Dell SonicWALL™ SonicOS 5.9 Upgrade Guide

April, 2015

This Upgrade Guide provides instructions for upgrading your Dell SonicWALL™ network security appliance to SonicOS 5.9 from a previous release.

This guide also provides information about importing the configuration settings from an appliance running SonicOS 5.8 or 5.9 to a different appliance. See Importing configuration settings for details about the models and firmware versions supported.

Topics:

- Obtaining the latest SonicOS firmware
- Creating a system backup and exporting your settings
- Upgrading firmware with current settings
- Upgrading firmware with factory default settings
- Using SafeMode to upgrade firmware
- Importing configuration settings

Obtaining the latest SonicOS firmware

To obtain a new SonicOS firmware image file for your Dell SonicWALL security appliance:

1 In a browser on your management computer, log into your MySonicWALL account at http://www.mysonicwall.com.

2 In MySonicWALL, click **Downloads** in the left navigation pane to display the Download Center screen.

3 Select your product in the **Software Type** drop-down list to display available firmware versions.

4 To download the firmware to your computer, click the link for the firmware version you want. You can download the Release Notes and other associated files in the same way.

Creating a system backup and exporting your settings

Create Backup

Before beginning the update process, you can use the **Create Backup** button to make a system backup on your Dell SonicWALL appliance.

On Dell SonicWALL NSA 2400 and above, the backup feature saves a copy of the current system state, firmware, and configuration settings on your appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

(i) **NOTE:** The TZ series, NSA 220 series, NSA 240, and NSA 250M series do not support a full firmware image backup.

Create Backup Settings

On TZ 105 series, TZ 205 series, NSA 220 series, NSA 240, and NSA 250M series, you can use the **Create Backup Settings** button to save a copy of the configuration settings locally on the firewall. The saved settings can be used with the current firmware version or with a newly uploaded firmware version.

(i) **NOTE:** The TZ 100 series and TZ 200 series do not support saving a copy of the settings directly on the unit.

Export Settings

On all appliance platforms, you can export the appliance configuration settings to a file on your local management station. This file serves as an external backup of the configuration settings, and can be imported into another appliance or into the same appliance if it is necessary to reboot the firmware with factory default settings.

To save a system backup on your appliance and export configuration settings to a file on your local management station:

1 To save a system backup or backup settings in the System > Settings page, do one of the following:

- On an NSA 2400 or above, click **Create Backup**. SonicOS takes a "snapshot" of your current system state, firmware, and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing System Backup image, if any. The System Backup entry is displayed in the Firmware Management table.

- On a TZ, NSA 220, NSA 240, or NSA 250M, click **Create Backup Settings**. SonicOS saves a small file on the appliance with all your configuration settings. Any previous backup settings file is overwritten. The Firmware Management table displays the **Current Firmware with Backup Settings** entry.

(i) **NOTE:** A Download button is displayed in the Firmware Management table for System Backup and for Current/Uploaded Firmware with Backup Settings. However, the downloaded files cannot be imported into another appliance, nor can they be uploaded like firmware. Use **Export Settings** to save your configuration settings for import into another appliance.

2 To export your settings to a local file, click **Export Settings** and then click **Export** in the popup window that displays the name of the saved file.

Upgrading firmware with current settings

You can update the SonicOS image on a Dell SonicWALL security appliance by connecting your computer to the LAN (X0) port or you can update it remotely if the LAN or WAN interface is configured for remote management access.

To upload new firmware to your Dell SonicWALL appliance and use your current configuration settings upon startup:

1 Download the SonicOS firmware image file from MySonicWALL and save it to a location on your local computer.

2 Point your browser to the appliance IP address, and log in as an administrator.

3 On the System > Settings page, click **Upload New Firmware**.

4 Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it is displayed in the Firmware Management table.

5 On the System > Settings page, click the Boot icon in the row for **Uploaded Firmware – New!**

6 In the confirmation dialog box, click **OK**. The appliance restarts and then displays the login page.

7 Enter your user name and password. Your new SonicOS image version information is displayed on the System > Status page.

Upgrading firmware with factory default settings

To upload new firmware to your Dell SonicWALL appliance and start it up using the default configuration:

1 Download the SonicOS firmware image file from MySonicWALL and save it to a location on your local computer.

2 Point your browser to the appliance IP address, and log in as an administrator.

3 Navigate to the System > Settings page and click **Upload New Firmware**.

4 Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.

5 On the System > Settings page, click the Boot icon in the row for **Uploaded Firmware with Factory Default Settings – New!**

6 In the confirmation dialog box, click **OK**. The appliance restarts and then displays the options to launch the Setup Wizard or go to the login page of the SonicOS management interface.

