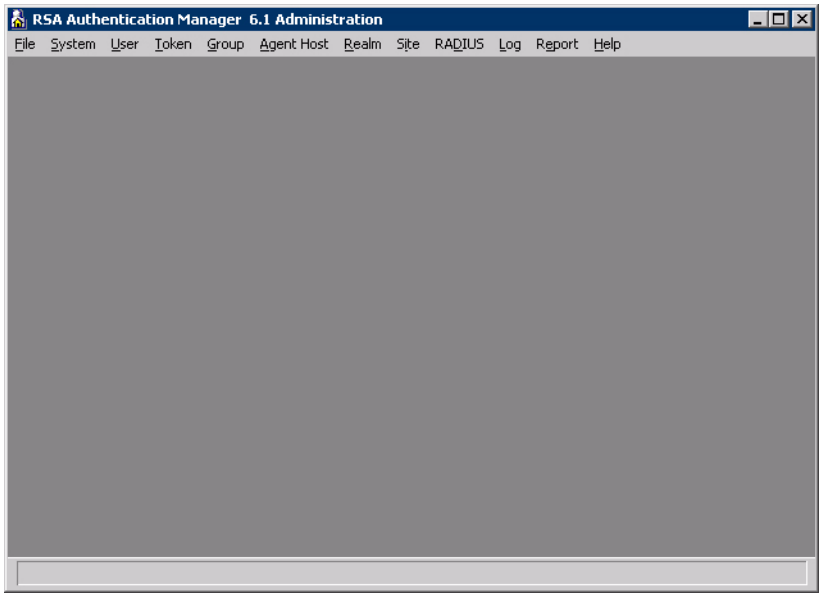
If you will be using VASCO instead of RSA, see "Configuring the VASCO VACMAN Middleware" on page 12.

Adding an Agent Host Record for the SonicWALL SSL-VPN Appliance

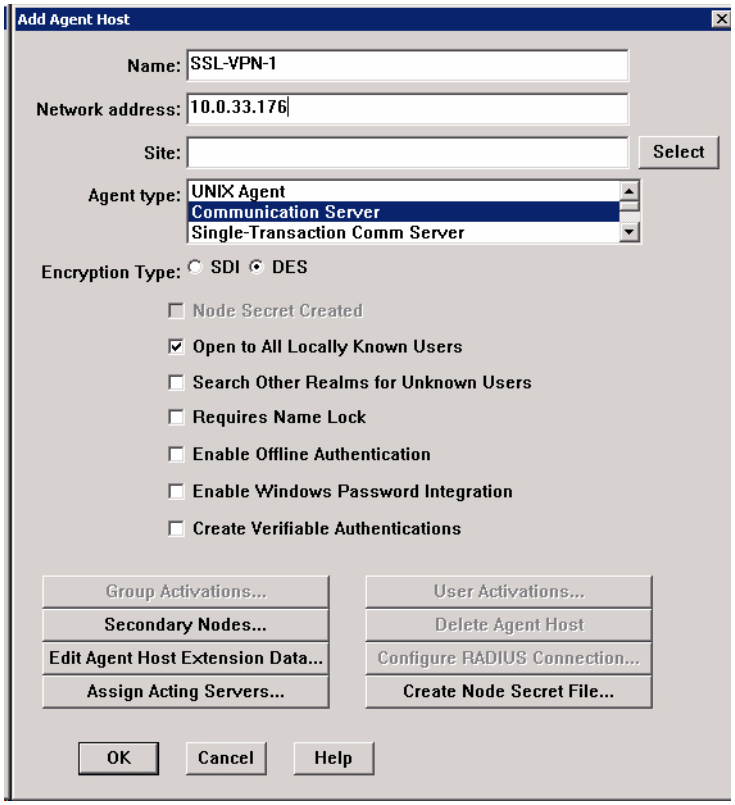
To establish a connection between the SSL-VPN appliance and the RSA Authentication Manager, an Agent Host record must be added to the RSA authentication Manger database. The Agent host record identifies the SSL-VPN appliance within its database and contains information about communication and encryption.

To create the Agent Host record for the SSL-VPN appliance, perform the following steps:

Step 1 Launch the RSA Authentication Manager.



Step 2 On the **Agent Host** menu, select **Add Agent Host**.



Step 3 Enter a hostname for the SSL-VPN appliance in the **Name** field.

Step 4 Enter the IP address of the SSL-VPN appliance in the **Network address** field.

Step 5 Select **Communication Server** in the **Agent type** window.

Step 6 By default, the **Enable Offline Authentication** and **Enable Windows Password Integration** options are enabled. SonicWALL recommends disabling all of these options except for **Open to All Locally Known Users**.

