

SonicWALL SSL-VPN 2000/4000 2.1 Early Field Trial Release Notes

SonicWALL, Inc.
February 5, 2007

Contents

Platform Compatibility
New Features
Known Issues
Resolved Known Issues
Upgrading SonicWALL SSL-VPN Software Procedures
Related Technical Documentation

Platform Compatibility

The SonicWALL SSL-VPN 2.1 release is supported on the following platforms:

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

New Features

The following features are introduced in the SonicWALL SSL-VPN 2000/4000 2.1 release:

- **File Shares Java Applet**—The File Shares Java Applet is a Java Virtual Machine (JVM) Web browser plug-in for remote users that provides improved navigation when using File Shares to access to shared network resources. Using the File Shares Java Applet, files and folders can be moved by drag-and-drop and multiple files and folders can be transferred with a single command. From the SSL-VPN portal, select HTML or Java File Shares application to launch by default.
- **LDAP Multiple Organizational Unit (OU) support**—Provides LDAP authentication capability for multiple organizational units (OUs) using multiple base distinguished names (baseDNs), including authentication of LDAP accounts in nested sub-OUs without additional configuration. Additionally, users can login as an LDAP user with a common name (CN) or user ID (UID), rather than a DN.
- **Active Directory (AD) Group support**—Provides access control based on existing AD group memberships. If a SonicWALL SSL-VPN group has one or more AD groups associated with it, only users from the associated AD groups will have access to that SSL-VPN group. SonicWALL SSL-VPN groups that are not associated with AD group(s) can be accessed by any user from the AD domain. By creating an “SSL-VPN User” group on the AD server and configuring the SonicWALL SSL-VPN to only accept members from that group, administrators can effectively limit SSL-VPN logins to specific AD users.
- **RADIUS Filter-ID Group support**—Provides access control based on existing RADIUS group memberships using the RADIUS Filter-ID attribute. If a SonicWALL SSL-VPN group has one or more RADIUS groups associated with it, only users from the associated RADIUS groups will have access to the SonicWALL group. SonicWALL SSL-VPN groups that are not associated with RADIUS groups can be accessed by any user from the RADIUS domain.

- **Support for GMS/ViewPoint Reporting**—SonicWALL SSL-VPN will support GMS and ViewPoint 4.1, which will be available later in 2007, by routing Syslog messages to a ViewPoint server for reporting and monitoring. Events that trigger a Syslog delivery to the server include: Reverse proxy, NetExtender, RDP, VNC, FTP, SSH/SSHv2, Telnet, export diagnostics, export config file, restart, and restore defaults.
- **ViewPoint manual key licensing requirements**—The SonicWALL SSL-VPN 2000 appliance requires the purchase and manual entry of a key in order to enable ViewPoint functionality. Support will be for ViewPoint 4.1, which will be available later in 2007.
- **NetExtender enhancements**—There are numerous enhancements to NetExtender in the SonicWALL SSL-VPN 2.1 release, including:
 - MSI stand-alone installer that allows NetExtender to be deployed through Windows Active Directory, supporting Windows 2000, XP, 2003 and Vista platforms with the Windows installer service installed
 - NT domain logon script support in NetExtender standalone client
 - Re-worded disconnect message in NetExtender standalone client
 - Option to enable auto-reconnect feature in NetExtender standalone client
 - Support for proxy servers using HTTPS and secure proxy server forwarding
 - Various performance improvements, including cleaned up lock files, deletion of policies upon disconnect, and removal of the netExtenderLog utility
 - Classful subnet route removed by the NetExtender client after the client connects
 - NetExtender does not re-launch with homepage CGI reloads
 - Full compatibility with Windows Vista. When launched from the portal, select the option to “run as administrator” and ensure that protected mode is turned off.
 - Improved reconnection after a break in network connection: If the IP pool is exhausted, the old connection is killed and the IP address from that connection is reused
 - When NetExender is launched from a portal session, the portal timeout will only count down when there is no traffic across the NetExtender tunnel
 - When NetExtender is launched from the portal, upon user logout using the Logout button or user logout by the administrator, the NetExtender session is also logged out
 - Server-level control of user name and password storage in NetExtender standalone client, allowing users to save user name and password if the server allows
 - New administrator configuration options, including automatically exiting the NetExtender client after disconnect, forcing an uninstall of the client after exit, creating a client connection profile, and controlling username and password caching options
 - Global tunnel-all control with added ability for user-level settings to inherit group and global tunnel-all settings

- **Reverse Proxy enhancements**—HTTP(S) reverse proxy now supports Windows SharePoint Services 2.0, a Web portal management tool. All features in Windows SharePoint Services are supported except those that require integration with the client program.
- **Variable HTTP(S) and CIFS Bookmark settings**—Provides the option to create a single bookmark that allows multiple users to access paths that have variable usernames in them by creating a bookmark with the case-sensitive variable %USERNAME%, where %USERNAME% is replaced with the current user's username. For example, if an administrator creates a bookmark named %USERNAME%'s Home with a link to \\1.2.3.4\&USERNAME%, a user (with access to the bookmark under policy) who logs in with the username BSmith will see a bookmark named BSmith's Home that links to \\1.2.3.4\BSmith. This variable can also be used for CIFS access policies.
- **RDP ActiveX enhancements**—RDP ActiveX enhancements include RDP6 support, encryption for sensitive parameters, proxy support that includes HTTPS proxy and automatic use of Internet Explorer proxy settings, and RDP5 ActiveX bookmarks that now work with custom ports.
- **SSHv2 Applet enhancements**—SSHv2 Applet enhancements include a status bar that displays SSHv2 activity, an option to automatically accept a server host key to more efficiently connect to a trusted server, and an option to bypass the username requirement for SSHv2 servers without authentication.
- **New diagnostic utilities**—DNS lookup and Traceroute diagnostic utilities have been added to the management interface under **System > Diagnostics**.
- **RADIUS Domain authentication support**—Added support for the following RADIUS Domain authentication methods: PAP, CHAP, MSCHAP, MSCHAPV2.
- **Additional enhancements**—Additional enhancements in the SSL-VPN 2.1 release include:
 - Administrator control over local users' ability to change password
 - Support for changing passwords for LDAP domains
 - For Active Directory users, new error message if appliance clock is not in sync with the AD server
 - Support for longer filenames in FTP

Known Issues

This section contains a list of known issues in the SonicWALL SSL-VPN 2000/4000 2.1 release.

