SonicWALL Authentication Service

SONICWALL

Table of Contents

Copyright Notice

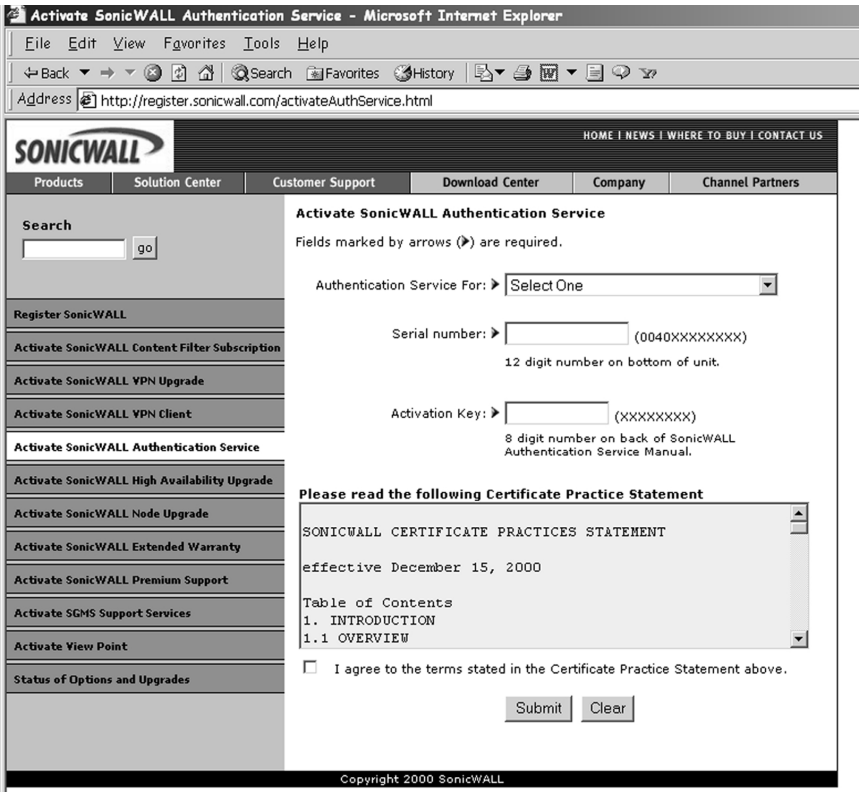
Getting Started with SonicWALL Authentication Service

SonicWALL now offers an optional **Authentication Service** for VPN users. The **Authentication Service** uses digital certificates for identification of remote VPN clients. The service adds another level of security for VPN users who remotely access a server for information. More information on the **Authentication Service** can be found in the **Authentication Service Data Sheet** located at http://www.sonicwall.com.

Registering the SonicWALL Authentication Service

It is necessary to register the SonicWALL **Authentication Service** before the administrator and remote user VPN certificates can be downloaded.

1. Using a Web browser, open <http://register.sonicwall.com> and click the Activate Authentication Service link.



2. Select the type of **Authentication Service** to be activated. Fill in the SonicWALL appliance's serial number and the 8-digit activation key shown on the back cover of this manual into the **Activation Key** field.

3. Read the **Certificate Practice Statement,** and check the **I agree to the terms in the Certificate Practice Statement** check box.

4. Click **Submit**. The operation takes a few seconds to complete. Once completed, a message confirming the registration is displayed in the Web browser window.

Installing and Activating the Firmware

Download the Authentication Service-enabled firmware to your computer from the SonicWALL Web site. After downloading, log into your SonicWALL management interface from a Web browser. If you're uncertain of this procedure, see your SonicWALL user manual for instructions.

***Note**: If you have firmware version 6.0.0 or greater, you do not need to upload the Authentication Service - enabled firmware.*

Obtaining the Administrator Certificate

After enabling the **Authentication Service** by registering the **Activation Code**, you may begin to configure the **Authentication Service** by requesting an **Administrator Certificate**. The **Administrator Certificate** is required for both box-to-box connections and end-user connections.

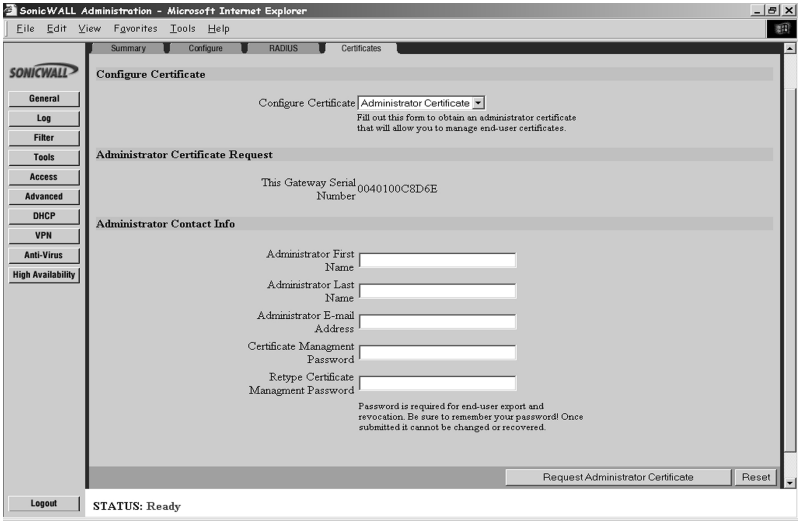
1. Log into the management interface and click **VPN**.

