Release Notes

Secure Remote Access

SonicWALL SSL VPN 2.5 Early Field Trial

Contents

Platform Compatibility

The SonicWALL SSL VPN 2.5 release is supported on the following platforms:

- **SonicWALL SSL VPN 2000**
- **SonicWALL SSL VPN 4000**

New Features

The following new features are supported on the SonicWALL SSL VPN 2.5 release:

- **SonicWALL Virtual Assist**: SSL VPN 2.5 allows a technician to remotely diagnose and fix issues an off-site computer may be experiencing. The technician can remotely take control of the machine through secure control of mouse and keyboard to repair the problem while the customer is watching. This feature allows IT to support users off-site as if they were physically there.
  Requirements: Virtual Assist can only take remote control of Windows based operating systems. The technician needs to be behind the SonicWALL SSL-VPN appliance or running NetExtender in order to utilize the Virtual Assist feature.
- **NetExtender for Mac & Linux**: SSL VPN 2.5 has a NetExtender client that is compatible with MacOS and Linux systems. It uses a similar graphical layout and has many of the same basic features as the NetExtender client for Windows for ease of use.
  Mac Requirements:
  - Mac OS X 10.4+
  - Apple Java 1.4+ (can be installed/upgraded by going to Apple Menu > Software Update; should be pre-installed on OS X 10.4+)

  Linux Requirements:
  - i386-compatible distribution of Linux
  - Fedora Core and Ubuntu.
  - Sun Java 1.4+
- **NetExtender Windows Client Enhancements**: The NetExtender client for Windows from SSL VPN 2.5 comes with added features and improved functionality including a new log system and log viewer that supports flexible log formats, such as binary log files. The standalone log viewer can filter logs by time and log levels.
- **Reverse-Proxy Enhancements**:
  - Java applet rewriting
  - Flash rewriting

  - URL/Port based policies
  - Variable response size
- **Portal Enhancements**: SSL VPN 2.5 features numerous enhancements to the Portal configuration capabilities such as: the web server can listen on different IP addresses, new management rules that can be set for HTTP, HTTPS, and Ping, Virtual Office portals that can now use customized logos and specify the server certificate used.
- **Per Bookmark Single Sign-On Credentials**: SSL VPN 2.5 supports Single Sign-On for RDP and FTP bookmarks.
- **RDP Enhancements**: SSL VPN 2.5 supports the 'Login as Console' option, the ability to control the number of colors used in RDP sessions, and the 'Execute in Folder' option.

Known Issues

This section contains a list of known issues in the SonicWALL SSL VPN 2.5 release.

- **51502**: **Symptom**: NetExtender client may have compatibility problems with Vista Ultimate. **Condition**: Occurs when NetExtender launches on Vista Ultimate and the initializing engine fails.
- **51572**: **Symptom**: The 'login as console session' option may not be saved. **Condition**: Occurs when a new RDP5 bookmark is created and the 'login as console session' option is selected.
- **51639**: **Symptom**: Mac NetExtender may not delete old routing table entries. **Condition**: Occurs when a NetExtender is disconnected and client routes that were added to the routing table should be removed.
- **51837**: **Symptom**: Linux NetExtender may be unable to establish a connection. **Condition**: Occurs when used by a non-administrator user.
- **51712**: **Symptom**: Linux and Mac NetExtender saved profiles may not save passwords. **Condition**: Occurs when a profile is created using NetExtender.

Resolved Issues

This section contains a list of resolved issues in the SonicWALL SSL VPN 2.5 release.

- **47464**: **Symptom**: SonicWALL SSL-VPN Portal sites can be listed by search engines. **Condition**: Occurs when a webcrawler, spider, or bot hits the Portal site's FQDN.
- **51454**: **Symptom**: Windows NetExtender may encounter the error "Failed to install NetExtender, the installation has been rolled back" while installing. **Condition**: Occurs when NetExtender is installed on a system whose operating system runs on a non-default drive.
- **50705**: **Symptom**: Files in an FTP session may be deleted without warning. **Condition**: Occurs when files are checked before clicking the "Go To Directory" or "Create New Folder" buttons.
- **50327**: **Symptom**: Logging into a group that has a Radius filter-id set may fail. **Condition**: Occurs when the Radius server sends vendor specific attribute before filter.
- **49902**: **Symptom**: NetExtender Installation may fail on Windows 2003 Server. **Condition**: Occurs when Windows 2003 Server runs with Terminal Services in Application Mode.