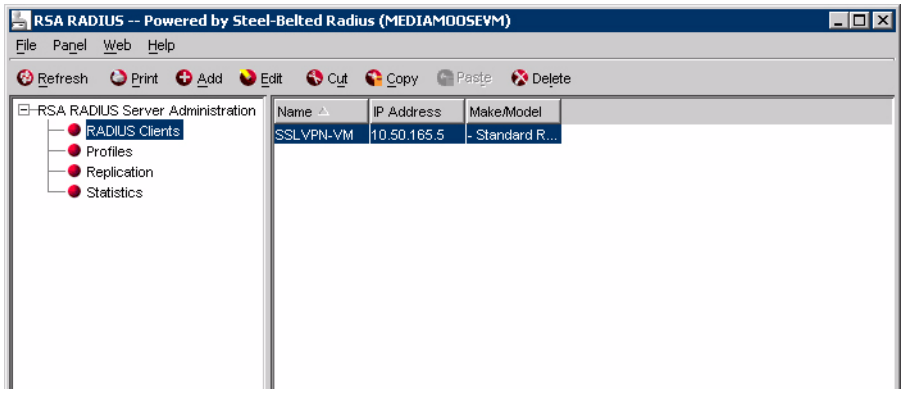
Step 7 Click **OK**.

Adding the SonicWALL SSL-VPN as a RADIUS Client

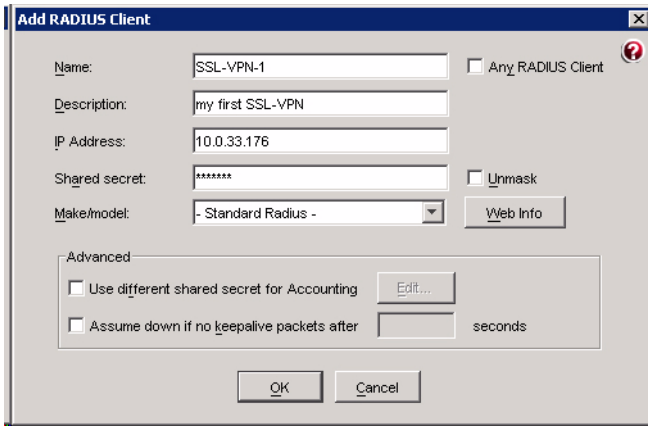
After you have created the Agent Host record, you must add the SonicWALL SSL-VPN to the RSA Authentication Manager as a RADIUS client. To do so, perform the following steps:

Step 1 In RSA Authentication Manager, go to the **RADIUS** menu and select **Manage RADIUS Server**. The RSA RADIUS Manager displays.

Step 2 Expand the **RSA RADIUS Server Administration** tree and select **RADIUS Clients**.



Step 3 Click **Add**. The **Add RADIUS Client** window displays.



Step 4 Enter a descriptive name for the SSL-VPN appliance.

Step 5 Enter the IP address of the SSL-VPN in the **IP Address** field.

Step 6 Enter the shared secret that is configured on the SSL-VPN in the **Shared secret** field.

Step 7 Click **OK** and close the RSA RADIUS Manager.

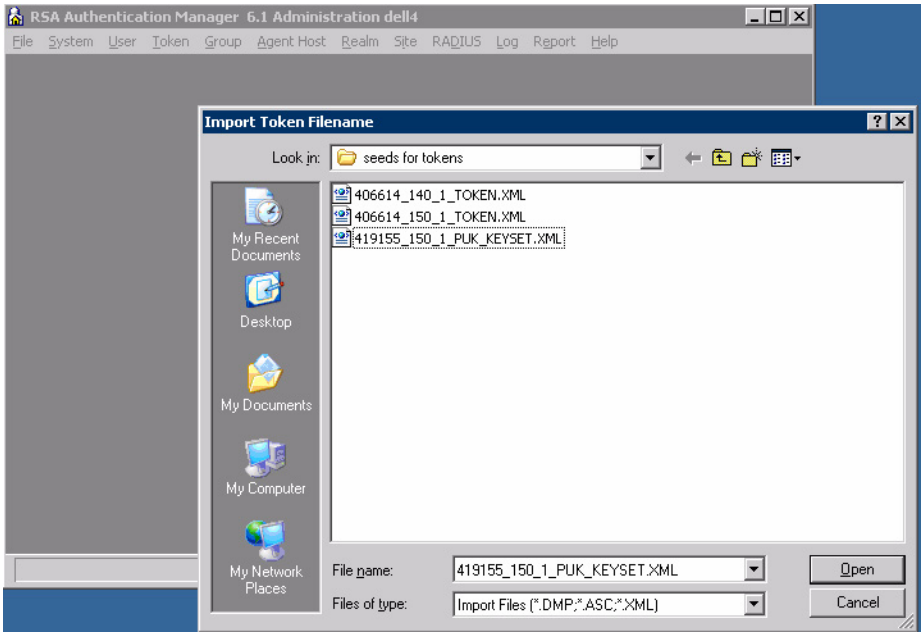
Setting the Time and Date

Because two-factor authentication depends on time synchronization, it is import that the internal clocks for the RSA Authentication Manager and the SSL-VPN appliance are set correctly.