2. Click the **Certificates** tab. Select **Administrator Certificate** from the **Configure Certificate** menu.

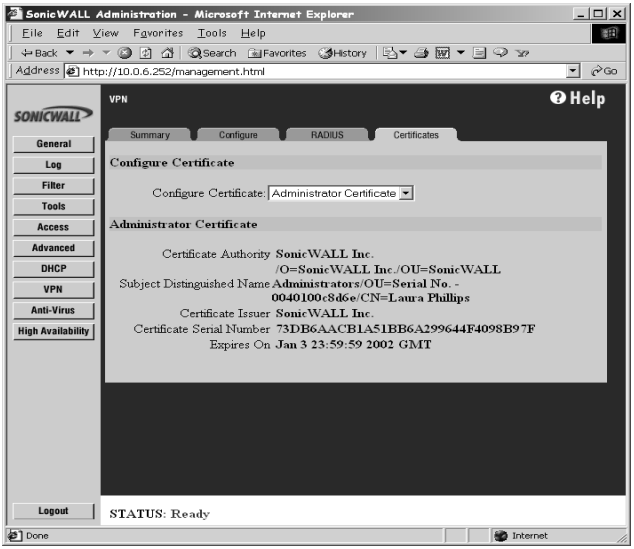
3. Fill in the requested information in the **Administrator Contact Info** section.

4. Create a unique **Certificate Management Password** using alphanumeric characters. It is also case-sensitive.

   ***Note**: The **Certificate Management Password** created by the administrator should be different from the administrator password used to log into the management interface. Store the Certificate Management Password in a safe place as it cannot be changed nor is it stored anywhere for retrieval.*



5. Click the **Request Administrator Certificate** button to submit the information to the **Certificate Authority** server. The submission takes a few seconds. As soon as the information is confirmed, a screen appears with the following information:



6. The **Authentication Service** is now ready and may be used to request end-user certificate or configure a remote appliance to use certificates.

Note: *It is very important to export the downloaded administrator certificate to an external medium (floppy disk or zip disk) and store in a safe, secure place. If the firmware is wiped, you will need the administration certificate to restore the* ***Authentication Service****. See the* ***Exporting with Private Key*** *section of* ***Managing the Authentication Service.***

Configuring VPN for Authentication Service

To use certificates in the VPN service in the Management interface, there are two ways of setting up the Authentication Service:

- Group VPN tunnel for VPN Clients
- SonicWALL appliance to SonicWALL appliance

Configuring Group VPN Tunnel

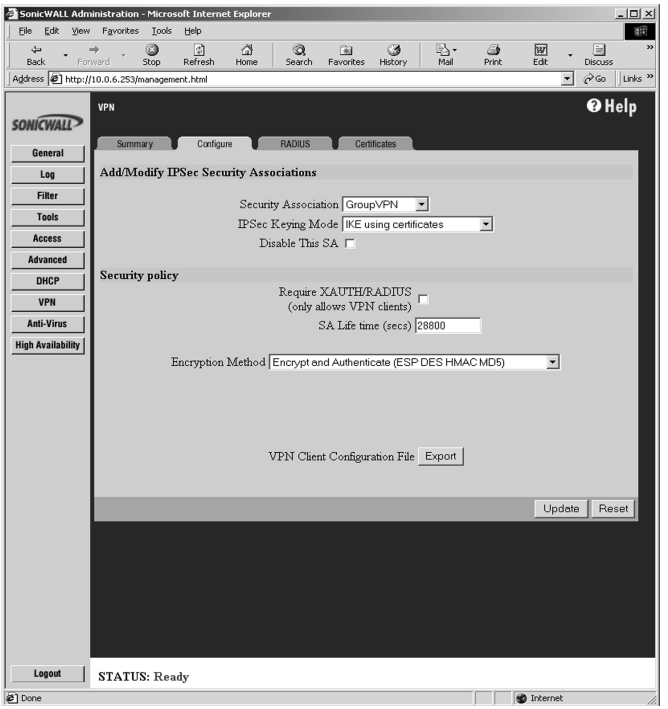
To use certificates with the Group VPN tunnel and to authenticate remote VPN users, the **IPSec Security Association** must be configured as follows:

1. Log into the Management interface and click **VPN**.Click on the **Configure** tab.

2. In the **Add/Modify IPSec Security Association** section, select **Group VPN** for the **Security Association**.

3. Select **IKE using certificates** in the **IPSec Keying Mode**.

4. Select **Encrypt and Authenticate** for the **Encryption Method**.



7. Click **Update** to enable the **Security Association**.

Configuring SonicWALL to SonicWALL VPN

Digital certificates can be used with a VPN tunnel from one SonicWALL appliance to another SonicWALL appliance. For instance, a remote VPN user has a SonicWALL SOHO2 and wants access to the corporate LAN behind a SonicWALL PRO-VX. The corporate PRO-VX downloads the Administrator Certificate into its VPN configuration. To configure the VPN tunnel using certificates, the following steps are used to configure the remote SOHO2 appliance:

1. Log into the Management interface of the remote appliance, and click on **VPN**.

2. Click the **Configure** tab.

3. In the **Add/Modify IPSec Security Association** section, select **Add New SA** for the **Security Association**.

4. Select **IKE using certificates** in the **IPSec Keying Mode**.

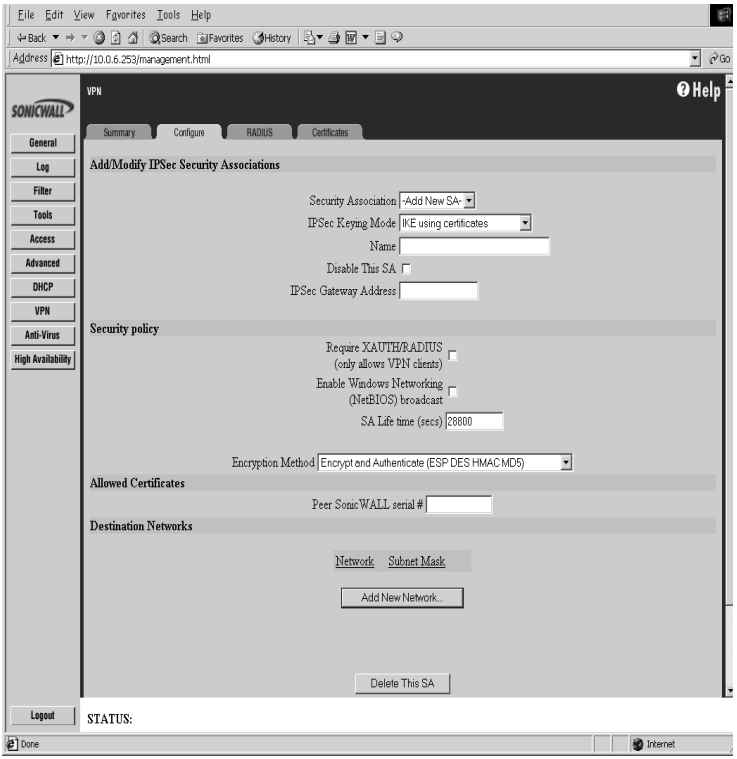
5. Create a name for the **SA** and type it in the **Name** box.