Upgrading SonicWALL SSL VPN Software Procedures

The following procedures are for upgrading an existing SonicWALL SSL VPN image to a newer version.

- OBTAINING THE LATEST SONICWALL SSL VPN IMAGE VERSION
- EXPORTING A COPY OF YOUR CONFIGURATION SETTINGS
- UPLOADING A NEW SONICWALL SSL VPN IMAGE
- RESETTING THE SONICWALL SSL VPN 2000 OR 4000 USING SAFEMODE

Obtaining the Latest SonicWALL SSL VPN Image Version

1. To obtain a new SonicWALL SSL VPN image file for your SonicWALL security appliance, connect to your mysonicwall.com account at <http://www.mysonicwall.com>.

   Note: *If you have already registered your SonicWALL SSL VPN appliance, and you selected* ***Notify me when new firmware is available*** *on the* ***System > Settings*** *page, you are automatically notified of any updates available for your model.*

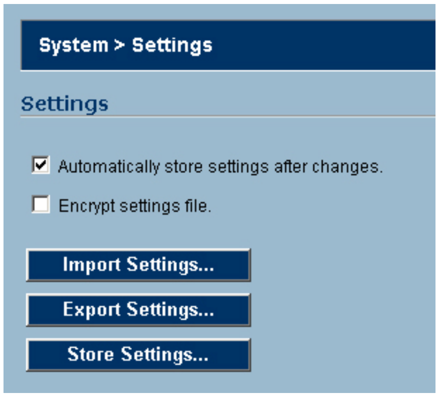
2. Copy the new SonicWALL SSL VPN image file to a directory on your management station.

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your SonicWALL SSL VPN appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your SonicWALL SSL VPN appliance, protecting all your existing settings in the event it becomes necessary to return to a previous configuration state.

Perform the following procedures to save a copy of your configuration settings and export them to a file on your local management station:

1. Click the **Export Settings . . .** button on the **System > Settings** page and save the settings file to your local machine. The default settings file is named *sslvpnSettings.zip*.



☑ Automatically store settings after changes.

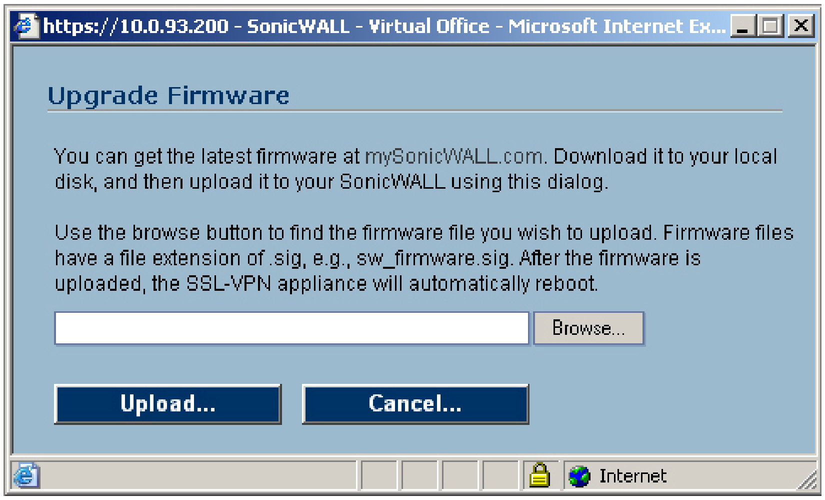
☐ Encrypt settings file.

Tip: To more easily restore settings in the future, rename the .zip file to include the version of the SonicWALL SSL VPN image from which you are exporting the settings.

Uploading a New SonicWALL SSL VPN Image

Note: *SonicWALL SSL VPN appliances do not support downgrading an image and using the configuration settings file from a higher version. If you are downgrading to a previous version of a SonicWALL SSL VPN image, you must select* ***Uploaded Firmware with Factory Defaults – New!*** ☞*. You can then import a settings file previously saved from the downgrade version or reconfigure manually.*

1. Download the SonicWALL SSL VPN image file from www.mysonicwall.com and save it to a location on your local computer.
2. Select **Upload New Firmware** from the **System > Settings** page. Browse to the location where you saved the SonicWALL SSL VPN image file, select the file, and click the **Upload** button. The upload process can take up to one minute.


https://10.0.93.200 - SonicWALL - Virtual Office - Microsoft Internet Ex...
Browse...
Upload...
Cancel...
Internet

Upgrade Firmware

You can get the latest firmware at mySonicWALL.com. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Use the browse button to find the firmware file you wish to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig. After the firmware is uploaded, the SSL-VPN appliance will automatically reboot.