Importing Tokens and Adding Users

After you have configured the RSA Authentication Manager to communicate with the SonicWALL SSL-VPN appliance, you must import tokens and add users to the RSA Authentication Manager. To do so, perform the following steps.

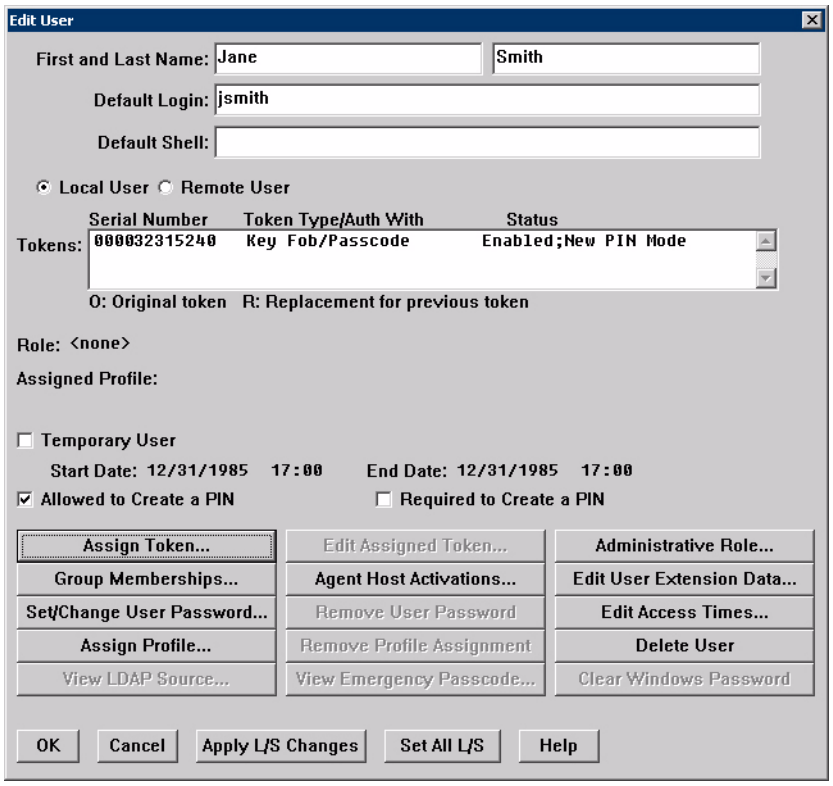
Step 1 To import the token file, select **Token > Import Tokens**.



Step 2 When you purchase RSA SecurID tokens, they come with an XML file that contains information on the tokens. Navigate to the token XML file and click **Open**. The token file is imported.

Step 3 The **Import Status** window displays information on the number of tokens imported to the RSA Authentication Manager.

Step 4 To create a user on the RSA Authentication Manager, click on **User > Add user**.