6. Leave **Disable this SA** unchecked.

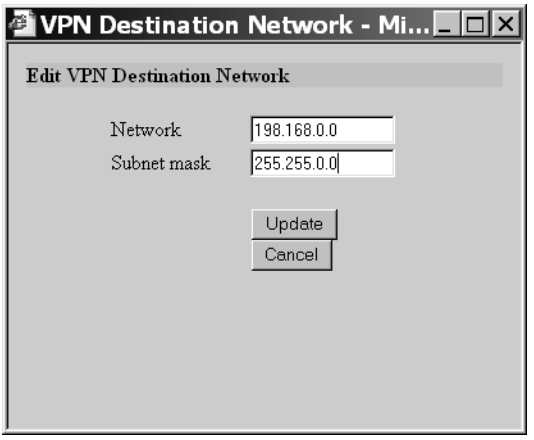
7. Type in the IP address of the remote VPN gateway in the **IPSec Gateway Address** box. To allow a VPN gateway with a dynamic IP address to connect, enter “0.0.0.0”.

8. In the **Security Policy** section, leave **Require XAUTH/RADIUS (only allows VPN clients)** and **Enable Windows Networking (NetBIOS) broadcast** unchecked. Select **Encrypt and Authenticate (ESP DES HMAC MD5)** in the **Encryption Method** box.

9. In the **Allowed Certificates** section, type in the serial number of the SonicWALL appliance that has an Administrator’s certificate.



10. In the **Destination Network** section, click **Add New Network**. Type in the destination network and the subnet mask. Click **Update**.

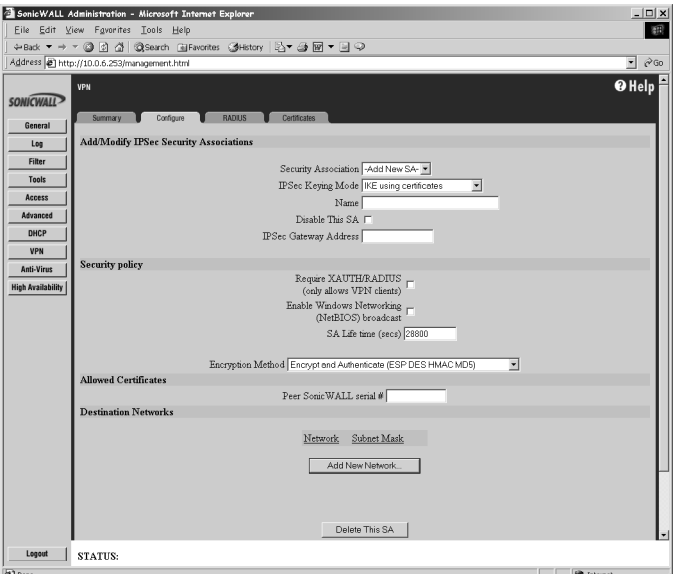


11. When you return to the management interface, click **Update** and the changes are applied to the SonicWALL appliance.

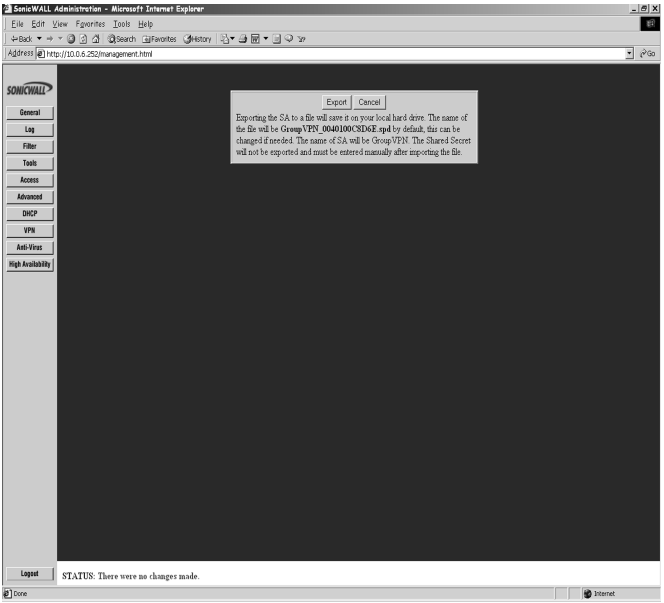
Exporting the Security Policy to a Remote Client

For easy configuration of remote VPN clients, exporting the security policy from the SonicWALL appliance to a file can be performed. However, only Group VPN Security Settings can be exported to a file. To export the security policy to a file, the following steps are used:

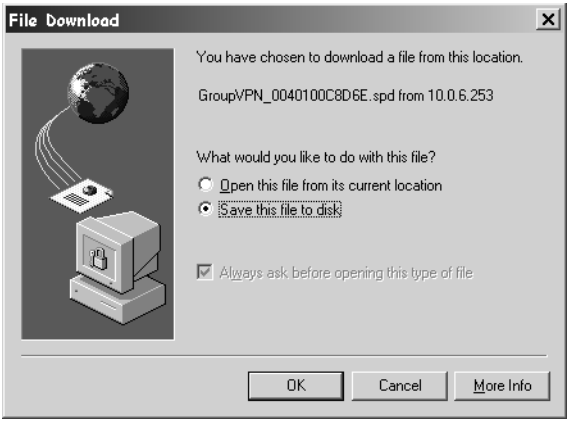
1. Log into the management interface and click **VPN**. Then select the **Configuration** tab.
2. In the Security Policy section, click on **Export** next to the **VPN Client Configuration File**.