ⓘ **NOTE:** The IP address for the X0 (LAN) interface reverts to the default, 192.168.168.168. You can log into SonicOS by connecting to X0 and pointing your browser to https://192.168.168.168.

7 Enter the default user name and password (admin / password) to access the SonicOS management interface.

Using SafeMode to upgrade firmware

If you are unable to connect to the SonicOS management interface, you can restart the Dell 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.

The SafeMode procedure uses a recessed reset button in a small pinhole for which the location varies:

- On the NSA models, the button is near the USB ports on the front.

- On the TZ models, the button is next to the power connection on the back.

To use SafeMode to upgrade firmware on a Dell SonicWALL security appliance:

1 Connect your computer to the X0 port on the appliance and configure your computer with an IP address on the 192.168.168.0/24 subnet, such as 192.168.168.20.

2   Do one of the following to restart the appliance in SafeMode:

  - 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 more than 20 seconds.

  - On platforms with an LCD screen and control buttons on the front bezel, you can use the LCD control buttons to set the appliance to SafeMode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The Dell SonicWALL security appliance changes to SafeMode.

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

  ⓘ | **NOTE:** Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.

3   Point the browser on your computer to 192.168.168.168. The SafeMode management interface displays.

4   Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.

5   Click the Boot icon in the row for one of the following:

  - **Uploaded Firmware – New!**

    Use this option to restart the appliance with your current configuration settings.

  - **Uploaded Firmware with Factory Default Settings – New!**

    Use this option to restart the appliance with factory default configuration settings.

6   In the confirmation dialog box, click **OK** to proceed.

7   If you booted with current configuration settings, reconfigure your computer as needed to automatically obtain an IP address and DNS server address, or reset it to its normal static values.

8   Connect the computer to your network or leave it connected to the X0 (LAN) interface of the appliance, and point your browser to the WAN or LAN (depending on how you are connected) IP address of the Dell SonicWALL appliance.

9   After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicOS management interface. The default IP address of the X0 interface is 192.168.168.168.

Importing configuration settings

You can import configuration settings from one appliance to another, which can save a lot of time when replacing an older appliance with a newer model. This feature is also useful when you need multiple appliances with similar configuration settings.

Importing configuration settings, or preferences ("prefs"), to Dell SonicWALL network security appliances running SonicOS 5.9 is generally supported from the following Dell SonicWALL appliances:

  - NSA E-Class Series

  - NSA Series

  - TZ 215/210/205/105 Series

  - TZ 200/100/190/180/170 Series

  - PRO Series

Preferences cannot be imported in the following cases:

  - Settings for VPN Tunnel Interfaces with OSPF and RIP configurations in SonicOS 5.8 cannot be imported into SonicOS 5.9. These VPN Tunnel Interfaces are eliminated during the settings import.

  - Settings files containing Portshield interfaces created prior to SonicOS 5.0

- Settings files containing VLAN interfaces are not accepted by the TZ 100/200 Series firewalls

- Settings files from a PRO 5060 with optical fiber interfaces where VLAN interfaces have been created

To export the configuration settings from an appliance, navigate to the System > Settings page in SonicOS and click the **Export Settings** button. You can then import the settings file to another appliance by clicking the **Import Settings** button on that page.

> ⓘ **NOTE:** Importing settings from SonicOS 5.8 to 5.9 on some platforms eliminates all OSPF and RIP configurations created over VPN tunnel interfaces. After upgrading to 5.9 and importing the 5.8 settings, the VPN tunnel interfaces used for OSPF and RIP are missing.
>
> Occurs when SonicOS does not automatically convert unnumbered tunnel interface configurations to numbered tunnel interface configurations. Numbered and unnumbered tunnel interface implementations are mutually exclusive in SonicOS 5.9.x.x, so if numbered tunnel interfaces are supported on a device, unnumbered tunnel interfaces are NOT supported on that device and vice versa.
>
> | Numbered Tunnel Interfaces Supported | Unnumbered Tunnel Interfaces Supported | No Tunnel Interfaces Supported |
> |---|---|---|
> | NSA E8510 | NSA 2400MX | TZ 200/200W |
> | NSA E8500 | TZ 210/210W | TZ 100/100W |
> | NSA E7500 | TZ 205/205W | |
> | NSA E6500 | TZ 105/105W | |
> | NSA E5500 | | |
> | NSA 5000 | | |
> | NSA 4500 | | |
> | NSA 3500 | | |
> | NSA 2400 | | |
> | NSA 250M/250MW | | |
> | NSA 240 | | |
> | NSA 220/220W | | |
> | TZ 215/215W | | |
>
> **Workaround**: Manually reconfigure VPN tunnel interfaces and routing settings in SonicOS 5.9 after importing settings from SonicOS 5.8.