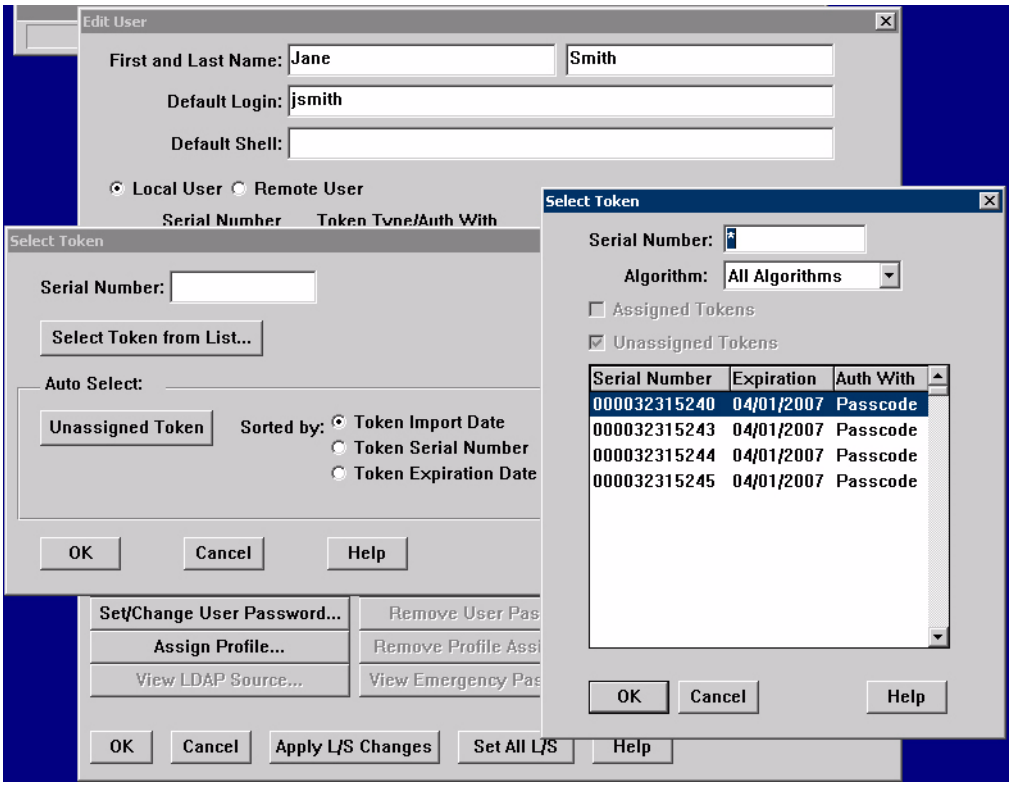


Step 5 Enter the user's **First and Last Name**.

Step 6 Enter the user's username in the **Default Login** field.

Step 7 Select either **Allowed to Create a PIN** or **Required to Create a PIN**. **Allowed to Create a PIN** gives users the option of either creating their own PIN or having the system generate a random PIN. **Required to Create a PIN** requires the user to create a PIN.

Step 8 To assign a token to the user, click on the **Assign Token** button. Click **Yes** on the confirmation window that displays. The **Select Token** window displays.



Step 9 You can either manually select the token or automatically assign the token:

- To manually select the token for the user, click **Select Token from List**. In the window that displays, select the serial number for the token and click **OK**.
- To automatically assign the token, you can optionally select the method by which to sort the token: the token's import date, serial number, or expiration date. Then click the **Unassigned Token** button and the RSA Authentication Manager assigns a token to the user. Click **OK**.

Step 10 Click **OK** in the **Edit User** window. The user is added to the RSA Authentication Manager.

Step 11 Give the user their RSA SecurID Authenticator and instructions on how to log in, create a PIN, and user the RSA SecurID Authenticator. See "RSA User Authentication Process" on page 17 for more information.

Configuring the VASCO VACMAN Middleware

The following sections describe how to configure two-factor authentication using VASCO's VACMAN Middleware Administration version 2.3:

Note This configuration procedure is specific to VACMAN Middleware Administration version 2.3.12. If you are using a different version of VACMAN Middleware Administration, the procedure will be slightly different.

If you will be using RSA instead of VASCO, see "Configuring the RSA Authentication Manager" on page 5.

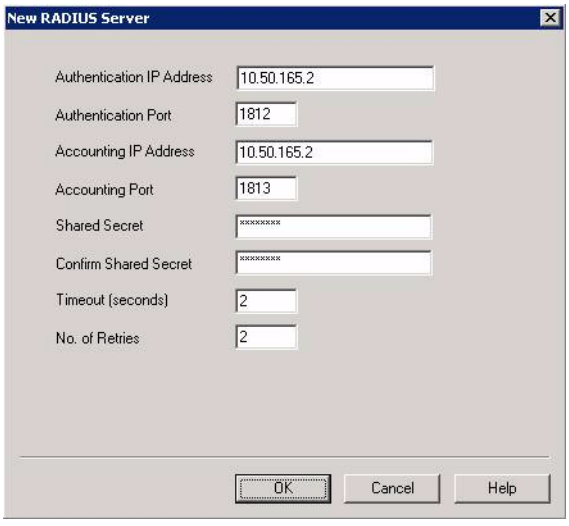
Adding the RADIUS Server to VACMAN Middleware

To create a connection between the Sonicwall SSL-VPN appliance and the VASCO server, you must create a component record for the external RADIUS server. VASCO servers do not have an internal RADIUS component, so they must use an external RADIUS server. To create a component record for the RADIUS server, perform the following steps:

Step 1 Launch the VACMAN Middleware Administration program.

Step 2 Expand the **VACMAN Middleware Administration** tree and the **VACMAN Server** tree.

Step 3 Right click on **RADIUS Servers** and click on **New RADIUS Server**.



Step 4 Enter the IP address of the RADIUS server in the **Authentication IP Address** field and the authentication port number in the **Authentication Port** field (the standard authentication port number is 1812). Note that this is the IP address of the RADIUS server and *not* the SonicWALL SSL-VPN appliance.