A dialogue box appears. Click **Export** to export the security policy file.



3. To download the file, click **OK**.



Standard Windows operating system dialogue boxes appear allowing you to change the location and file name of the security policy. Once the file is saved, you can distribute the security policy to your remote VPN clients.

Managing the Authentication Service

The administrator of the SonicWALL appliance has complete control over the **Authentication Service** function and the remote VPN clients. By default, there are two subsections within the **Certificates** tab panel:

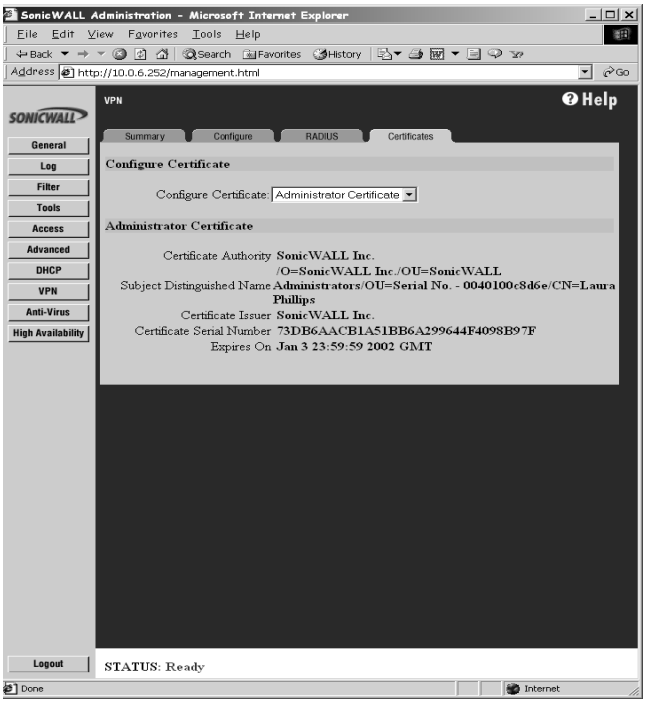
- **Administrator Certificate**
- **Services**

Once an Administrator certificate is successfully received by the SonicWALL unit, a third view, **End-User Certificates** is available. To change views, use the pulldown menu in the **Configure Certificate** subsection which appears in every view of the **Certificates** tab panel.

The Administrator Certificate View

The **Administrator Certificate** view displays the following information:

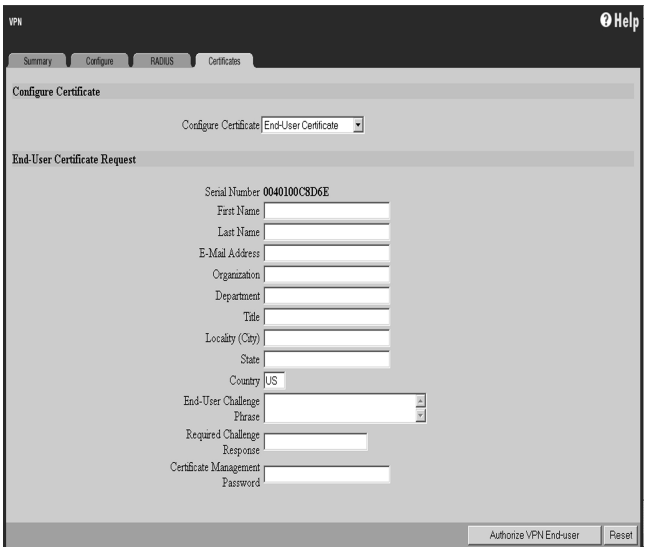
- **Certificate Authority** - the issuing authority of the certificate
- **Subject Distinguished Name** - the name of the administrator
- **Certificate Issuer** - who issued the certificate
- **Certificate Serial Number** - generated by the certificate issuer
- **Expires on** - date and time of certificate expiration



The Request End-User Certificate Function

The **Request End-User Certificate** screen is used to request digital certificates for VPN Clients. The following information is required for the certificate to be issued:

- **First Name**
- **Last Name**
- **Email Address**
- **Organization**
- **Department**
- **Title**
- **Locality (City)**
- **State**
- **Country**
- **End-User Challenge Phrase**
- **Required Challenge Response**
- **Certificate Management Password**



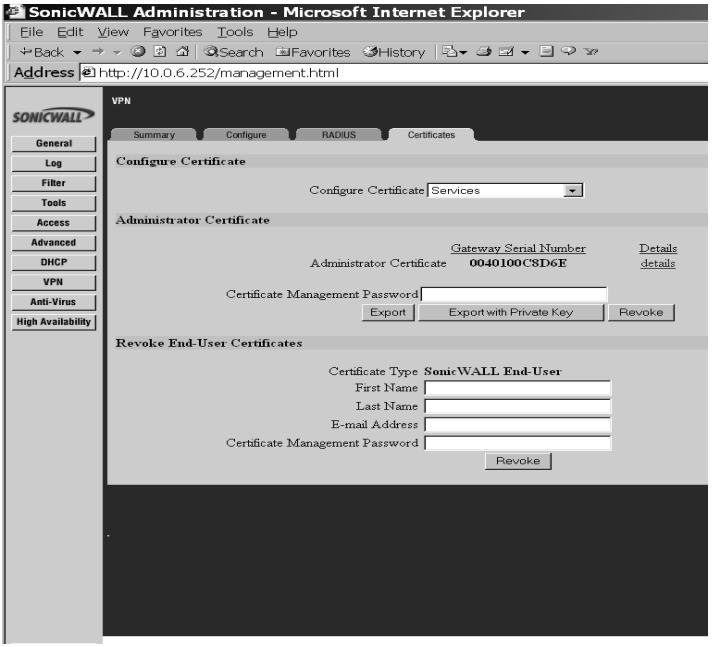
It is very important to enter the correct email address for an end-user VPN client as the e-mail message directs the end-user to the digital certificate web site. The **End-User Challenge Phrase** and **Required Challenge Response** are used to communicate password information between the administrator and the end-user. This information is required to obtain the digital certificate. More detailed information on the end-user certificate can be

found in the **End-User Certificates** section of this manual. Additionally, the certificate server does not verify the validity of the information entered into the on-line form as outlined in the **Certificate Practice Statement** (CPS). You are responsible for all the information you enter for an end-user.