See the related topics and import matrices in the following sections:

- Importing settings from SonicOS Standard to SonicOS 5.9 Enhanced

- SonicOS versions supporting configuration import

- SOHO configuration import support

- NSA / E-Class NSA configuration import support

- TZ / NSA configuration import support

- PRO / TZ configuration import support

Importing settings from SonicOS Standard to SonicOS 5.9 Enhanced

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target appliance running SonicOS Enhanced, such as SonicOS 5.9. Due to the more advanced nature of SonicOS Enhanced, its Network Settings file is more complex than the one SonicOS Standard uses. They are not compatible. The Settings Converter creates an entirely new target Enhanced Network Settings file based on the network settings found in the source Standard file. This allows for a rapid upgrade from a Standard deployment to an Enhanced one with no time wasted in re-creating network policies.

(i) NOTE: Dell SonicWALL recommends deploying the converted target Network Settings file in a testing environment first and always keeping a backup copy of the original source Network Settings file.

The SonicOS Standard to Enhanced Settings Converter is available at:
https://convert.global.sonicwall.com/

If the preferences conversion fails, email your SonicOS Standard configuration file to settings_converter@sonicwall.com with a short description of the problem. In this case, you may also consider manually configuring your Dell SonicWALL appliance.

To convert a Standard Network Settings file to an Enhanced one:

1 Log in to the management interface of your SonicOS Standard appliance, navigate to System > Settings, and export your network settings to a file on your management computer.

2 On the management computer, point your browser to https://convert.global.sonicwall.com/.

3 Click the **Settings Converter** button.

4 Log in using your MySonicWALL credentials and agree to the security statement.

   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that Dell SonicWALL will retain a copy of their network settings after the conversion process is complete.

5 Upload the source Standard Network Settings file:

   • Click **Browse**.

   • Navigate to and select the source SonicOS Standard Settings file.

   • Click **Upload**.

   • Click the right arrow to proceed.

6 Review the source SonicOS Standard Settings Summary page.

   This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.

   • (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.

   • Click the right arrow to proceed.

7 Select the target Dell SonicWALL appliance for the Enhanced deployment from the available list.

   SonicOS Enhanced is configured differently on various Dell SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.

8 Complete the conversion by clicking the right arrow to proceed.

9 Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.

10 Click the **Download** button, select **Save to Disk**, and click **OK** to save the new target SonicOS Enhanced Network Settings file to your management computer.

11 Log in to the management interface for your Dell SonicWALL appliance.

12 Navigate to System > Settings, and click the **Import Settings** button to import the converted settings to your appliance.

SonicOS versions supporting configuration import

The following matrix illustrates the supported source and destination versions of SonicOS when importing configuration settings from one appliance to another. As the matrix shows, it is not supported to import configuration settings from an appliance running SonicOS 6.x to one running SonicOS 5.9.

(i) NOTE: For information about importing settings from SonicOS 5.9 to SonicOS 6.2, see the *SonicOS 6.2 Upgrade Guide*, available on https://mysonicwall.com or on any of the Support pages for Dell SonicWALL platforms that run SonicOS 6.2. You can access these Support pages from https://support.software.dell.com/release-notes-product-select.

SonicOS Configuration Import/Export Support

		To				
		5.8 (Min. 5.8.1.12)	**5.9**	**6.1.1.x**	**6.1.2.x**	**6.2**
From	**5.8** (Min. 5.8.1.12)	Y	Y	Y	Y	Y
	5.9	N	Y	N	N	Y (Min. 5.9.0.4)
	6.1.1.x	N	N	Y	Y	Y
	6.1.2.x	N	N	Y	Y	Y
	6.2	N	N	N	N	Y

If answer is "Y" above, please look in below table for your specific products
If answer is "N" above, this configuration upgrade is not supported

Legend

This legend defines the letter-codes used in the tables below.

Y	Supported
N	Unsupported. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.
B	Portshield interfaces prior to SonicOS 5.x are not supported.
C	Configuration information from extra interfaces will be removed. NAT policies, Firewall access rules and other interface-dependent configuration will also be removed.
D	When importing from non-SonicOS 5.x devices, the X2 interface will be configured in the DMZ zone.
E	VLANs created as sub-interfaces of the fiber interfaces will be renamed.

SOHO configuration import support

The following matrix shows the Dell SonicWALL firewalls whose configuration settings can be imported to Dell SonicWALL SOHO platform. The source firewalls are in the left column, and the destination firewalls are listed across the top.