Step 5 Enter the IP address and port number for RADIUS accounting communication in the **Accounting IP Address** and **Accounting Port** fields, respectively. If a single RADIUS server is performing both authentication and accounting, the IP address is the same. The standard accounting port number is 1813.

Step 6 Enter the RADIUS shared secret in the **Shared Secret** and **Confirm Shared Secret** fields.

Step 7 Enter the desired timeout length number of retries in the **Timeout (seconds)** and **No. of Retries** fields.

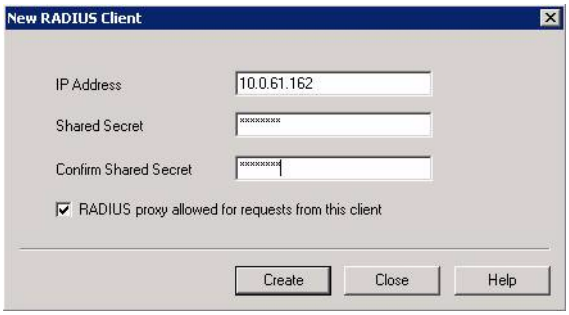
Step 8 Click **OK**.

Adding the SSL-VPN Appliance to VASCO

To add the SonicWALL SSL-VPN appliance to VACMAN Middleware Administrator as a RADIUS client, perform the following steps.

Step 1 Expand the **VACMAN Server** tree.

Step 2 Right-click on **RADIUS Clients** and click **New RADIUS Client**.



Step 3 Enter the **IP Address** of the SSL-VPN appliance.

Step 4 Enter the shared secret in the **Shared secret** and **Confirm Shared secret**.

Step 5 Click **Create**.

Setting the Time and Date

The DIGIPASS token is based on time synchronization. All tokens are created with their internal real-time clocks set to GMT. As such, it is important to set the date and time zone of the server running the VACMAN middleware to correctly so the GMT can be local derived correctly.

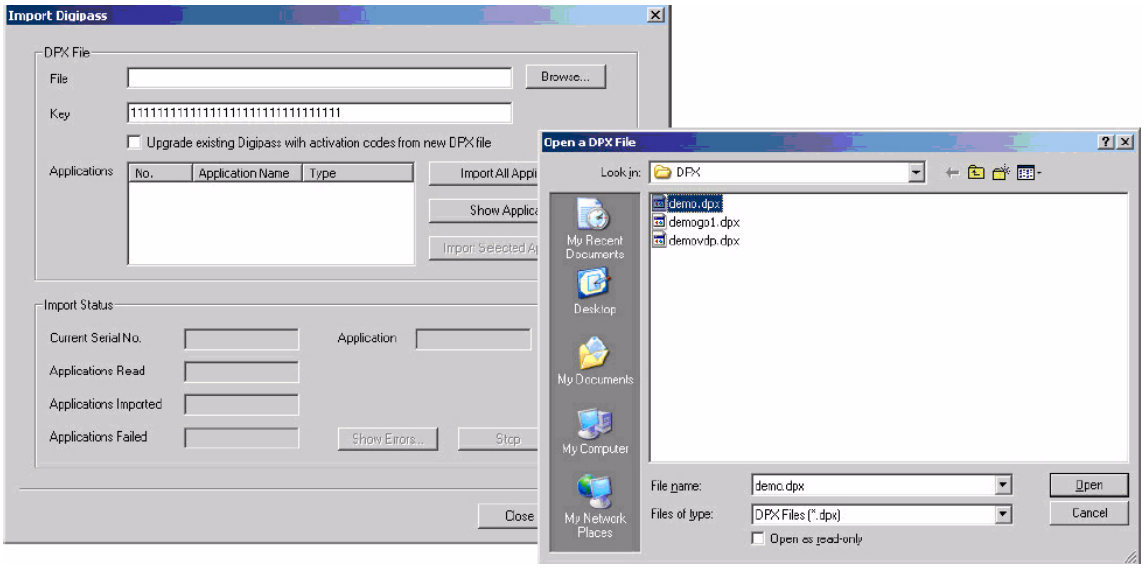
Importing Digipass Token Secret

Before Digipass tokens can be assigned to a user, their application records must be imported to the VACMAN middleware. To do this, perform the following steps.

Step 1 Right-click on the **Digipass** node under the **VACMAN server** tree.

Step 2 Click **Import Digipass**.

Step 3 Click **Browse**, navigate to the location of the Digipass import file, and click **Open**.



Step 4 Enter the Digipass import key in the **Key** field. The key is a 32-character hexidecimal number.