Using the Services Function

The basic functions of the **Services** screen are listed below:

- **Export** the administrator certificate information
- **Export** the administrator certificate information with the Private Key
- **Revoke** an administrator certificate
- **Revoke** remote VPN Client certificates



Exporting the Administrator Certificate Information

If it is necessary to export your certificate information without the private key, use the **Export** function. In the event that your firmware is reset or wiped, however, this certificate file does not contain enough information to restore the **Authentication Service**. Use the **Export with Private Key** to create a secure back up file for your **Authentication Service**. To export the information, follow these steps:

1. If using a floppy disk or zip disk for storage, insert the disk into the disk drive.

2. In the management interface, select **Services** in the **Configure Certificate** subsection.
3. Under the **Administrator Certificate** subsection, type in the **Certificate Management** password, and click **Export**.

The following screen is displayed:

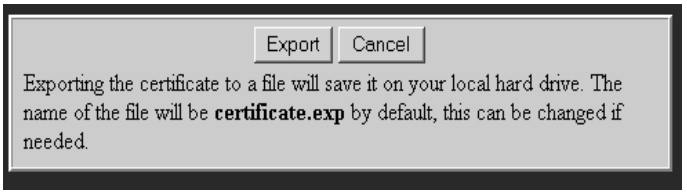
4. Click **Export** to open a file directory dialogue box and save the settings to your storage medium or directory.

Exporting with Private Key

It is very important to create a backup copy of your administrator certificate information in the event that your firmware becomes corrupted, wiped out, or reset. To restore the **Authentication Service** to the SonicWALL appliance, the private key is required by the firmware. To **Export with Private Key**, use these steps:

1. If using a floppy disk or zip disk for storage, insert the disk into the disk drive.
2. In the management interface, select **Services** in the **Configure Certificate** subsection.
3. Under the **Administrator Certificate** subsection, type in the **Certificate Management** password, and click **Export with Private Key**.

The following screen is displayed:



4. Click **Export** to open a file directory dialogue box and save the certificate file to your storage medium or directory.
5. Store the storage medium in a safe, secure place such as a fireproof safe.

Revoking an Administrator Certificate

***Warning**: Revoking an administrator certificate is irreversible and will disable the Authentication Service.*

An administrator certificate may have to be revoked in certain situations:

- The certificate management password is compromised.
- The SonicWALL appliance is stolen.
- The **Authentication Service** is no longer required for your VPN clients.

Careful consideration should be given to the decision to revoke an administrator certificate as you no longer have a valid activation key and cannot restore the service. Even if the firmware is reset and the backup copy of your certificate is used, the service cannot be restored. You must be absolutely sure that you wish to revoke the administrator certificate.

If the SonicWALL appliance is compromised or stolen, you may revoke the administrator certificate by contacting SonicWALL Technical Support.

Renewing an Administrator Certificate

The SonicWALL **Authentication Service** is valid for one year from date of purchase. To continue the service, you may purchase another subscription from SonicWALL and register your upgrade to continue uninterrupted **Authentication Service**. You are then able to renew the **Authentication Service**. To renew the **Authentication Service**, proceed as follows:

1. Register your upgrade at http://register.sonicwall.com with the purchased Activation Key to re-activate the **Authentication Service**.

2. Log into the management interface, and click **VPN**.

3. Click the **Certificates** tab, and select the **Services** view.

4. In the **Administrator Certificate** subsection, type in the **Certificate Management** password.

5. Click **Revoke**.

Obtain a new **Administrator Certificate** by following the steps in the front of this manual.

End-User Certificate Management

***Note**: The remote VPN client must download the VPN Client software version 5.1.3 before using Authentication Service.*

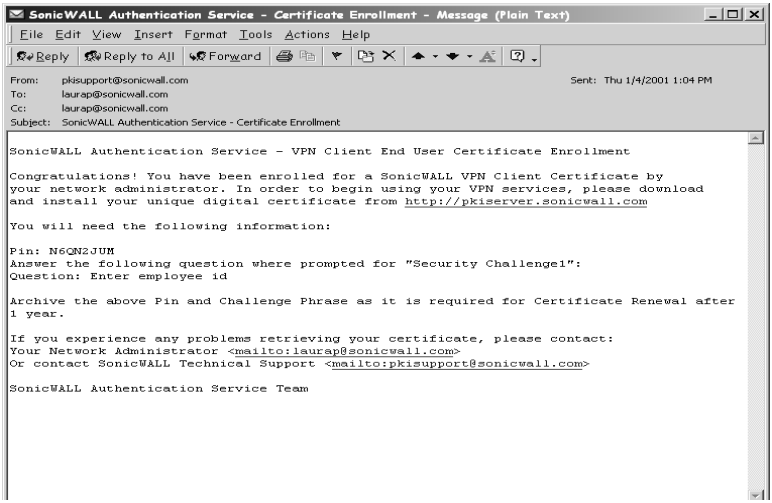
The SonicWALL **Authentication Service** requires the remote VPN Client to use a digital certificate for identification on the local network. The SonicWALL appliance administrator manages the end-user certificate by notifying the remote VPN client to pick up a digital certificate or by revoking a client certificate. If you are using Microsoft Internet Explorer Version 5.0, you have to download the 128-bit encryption security patch available at http://www.microsoft.com/windows/ie/download/128bit/intro.htm. Netscape Navigator version 4.75 and higher currently use 128-bit encryption.