DESTINATION

		SOHO
S	TZ 100 / TZ 200	Y
O	TZ 100W / TZ 200W	C
U	TZ 105 / TZ 205	Y
R	TZ 105W / TZ 205W	C
C	TZ 210	C
E	TZ 210W	C
	TZ 215	C
F	TZ 215W	C
I	NSA 220	N
R	NSA 220W	N
E	NSA 240	N
W	NSA 250M	N
A	NSA 250MW	N
L	NSA 2400	N
L	NSA 2400MX	N
S	NSA 3500	N
	NSA 4500	N
	NSA 5000	N
	NSA E5500	N
	NSA E6500	N
	NSA E7500	N
	NSA E8500	N
	NSA E8510	N

NSA / E-Class NSA configuration import support

The following matrix shows the Dell SonicWALL firewalls whose configuration settings can be imported to Dell SonicWALL NSA and E-Class NSA platforms. The source firewalls are in the left column, and the destination firewalls are listed across the top.

DESTINATION FIREWALLS

	NSA 2400	NSA 2400MX	NSA 3500	NSA 4500	NSA 5000	NSA E5500	NSA E6500	NSA E7500	NSA E8500	NSA E8510
PRO 1260	N	N	N	N	N	N	N	N	N	N
PRO 2040	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PRO 3060	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PRO 4060	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PRO 4100	C	Y	C	C	C	C	C	C	C	C
PRO 5060	C,E	E	C,E	C,E	C,E	C,E	C,E	C,E	C,E	C,E
TZ 170	N	N	N	N	N	N	N	N	N	N
TZ 170W	N	N	N	N	N	N	N	N	N	N
TZ 170SP	N	N	N	N	N	N	N	N	N	N
TZ 170SPW	N	N	N	N	N	N	N	N	N	N
TZ 180	N	N	N	N	N	N	N	N	N	N
TZ 180W	N	N	N	N	N	N	N	N	N	N
TZ 190	N	N	N	N	N	N	N	N	N	N
TZ 190W	N	N	N	N	N	N	N	N	N	N
TZ 100/TZ 200	N	N	N	N	N	N	N	N	N	N
TZ 100W/TZ 200W	N	N	N	N	N	N	N	N	N	N
TZ 105/TZ 205	N	N	N	N	N	N	N	N	N	N
TZ 105W/TZ 205W	N	N	N	N	N	N	N	N	N	N
TZ 210	N	N	N	N	N	N	N	N	N	N
TZ 210W	N	N	N	N	N	N	N	N	N	N
TZ 215	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TZ 215W	N	N	N	N	N	N	N	N	N	N
NSA 220	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NSA 220W	N	N	N	N	N	N	N	N	N	N
NSA 240	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NSA 250M	N	N	N	N	N	N	N	N	N	N
NSA 250MW	N	N	N	N	N	N	N	N	N	N
NSA 2400	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NSA 2400MX	C	Y	C	C	C	C	C	C	C	C
NSA 3500	C	Y	Y	Y	Y	Y	Y	Y	Y	Y
NSA 4500	C	Y	Y	Y	Y	Y	Y	Y	Y	Y
NSA 5000	C	Y	C	C	Y	Y	Y	Y	Y	Y
NSA E5500	C	Y	C	C	C	Y	Y	Y	Y	C
NSA E6500	C	Y	C	C	C	Y	Y	Y	Y	C
NSA E7500	C	Y	C	C	C	Y	Y	Y	Y	C
NSA E8500	C	Y	C	C	C	Y	Y	Y	Y	C
NSA E8510	Y	Y	Y	Y	Y	C	C	C	C	Y

(Left margin label: SOURCE FIREWALLS)

TZ / NSA configuration import support

The following matrix shows the Dell SonicWALL firewalls whose configuration settings can be imported to Dell SonicWALL TZ 100/200/105/205/210/215 series and NSA 220/240/250M series platforms. The source firewalls are in the left column, and the destination firewalls are listed across the top.