Step 5 Click **Import All Applications** to import all records in the file. Or to select the records to import, click **Show Applications**, select the records to import, and click **Import Selected Applications**.

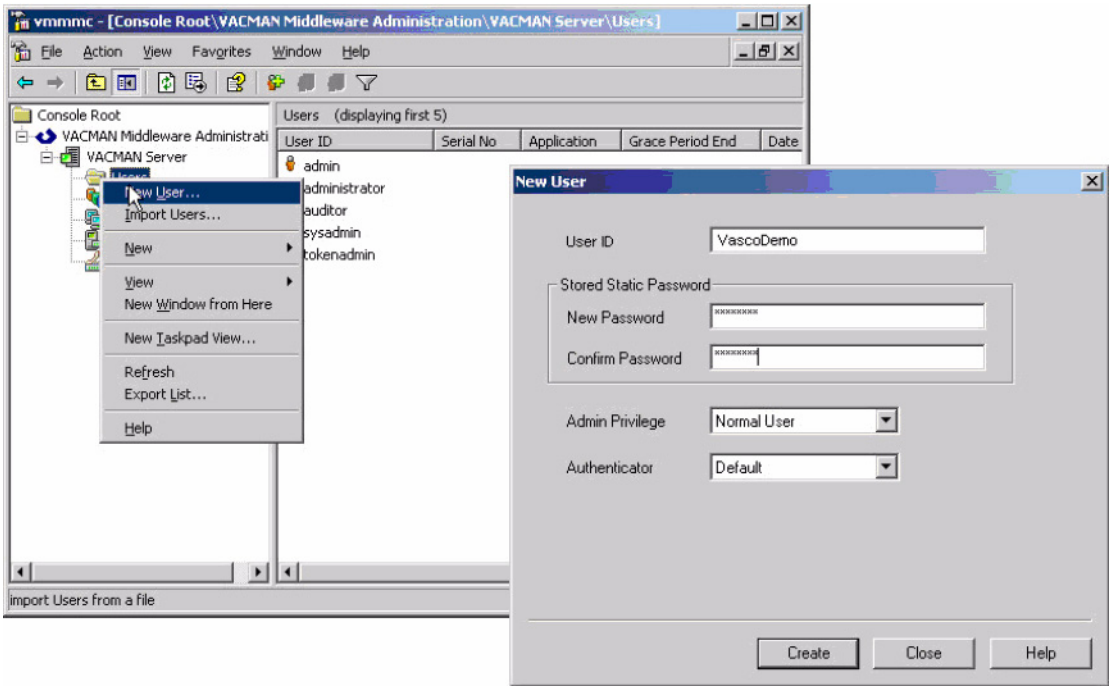
Step 6 The progress of the import procedure will be shown in the bottom **Import Status** section.

Creating Users

To add users to the VACMAN Middleware Administration, perform the following steps.

Step 1 Expand the **VACMAN Server** tree and right-click on **Users**.

Step 2 Click **New User**.



Step 3 Enter the username in the **User ID** field.

Step 4 Enter the user's password in the **New Password** and **Confirm Password** fields.

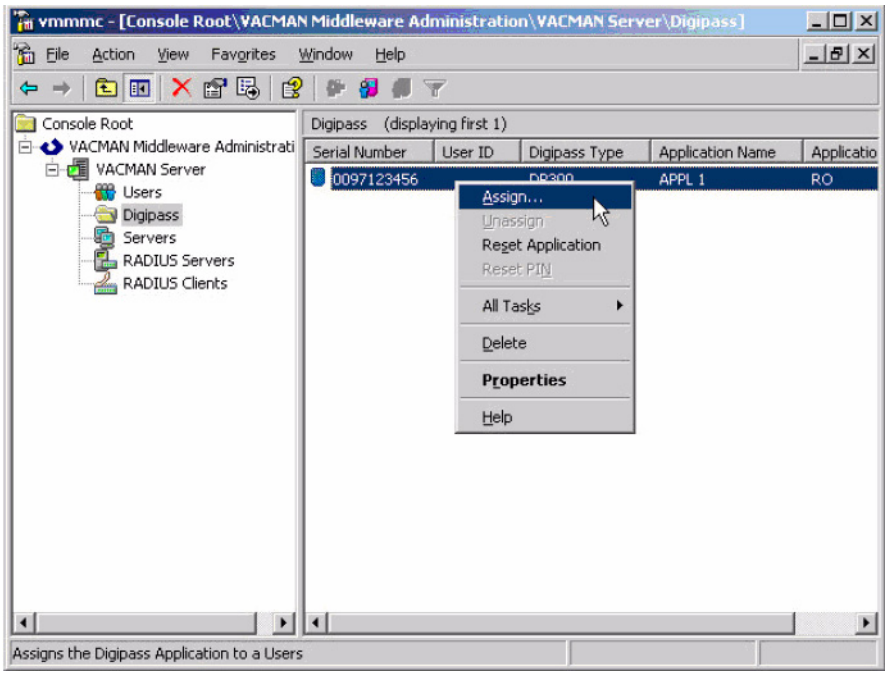
Step 5 Select the appropriate **Admin Privilege** and **Authenticator**.