3. When the upload is complete, you are ready to reboot your SonicWALL SSL VPN appliance with the new SonicWALL SSL VPN image. You can either reboot the SonicWALL SSL VPN appliance with the current settings or with the factory default settings:

   a. To reboot the image with current preference, click the boot icon for the following entry: **Uploaded Firmware – New!** ☞

   b. To reboot the image with factory default settings, click the boot icon for the following entry: **Uploaded Firmware with Factory Defaults – New!** ☞

   Note: *Be sure to save a backup of your current configuration settings to your local machine before rebooting the SonicWALL SSL VPN appliance with factory default settings, as described in the previous "Saving a Backup Copy of Your Configuration Settings" section.*

4. A warning message dialog is displayed saying **Are you sure you wish to boot this firmware? Click OK to proceed**. After clicking OK, do not power off the device while the image is being uploaded to the flash memory.
5. After successfully uploading the image to your SonicWALL SSL VPN appliance, the login screen is displayed. The updated image information is displayed on the **System > Settings** page.

Resetting the SonicWALL SSL VPN 2000 or 4000 Using SafeMode

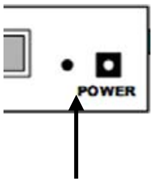
If you are unable to connect to the SonicWALL security appliance’s management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.200.0/24 subnet, such as 192.168.200.20.

   Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*

2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is in a small hole next to the power supply.

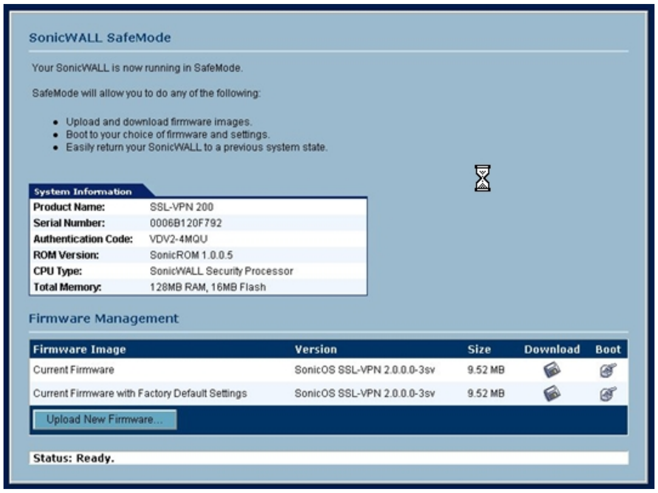
   

   Reset Button – SSL VPN

   Tip: *If this procedure does not work while the power is on, turn the unit off and on while holding the reset button until the Test light starts blinking.*

   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

3. Connect to the management interface: Point the Web browser on your management station to **http://192.168.200.1**. The SafeMode management interface displays.

   SonicWALL SafeMode

   Your SonicWALL is now running in SafeMode.

   SafeMode will allow you to do any of the following:

   - Upload and download firmware images.
   - Boot to your choice of firmware and settings.
   - Easily return your SonicWALL to a previous system state.

   System Information

Product Name:	SSL-VPN 200
Serial Number:	0006B120F792
Authentication Code:	VDV2-4MQU
ROM Version:	SonicROM 1.0.0.5
CPU Type:	SonicWALL Security Processor
Total Memory:	128MB RAM, 16MB Flash

   Firmware Management

Firmware Image	Version	Size	Download	Boot
Current Firmware	SonicOS SSL-VPN 2.0.0.0-3sv	9.52 MB		
Current Firmware with Factory Default Settings	SonicOS SSL-VPN 2.0.0.0-3sv	9.52 MB		

