

Mandatory SonicOS firmware upgrade for your firewall.

1024-bit certificates expire December 31, 2013

Issue Summary

In the past, Dell SonicWALL used industry standard 1024-bit certificates. To comply with Certification Authority/Browser forum requirements based on NIST Special Publication 800-131A, as of January 1, 2014, all web browsers and Certification Authorities (CAs) will no longer sell or support 1024-bit RSA certificates. Certificates with less than 2048-bit key length will need to be revoked and replaced with certificates of higher encryption strength. All current Dell SonicWALL firewalls use versions of SonicOS firmware with the 2048-bit security standard. Recent updates and upgrades of SonicOS firmware use the industry standard and recommended 2048-bit certificate. This is an urgent notification that on January 1, 2014, all web browsers and Certification Authorities (CAs) will no longer support 1024-bit RSA certificates. This change is not driven by Dell SonicWALL, but rather a decision by Certificate Authorities to enforce the use of highly secure certificates. Certificates using the 1024-bit key length will be revoked and must be replaced with certificates of higher encryption strength. If you own a Dell SonicWALL firewall with an older firmware version that does not use 2048-bit certificates you must upgrade the firmware to the latest version or the minimum General Release version which includes the 2048-bit certificate as listed in the Firmware Upgrade Table below by December 31, 2013. Dell SonicWALL is providing the minimum firmware upgrade to all customers regardless of support contract status.

How does this issue affect me?

If you own a Dell SonicWALL firewall with an older firmware version that does not support 2048-bit certificates, the firewall will NOT be able to get real-time license information or the latest security services updates from our back-end systems. Existing security services on Dell SonicWALL firewalls that use 1024-bit certificates will continue to block previously-known threats, but the lack of updates may expose the protected network to new threats and exploits. In addition, you will NOT be able to activate and renew security services.

How can I tell what firmware version is running on my firewall?

Follow these steps to find the firmware version running on your Dell SonicWALL firewall.

1. Log into your Dell SonicWALL firewall
2. Click on "System" in the left-hand navigation
3. Look for "Firmware Version" under the "System Information" heading

What actions do I need to take?

Dell SonicWALL strongly recommends upgrading firewalls running older firmware to the minimum General Release version indicated in the table below. The table lists the affected Dell SonicWALL products and the associated minimum required firmware versions. All General Release versions of the required minimum SonicOS version for your appliance(s) are available on MySonicWALL.com.

Note: Active support is not required to download the minimum General Release version of the firmware listed in the Firmware Upgrade Table below.

When do I need to do this by?

If you have a Dell SonicWALL firewall that does not support 2048-bit certificates you must upgrade the firmware on the firewall by December 31, 2013.

How do I upgrade the firmware on my firewall?

Firmware must be upgraded on your Dell SonicWALL firewall(s) to the latest firmware version or the minimum firmware version as listed in the Firmware Upgrade Table below. The latest or minimum required General Release firmware can be downloaded from the [MySonicWALL.com Download Center](#). The following Knowledge Base articles will guide you through the processes for downloading and upgrading the firmware on your firewall.

[How to Download SonicOS Firmware](#)

[How to Upgrade SonicOS Firmware with Current Preferences on a Dell SonicWALL Firewall](#)

[Upgrading Firmware Using GMS](#)

What firmware version do I need to upgrade to?

Follow these steps to determine the required firmware version for your Dell SonicWALL firewall.

1. Find your firewall model under the "Dell SonicWALL Firewall" column.
2. Determine if your firewall is running one of the versions listed under "Currently Running Firmware."
3. Check the "Minimum Required SonicOS Firmware Version" to see if an upgrade is required. If it is, you will need to upgrade to at least the minimum required version listed in the right-hand column of the table.

FIRMWARE UPGRADE TABLE

Dell SonicWALL Firewall	Current Running Firmware	Minimum Required SonicOS Firmware Version
NSA E5500/E6500/E7500/E8500/E8510 NSA 240/2400/3500/4500/5000 TZ 210/210W TZ 200/200W TZ 100/100W	5.3.x.x - 5.6.0.11 or older	5.6.0.12
	5.9.0.0 or newer	Upgrade not required
	5.8.1.0 or newer	Upgrade not required
	5.8.0.0 - 5.8.0.7	5.8.0.8
NSA 2400MX	5.7.0.0 - 5.7.1.0	5.7.2.0
	5.9.0.0 or newer	Upgrade not required
TZ 205/205W TZ 105/105W	5.8.0.0 - 5.8.1.5	5.8.1.6
	5.9.0.0 or newer	Upgrade not required
PRO 4060/4100/5060	4.2.1.6 Enhanced or older	4.2.1.7 Enhanced
PRO 2040/3060	4.2.1.6 Enhanced or older	4.2.1.7 Enhanced
	3.1.6.5 Standard or older	3.1.6.6 Standard
PRO 1260	3.4.1.3 Enhanced or older	3.4.1.4 Enhanced
	3.1.6.5 Standard or older	3.1.6.6 Standard

TZ 190/190W	4.2.1.6 Enhanced or older	4.2.1.7 Enhanced
TZ 180/180W	3.9.1.4 Standard or older	3.9.1.5 Standard
	4.2.1.6 Enhanced or older	4.2.1.7 Enhanced
TZ 170/170W/170 SP	3.4.1.3 Enhanced or older	3.4.1.4 Enhanced
	3.1.6.5 Standard or older	3.1.6.6 Standard
TZ 170 SPW	3.4.1.3 Enhanced or older	3.4.1.4 Enhanced
TZ 150/150W/150W Rev B	3.1.6.5 Standard or older	3.1.6.6 Standard
Product models not affected by this certificate issue include:		
<ul style="list-style-type: none"> • SuperMassive 9200/9400/9600 • NSA 2600/3600/4600/5600/6600 • NSA 250M/250MW • NSA 220/220W • TZ 215/215W 		
Legacy Dell SonicWALL firewalls are out of scope of this notification.		
<ul style="list-style-type: none"> • Gen3: http://www.sonicwall.com/downloads/Gen3_EOS_Public_Notification.pdf • Gen1 and Gen2: http://www.sonicwall.com/downloads/Gen1and2EOSPublicNotification.pdf 		

What happens if I don't upgrade the firmware on my Dell SonicWALL firewall?

If you do not upgrade the firmware to a version that does support 2048-bit certificates your Dell SonicWALL firewall will NOT be able to get real-time license information or the latest security services updates from our back-end systems. Existing security services on Dell SonicWALL firewalls that use 1024-bit certificates will continue to block previously-known threats, but the lack of updates may expose the protected network to new threats and exploits. In addition, you will NOT be able to activate and renew security services.

Where can I get more information?

If you have any questions or need additional information, please contact your local Dell SonicWALL reseller, Dell SonicWALL Sales Representative or send an email to Dell SonicWALL Technical Support at Customer_service@sonicwall.com with subject line: **"End of 1024 Certificate Support"**.

Who is NIST?

NIST stands for "National Institute of Standards and Technology" which is a U.S. federal government "technology agency that works with industry to develop and apply technology, measurements, and standards." NIST recommendations are part of the standards ecosystem by which web browsers and CAs abide.

Why is NIST recommending a transition to 2048-bit certificates?

In order to provide greater security against malicious attacks, NIST guidelines suggest discontinuing the use of 1024-bit certificates at the end of 2013. Browsers and Commercial CAs within the CA/Browser Forum have decided to abide by this recommendation and created steadfast rules to proactively convert end-users to higher levels of signing.