Step 6 Click **Create**.

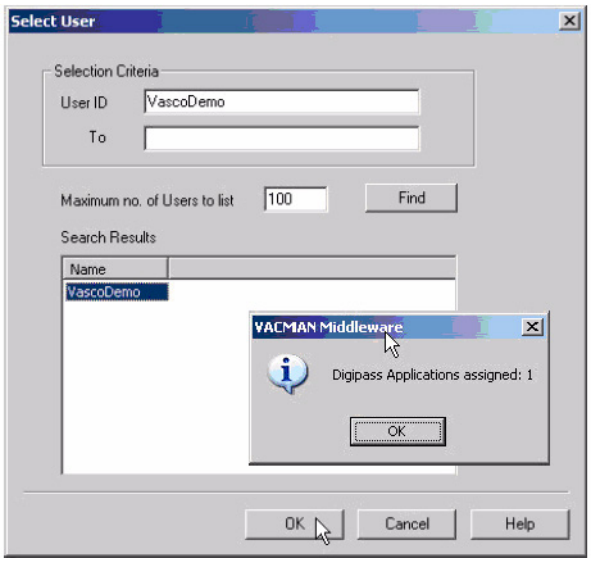
Assigning Digipass Tokens to Users

After you have imported the digipass tokens and created the users, you need to assign the Digipass tokens to the users. To do so, perform the following steps.

Step 1 Expand the **VACMAN Server** tree and click on **Digipass**.



Step 2 Right-click on the serial number of the Digipass token you want to assign and click **Assign**.



Step 3 Enter the username in the **User ID** field and click the **Find** button.

Step 4 When the username is displayed in the **Search Results** window, select the username and click **OK** to assign the Digipass token.

User Prerequisites

Before you can log in using two-factor authentication, you must meet the following prerequisites:

- Your administrator has created your user account.
- You have either an RSA SecurID token or a VASCO Digipass token.

User Configuration Tasks

The following sections describe how users log in to the SonicWALL SSL-VPN appliance using the two types of two-factor authentication:

- "RSA User Authentication Process" on page 17
- "VASCO User Authentication Process" on page 19

RSA User Authentication Process

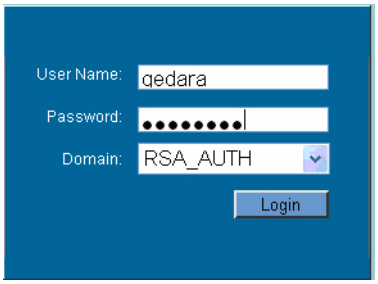
The following sections describe user tasks when using RSA two-factor authentication to log in to the SonicWALL SSL-VPN Virtual Office:

- "Logging into the SSL-VPN Virtual Office Using RSA Two-Factor Authentication" on page 17
- "Creating a New PIN" on page 18
- "Waiting for the Next Token Mode" on page 19

Logging into the SSL-VPN Virtual Office Using RSA Two-Factor Authentication

To log in to the SonicWALL SSL-VPN Virtual Office using RSA two-factor authentication, perform the following steps.

Step 1 Enter the IP address of the SSL-VPN appliance in your computers browser. The authentication window is displayed.



Step 2 Enter your username in the **Username** field.

Step 3 The first time you log in to the Virtual office, your entry in the password field depends on whether you have been given a PIN or if you need to create the PIN.

- If you already have a PIN, enter the passcode in the **Password** field. The passcode is the user PIN and the SecurID token code. For example, if the user's PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.
- If you do not have a PIN, enter the SecurID token code in the **Password** field.

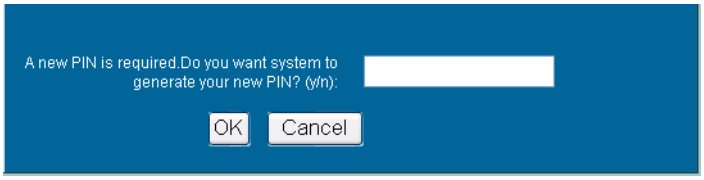
Step 4 Select the appropriate **Domain**.

Step 5 Click **Login**.