DESTINATION FIREWALLS

	TZ100/ TZ200	TZ100w/ TZ200w	TZ105/ TZ205	TZ105w/ TZ205w	TZ210	TZ210w	TZ215	TZ215w	NSA 220	NSA 220W	NSA 240	NSA 250M	NSA 250MW
PRO 1260	B,D	B,D	B,D	B,D	B,D	B,D	B,D	B,D	N	N	B,D	N	N
PRO 2040	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 3060	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 4060	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 4100	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 5060	N	N	N	N	N	N	N	N	N	N	C,E	N	N
TZ 170	B,D	B,D	B,D	B,D	B,D	B,D	B,D	B,D	N	N	B,C,D	N	N
TZ 170W	B,C,D	B,D	B,C,D	B,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
TZ 170SP	B,C,D	B,C,D	B,C,D	B,C,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
TZ 170SPW	C,D	B,C,D	C,D	B,C,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
TZ 180	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,D	N	N
TZ 180W	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,C,D	N	N
TZ 190	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,D	N	N
TZ 190W	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,C,D	N	N
TZ 100/TZ 200	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TZ 100W/TZ 200W	C	Y	C	Y	C	Y	C	Y	N	N	Y	N	Y
TZ 105/TZ 205	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TZ 105W/TZ 205W	C	Y	C	Y	C	Y	C	Y	N	N	Y	N	Y
TZ 210	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
TZ 210W	C	Y	C	Y	C	Y	C	Y	C	Y	Y	N	N
TZ 215	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
TZ 215W	C	Y	C	Y	C	Y	C	Y	C	Y	N	N	N
NSA 220	N	N	N	N	N	N	N	N	Y	Y	Y	N	N
NSA 220W	N	N	N	N	N	N	N	N	C	Y	N	N	N
NSA 240	N	N	N	N	N	N	N	N	N	N	Y	C	C
NSA 250M	N	N	N	N	N	N	N	N	N	N	N	Y	Y
NSA 250MW	N	N	N	N	N	N	N	N	N	N	N	N	Y
NSA 2400	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA 2400MX	N	N	N	N	N	N	N	N	C	C	C	C	C
NSA 3500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA 4500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA 5000	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E5500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E6500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E7500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E8500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E8510	N	N	N	N	N	N	N	N	C	N	Y	N	N

(Left vertical label: SOURCE FIREWALLS)

PRO / TZ configuration import support

The following matrix shows the Dell SonicWALL firewalls whose configuration settings can be imported to Dell SonicWALL PRO and older TZ platforms. These legacy appliances do not run SonicOS 5.9, but are listed here for reference. The source firewalls are in the left column, and the destination firewalls are listed across the top.

DESTINATION FIREWALLS

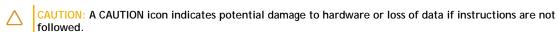|		PRO 1260	PRO 2040	PRO 3060	PRO 4060	PRO 4100	PRO 5060	TZ 170	TZ 170W	TZ 170SP	TZ 170SPW	TZ 180	TZ 180W	TZ 190	TZ 190W
	PRO 1260	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 2040	N	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N
	PRO 3060	N	C	Y	Y	Y	Y	N	N	N	N	N	N	N	N
	PRO 4060	N	C	Y	Y	Y	Y	N	N	N	N	N	N	N	N
S	PRO 4100	N	C	C	C	Y	C	N	N	N	N	N	N	N	N
O	PRO 5060	N	C	C	C	C,E	Y	N	N	N	N	N	N	N	N
U	TZ 170	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
R	TZ 170W	Y	N	N	N	N	N	C	Y	Y	Y	C	Y	C	Y
C	TZ 170SP	C	N	N	N	N	N	C	C	Y	Y	C	C	Y	C
E	TZ 170SPW	C	N	N	N	N	N	C	C	C	Y	C	C	C	Y
	TZ 180	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
F	TZ 180W	C	N	N	N	N	N	C	Y	C	Y	C	Y	C	Y
I	TZ 190	C	N	N	N	N	N	C	C	Y	Y	C	C	Y	Y
R	TZ 190W	C	N	N	N	N	N	C	Y	C	Y	C	Y	C	Y
E	TZ 100/TZ 200	N	N	N	N	N	N	N	N	N	N	N	N	N	N
W	TZ 100W/TZ 200W	N	N	N	N	N	N	N	N	N	N	N	N	N	N
A	TZ 105/TZ 205	N	N	N	N	N	N	N	N	N	N	N	N	N	N
L	TZ 105W/TZ 205W	N	N	N	N	N	N	N	N	N	N	N	N	N	N
L	TZ 210	N	N	N	N	N	N	N	N	N	N	N	N	N	N
S	TZ 210W	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	TZ 215	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	TZ 215W	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 220	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 220W	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 240	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 250M	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 250MW	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 2400	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 2400MX	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 3500	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 4500	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA 5000	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA E5500	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA E6500	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA E7500	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA E8500	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	NSA E8510	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Patents

For more information about applicable patents, refer to http://software.dell.com/legal/patents.aspx.

Trademarks
Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

⚠ **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

ⓘ **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

_____