Requesting a Digital Certificate for a VPN Client

To request a digital certificate for an end-user, you activate the service on the SonicWALL web site at http://register.sonicwall.com. After the service is activated, log into the SonicWALL management station and follow the instructions below:

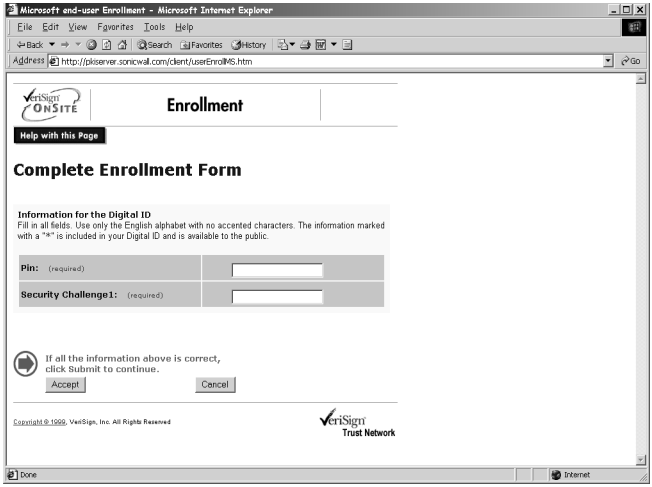
1. Click **VPN** on the left side of the interface. Then click on the **Certificates** tab.
2. Select **End-User Certificate** from the pull-down menu in the **Configure Certificate** subsection.
3. Fill out the information requested by the form. Be sure all of your information is correct as the certificate server does not verify the validity of the information.
4. The **End-User Challenge Phrase** and **Challenge Response** can be managed in a variety of ways. For instance, the administrator could use "Enter your employee id number" for the **Challenge Phrase** and type in the employee id number in the **Challenge Response** box. When the employee receives the email notification that a digital certificate is waiting for pick up, the employee goes to the certificate web site, types in the PIN and the response to the **Challenge Phrase**. Another example of managing the **End-User Challenge Phrase** is to use a familiar item to the end-user such as a cell phone number or asking the user via a separate email message to call the administrator for the **Challenge Response** answer. The strength of the Authentication Service is dependent on the **Challenge Response.**
5. When the End-User Certificate is successfully requested, an email is generate to the end-user and the administrator notifying them that a digital

certificate is ready for pick up. An example email message is displayed below:



6. The end-user clicks on the web address for the PKI Server, and then clicks on **Pick-Up Certificat**e to download the certificate.

7. When **Pick-Up Certificate** is clicked, the **Pick Up Digital Certificate** page is displayed.



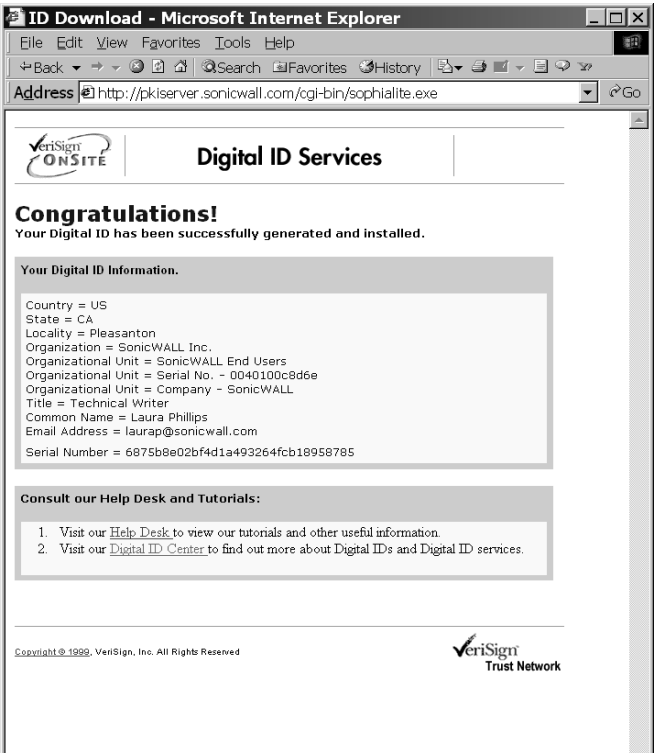
8. The End-User types in the PIN from the email notification and the **Challenge Response** and clicks **Submit**.
9. If the **Challenge Response** and **PIN** are correct, the digital certificate is issued. A successful submission is shown below.

After a successful submission and issuance of a certificate, you are asked to download the certificate file using **Medium** security.

10. Click **Set Security Level** to set the security level for downloading the certificate. You should set the **Security Level** to **High** as this level of security requires a password for the user to export the certificate from the web browser. The password is also required to import the certfi cate into the VPN Client. If there are multiple users on one computer, a user can only export a personal certificate accessed with a pass word.

11. Select **High** and click **Next**. You are asked to create a name for the password, and then create a password. It is recommended that you name the password with your first name, and create a personal password using alphanumeric characters. A combination of letters and symbols is recommended, and the password is cas-sensitive.
12. When you click **Finish**, the Creating a New RSA Exchange Key screen appears, and you can click **Details** to review the security policy.

13.Click **OK,** and the digital certificate is waiting to be issued.

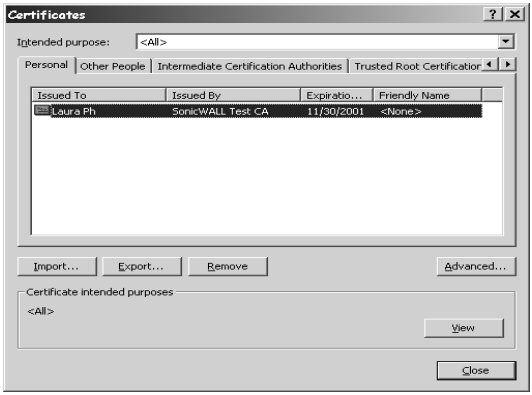


The digital certificate is successfully issued to you, and you are ready to begin exporting the certificate from the web browser . After exporting the file from the web browser, you may import it into the VPN Client.