- **43379: Symptom:** Digest access authentication fails with IIS 6.0 and the SSL-VPN security appliance. **Condition:** Occurs when access to a Web server running IIS 6.0 is set to use digest authentication, and a reverse proxy bookmark on the SSL-VPN is used to reach the Web server. **Workaround:** For servers using IIS 6.0, reconfigure the server to use basic or anonymous HTTP authentication. Alternatively, run IIS 5.0 or Apache on the Web server, either of which work with digest authentication through the SSL-VPN.
- **47266: Symptom:** A NetExtender session launched from the portal does not connect when using a proxy server with authentication. If no authentication is configured for the proxy server, the NetExtender user interface does not display until the portal window is closed. **Condition:** Occurs when using a proxy server with or without authentication configured.

Resolved Known Issues

The following issues are resolved in the SonicWALL SSL-VPN 2000/4000 2.1 release:

- **41861: Symptom:** The SSL-VPN security appliance does not authenticate user accounts in some instances. **Condition:** Occurs when the user account is defined within a nested organizational unit (sub-OU) and LDAP is used for authentication. **Workaround:** Configure a domain for each OU, including each sub-OU.
- **44868: Symptom:** Users see a blank Web page when trying to access a Sharepoint portal through the SSL-VPN security appliance. **Condition:** Occurs when an HTTP bookmark to the Sharepoint portal is created on the SSL-VPN appliance, and the user selects the bookmark to access Sharepoint. **Workaround:** Instead of using the bookmark, click NetExtender on the SSL-VPN screen to access the internal network, and then use a local Web browser to access the Sharepoint portal.
- **46012: Symptom:** Portal home page and login message files cannot be deleted from the SSL-VPN security appliance after loading a configuration without the portal. **Condition:** Occurs when you create a portal layout on the appliance, and then import a configuration that does not contain the portal. The LoginMessage.txt, HomeMessage.txt, and HomeInclude.html files for the portal cannot be deleted because the portal is gone. **Workaround:** Create another portal layout with the same name as the missing one, and then delete it. The files are deleted when the portal layout is deleted.
- **46028: Symptom:** CIFS Access Policy can fail to block access. **Condition:** Occurs when a CIFS bookmark is created, and then a CIFS access policy is created that denies access to the file share that is bookmarked.
- **46881: Symptom:** CIFS and HTTP bookmark paths containing spaces disappear after the appliance is restarted. **Condition:** Occurs when a space is included in a CIFS or HTTP bookmark.
- **46533: Symptom:** Delayed access to file shares when User policies are created to deny access to an IP address or an IP address range. **Condition:** Occurs when deny policies are created for an IP address or an IP address range and a simultaneous allow policy is created for an IP address or IP address range that is also included in the deny policy.


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
- ARCHIVING OTHER CRITICAL INFORMATION
- 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*. You can rename the file but you should keep the .zip filename.

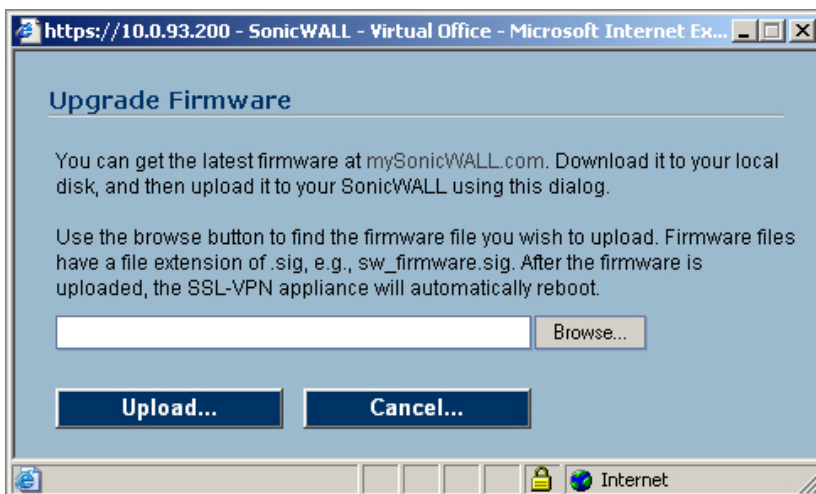




Tip: Rename the .zip file to include the version of the SonicWALL SSL-VPN image from which you are exporting the settings. For example, if you export the settings from the SonicWALL SSL-VPN 1.5.0.0 image, rename the file using the format: [date]_[version]_[mac].zip to "041606_SSL-VPN_1.5.0.0-19_0006B1223344.zip" (the [mac] format entry is the serial number of the SonicWALL security appliance). Then if you need to roll back to that version of the SonicWALL SSL-VPN image, you can choose the correct file to import.


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.



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.

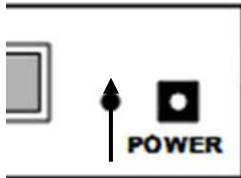
To reset the SonicWALL security appliance, perform the following steps:

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>

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*

Document version: February 5, 2007

Page 10 of 10