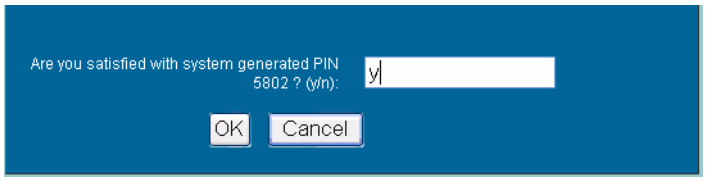
Creating a New PIN

The RSA Authentication Manager automatically determines when users are required to create a new PIN. will determines that user associated with a particular token requires a new PIN. SSL-VPN appliance prompts the user to enter new PIN.

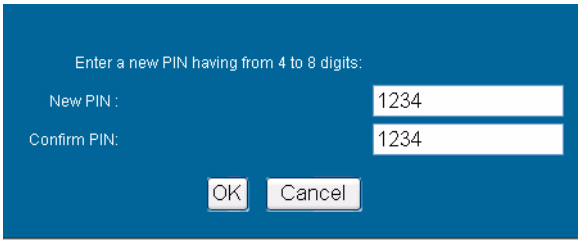
Step 1 If the user is configured for the **Allowed to Create a PIN** option, users are first asked if they want the system to generate a PIN. To have the system generate a PIN, type **y** and click **OK**. To create your own PIN, type **n** and click **OK**.



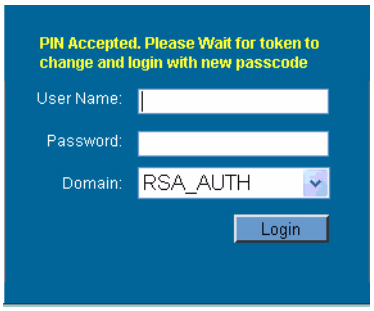
Step 2 The new PIN is displayed. To accept the PIN type **y** and click **OK**. To have the system generate a different PIN, type **n** and click **OK**.



Step 3 If you declined to accept a system-generated PIN, or if your username is configured for **Required to Create a PIN**, you are prompted to enter your new PIN. Enter the PIN in the **New PIN** field and again in the **Confirm PIN** field and click **OK**.

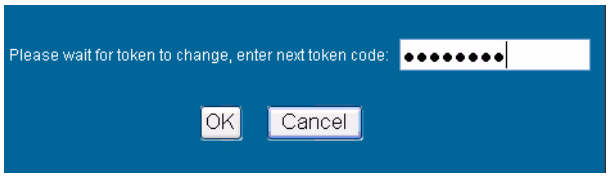


Step 4 The RSA Authentication Manager verifies that the new PIN is an acceptable PIN. If the PIN is accepted, the user is prompted to log in with the new passcode.



Waiting for the Next Token Mode

If user authentication fails three consecutive times, the RSA server requires the user to generate and enter a new token. To complete authentication, the user is prompted to wait for the token to change and enter the next token.



VASCO User Authentication Process

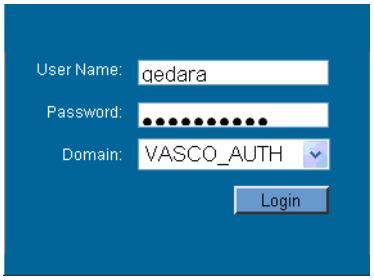
The following sections describe user tasks when using RSA two-factor authentication:

- "Logging into the SSL-VPN Virtual Office Using VASCO Two-Factor Authentication" on page 19
- "Creating a New PIN" on page 18

Logging into the SSL-VPN Virtual Office Using VASCO Two-Factor Authentication

To log in to the SonicWALL SSL-VPN Virtual Office using VASCO two-factor authentication, perform the following steps:

Step 1 Enter the IP address of the SSL-VPN appliance in your computers browser. The authentication window is displayed.



Step 2 Enter your username in the **Username** field.

Step 3 Enter the passcode in the **Password** field. The passcode is the user PIN and the VASCO Digipass token code. For example, if the users PIN is 8675 and the token code is 30966673, then the passcode is 867530966673.

Step 4 Select the appropriate **Domain**.

Step 5 Click **Login**.

Creating a New PIN

To manually change your PIN using the SSL-VPN Virtual Office login page, perform the following steps.

Step 1 Enter the IP address of the SSL-VPN appliance in your computers browser. The authentication window is displayed.

Step 2 Generate a VASCO token.

Step 3 Enter your username in the **Username** field.

Step 4 In the **Password** field, enter the following string: existing PIN + token + new PIN + new PIN.

For example, if your existing PIN is 5555, the token is 3333, and your new PIN is 1234, you would enter the following in the **Password** field: 5555333312341234.

Solution Document Version History

Version Number	Date	Notes
1	9/22/2006	This document was created.