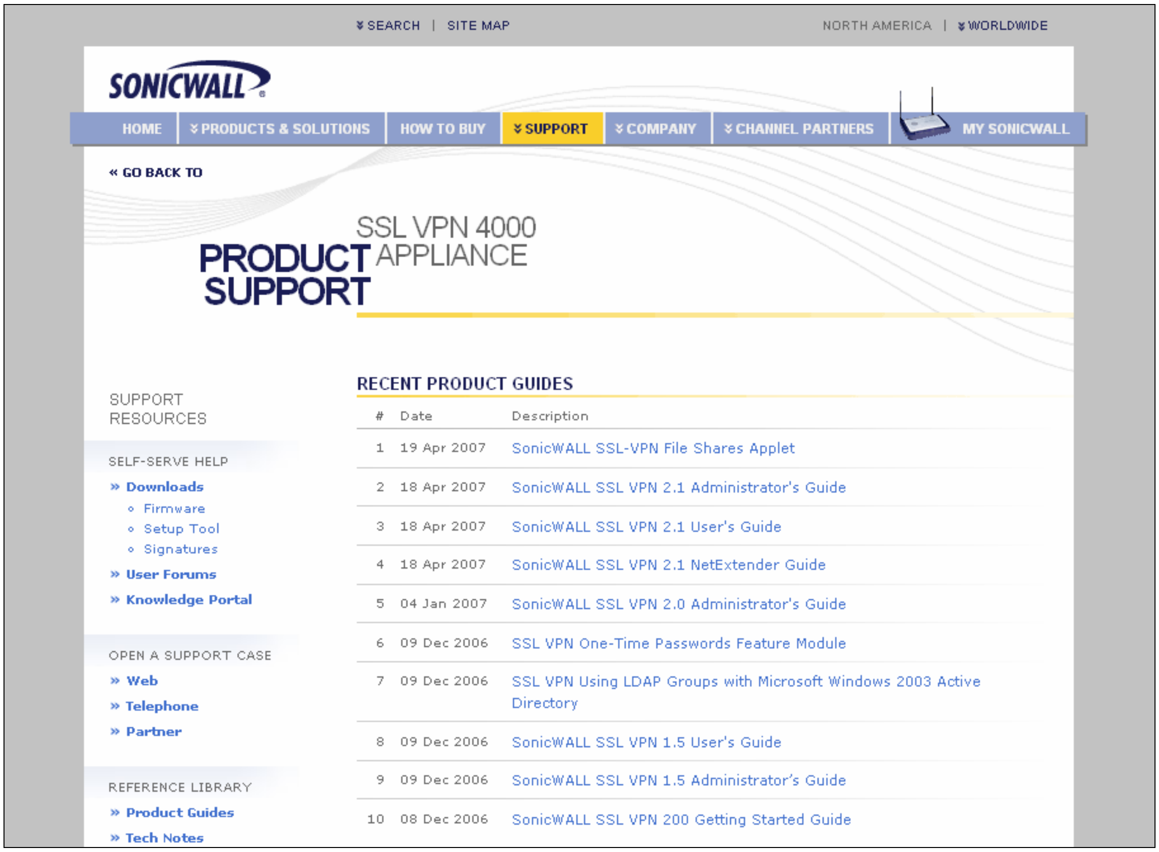
   Status: Ready.

4. Try rebooting the SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.

5. After the SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the reset button to restart the appliance in SafeMode again. In SafeMode, restart the SonicOS SSL VPN image with the factory default settings. Click the boot icon in the same line with **Current Firmware with Factory Default Settings**.

Related Technical Documentation

This section contains a list of technical documentation available on the SonicWALL Technical Documentation Online Library located at:
http://www.sonicwall.com/support/documentation.html



RECENT PRODUCT GUIDES

#	Date	Description
1	19 Apr 2007	SonicWALL SSL-VPN File Shares Applet
2	18 Apr 2007	SonicWALL SSL VPN 2.1 Administrator's Guide
3	18 Apr 2007	SonicWALL SSL VPN 2.1 User's Guide
4	18 Apr 2007	SonicWALL SSL VPN 2.1 NetExtender Guide
5	04 Jan 2007	SonicWALL SSL VPN 2.0 Administrator's Guide
6	09 Dec 2006	SSL VPN One-Time Passwords Feature Module
7	09 Dec 2006	SSL VPN Using LDAP Groups with Microsoft Windows 2003 Active Directory
8	09 Dec 2006	SonicWALL SSL VPN 1.5 User's Guide
9	09 Dec 2006	SonicWALL SSL VPN 1.5 Administrator's Guide
10	08 Dec 2006	SonicWALL SSL VPN 200 Getting Started Guide

The SonicWALL SSL VPN 2000 and 4000 appliances include the following reference guides:

- *SonicWALL SSL VPN 2000 Getting Started Guide*
- *SonicWALL SSL VPN 4000 Getting Started Guide*
- *SonicOS SSL VPN 2.1 Administrator’s Guide*
- *SonicOS SSL VPN 2.1 User’s Guide*
- *SonicWALL Secure Wireless Integrated Solutions Guide*
- *Advanced Deployment Technotes*

Last updated: 9/14/2007