Exporting the Digital Certificate to SonicWALL VPN Client

The digital certificate is exported from the web browser to a directory for the Remote VPN Client configuration. To export the digital certificate, use the following steps:

1. Open the browser to the default home page. Select **Tools** from the **Menu** bar, then select **Internet Options**.
2. Click on the **Content** tab. In the **Certificates** subsection, click **Certificates**.



3. Click on the certificate issued by SonicWALL, and then click on **Export**.

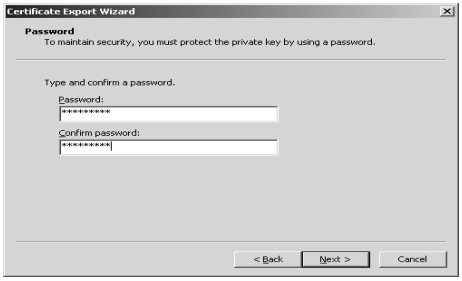
The **Export Certificate Wizard** appears and walks through the **Export** steps. After the Wizard appears, click **Next** to continue.

4. Select **Personal Information Exchange** and **Enable Strong Encryption**. Click **Next**

.

5. The **Export Private Key** dialogue box appears asking to export the certificate with or without the private key. Select **Yes, export the private key**.

6. To export a certificate with the private key, a password is required. Create and enter a password for the certificate. Click **Next**.
7.



8. Create a file name for the certificate and then **Browse** for a directory to save the file. Click **Next** to continue.

9. A window listing the file attributes is displayed. Click **Next** to continue

.

10. A warning box appears as a notification that you are exporting the private key and that a password is necessary to export the file. The password created in Step 6 is used to import the file into the VPN Client later. Click **OK** to continue.

11. IF the file export is successful, then a message box appears with the message that the file export is successful.

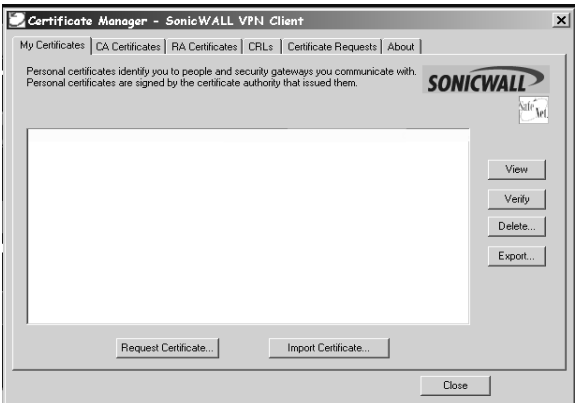
Importing a Digital Certificate into VPN Client

The remote VPN Client imports the digital certificate into the VPN Client software using the **Certificate Manager**. The VPN Client uses the following steps:

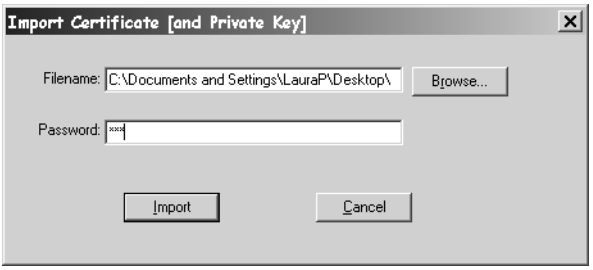
1. Right click on the VPN Client icon in the right end of the task bar. Select **Certificate Manager**.

2. The **Certificate Manager** window is displayed. Select **Import Certificate.**

.



3. The **Import Certificate** dialogue box is displayed. Use the **Browse** button to navigate to the directory where you saved the certificate file. It is in a *.pfx or *.p12 file format. Type in the password created using the **Export File Wizard**. Click **Import**.



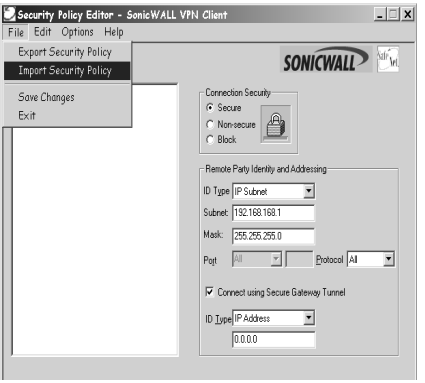
4. A confirmation box displays the certificate information and asks you to confirm importing the file. Click **Yes** to import the certificate

5. The certificate is now imported into the VPN Client software.

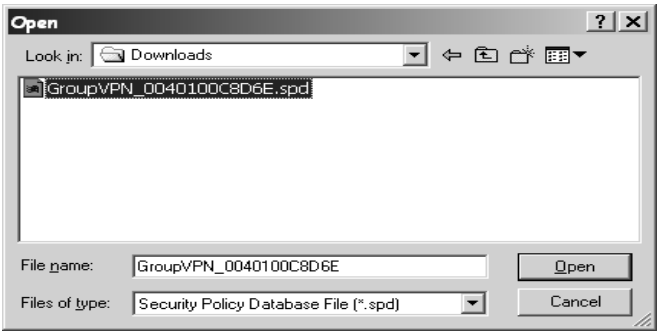
Importing a Security Policy into VPN Client

You, as the administrator of the SonicWALL appliance, can export the security policy for remote VPN Client use as explained earlier in the Group VPN policy export section of this manual. By providing the policy in a file format, the remote user doesn't configure the settings, but simply imports the policy into the client software.

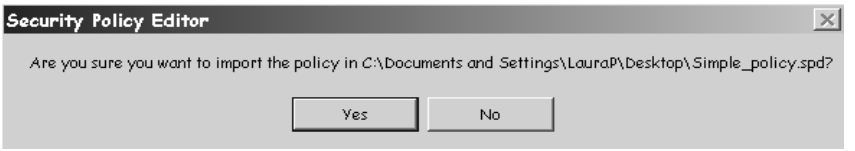
1. Right click on the **VPN Client** icon in the task bar. Click on **Security Policy Editor**.
2. Click **File**, then **Import Security Policy**. The **File Import** dialogue box appears.



3. Browse to the location that the security policy file is saved, and select the file. Click **Open**.

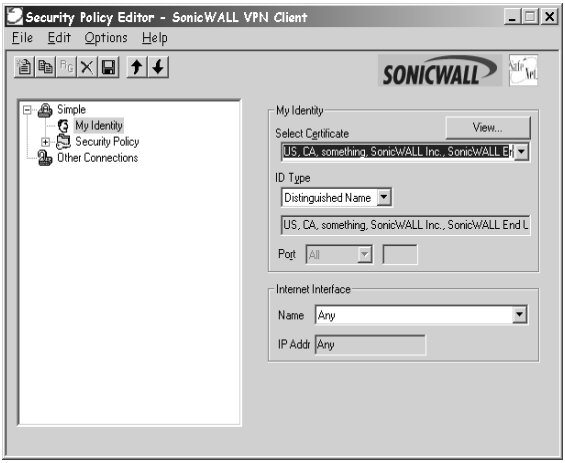


4. Confirm that you want to import the security policy file. Click **Yes** to import the policy and to complete the importing process.



Configuring the VPN Client Security Policy to Use Certificates

1. Open the **Security Policy Editor** and click on **My Identity**.

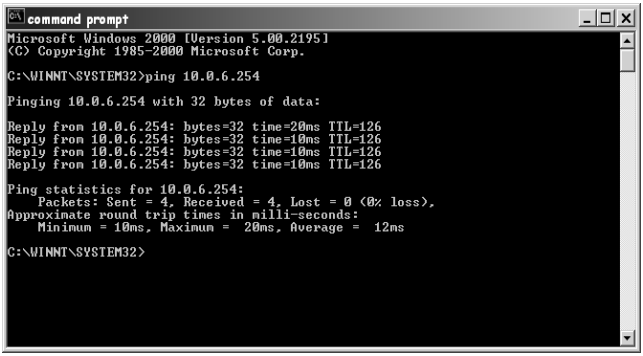


2. In the **My Identity** section, select the certificate from the **Select Certificate** pulldown menu. The **ID Type** changes to **Distinguished Name**.
3. The remote VPN Client is now configured to use the **Authentication Service** for the VPN tunnel.

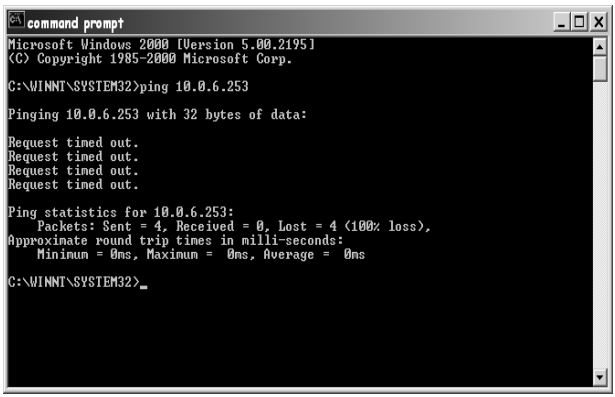
Verifying the Remote VPN Client Connection

To verify that the VPN tunnel is working, it is necessary to ping the IP address of a computer on the remote network. The instructions below show step by step how to ping the remote IP address.

1. Locate the Windows **Start** button in the lower left hand corner of the desktop operating system. Click **Start**, then **Run**, and then type **Command** in the **Open** filepath box. A DOS window will open to the **C:\ prompt**.



2. Type **ping** and the IP address of the computer on the remote network. You may need to provide the IP address to the VPN Client. A successful **ping** shows that the remote IP address is receiving data and shows replies from the data packets.
3. If the **ping** is unsuccessful, the data packets time out during transmission and no data is returned from the remote IP address. You may have to **ping** a few times until the connection is established. An unsuccessful ping appears below:



The **VPN Client Log Viewer** may be used to review successful or unsuccessful data packet transmissions. The **Log Viewer** is opened by right-clicking on the **Client** icon in the system tray. Successful **pinging** will return SPI values in the Log Viewer. If you cannot ping the computer on the remote network, contact your administrator for assistance.

Revoking VPN Client Certificates by the Administrator

Warning: *Revoked certificates cannot be restored unless another certificate is purchased.*

A VPN client certificate can be revoked by the administrator. The administrator can revoke the certificate without reconfiguring the SonicWALL appliance. You must carefully consider the decision to revoke a remote client certificate as it cannot be re-instated. To issue a certificate to a remote client ,but you do not have any unissued certificates, you will need to purchase **End-User Certificates** from SonicWALL. After activating the certificates on the web site, you will request another digital certificate through the **Certificate** tab of the VPN service of the management interface.

1. Log into the SonicWALL management interface. Click **VPN**, and then the **Certificates** tab.
2. In the **Configure Certificates** section, select **Services** from the pull-down menu.
3. In the **Revoke End-User Certificates** section, fill in the required boxes. The required information must match the original request information to revoke the certificate. Type in the **Certificate Management** password, and click **Revoke**.

The management interface updates and then displays a message, **"pki revoke complete.**"

The Remote VPN Client may also revoke their own certificate from the http://pkiserver.sonicwall.com web site. The end-user must remember the challenge phrase response to revoke the certificate.

Warning: *Revoked certificates cannot be restored unless another certificate is purchased.*

Authentication Service Activation Key

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Phone:408-745-9600
E-mail: sales@sonicwall.com
Web: http://www.sonicwall.com

Part #232-000100-00
Rev. A 01/01