



## Dell SonicWALL Notice Concerning Multiple LDAP Vulnerabilities

Dell SonicWALL has identified multiple LDAP authentication protocol vulnerabilities exposed when SonicOS is configured to use Microsoft Active Directory / LDAP for authentication of AD/LDAP usernames who are members of SonicWALL Administrator groups.

 **Note:** SonicOS configurations utilizing *User > Settings* authentication methods *Local Users*, *RADIUS*, *RADIUS + Local Users*, are NOT exposed to LDAP protocol vulnerabilities.

The exposure is limited to SonicOS configurations utilizing Active Directory / LDAP for authentication of SonicWALL Administrator usernames, specifically:

- IF SonicOS *User > Settings* is configured to use LDAP authentication
- AND any LDAP usernames in Microsoft Active Directory /LDAP directories are members of SonicWALL Administrator groups (locally or in LDAP directories),
- THEN it is critical to immediately upgrade to the firmware versions listed in the table below OR to immediately apply the configuration remediation described below. The *SonicwallLDAPAdminUserChk.vbs* script (see below) can help diagnose configurations.

 **Note:** Many non-Microsoft LDAP directories securely implement the latest LDAP RFCs and do not expose LDAP protocol vulnerabilities, however, upgrade/remediate as a precaution.

### SonicOS Firmware Versions to Upgrade:

Platforms	Running Version	Upgrade to Version
SuperMassive 9200 / 9400 / 9600 NSA 3600 / 4600 / 5600 / 6600	6.1.x	6.1.1.9
NSA 2600	6.1.x	6.1.2.3
SuperMassive E10200 / E10400 / E10800	6.0.x	6.0.5.0-40o 6.0.1.8-202o
NSA E-Class E5500 / E6500 / E7500 / E8500 / E8510 NSA 220 / 220W / 240 / 250M / 250MW / 2400 / 3500 / 4500 / 5000 TZ 100 / 100W / 105 / 105W / 200 / 200W / 205 / 205W / 210 / 210W / 215 / 215W	5.9.x	5.9.0.6
	5.x	5.9.0.6 5.8.1.15
NSA 2400MX	5.7.x	5.9.0.6 5.7.2.1
PRO 2040 / 3060 / 4060 / 4100 / 5060 TZ 180 / 180W / 190 / 190W	4.x	4.2.1.9

# Dell SonicWALL Service Bulletin

This document contains the following sections:

Determining Vulnerable SonicOS LDAP Configurations .....	3
Upgrading SonicOS Firmware (Recommended).....	4
Remediation via SonicOS Configuration and LDAP/AD Configuration (If Not Upgrading SonicOS Firmware Immediately).....	5
Upgrading Firmware and Importing Original Settings (After Configuration Remediation Steps) .....	11
Returning Your Active Directory / LDAP Server to Original Settings (After Configuration Remediation Steps) .....	12
Dell SonicWALL GMS Web Services Vulnerability .....	13
GMS Specific Versions to Upgrade .....	13
GMS Remediation - Recommended Action.....	13
Installing the GMS Hotfix.....	13
Immediate GMS Configuration Remediation (Utilized Before Applying Hotfix) .....	14
Using GMS to Export Configuration Settings of Managed Firewalls.....	15
Using GMS to Edit User Groups in the Managed Firewalls.....	15
Obtaining the Recommended SonicOS Firmware Versions.....	16
Using GMS to Upgrade Firmware .....	17
Using GMS to Restore Configuration Settings of Managed Firewalls.....	18
Appendix - SonicwallLDAPAdminUserChk / SonicwallLDAPAdminGroups.....	19

# Dell SonicWALL Service Bulletin


## Determining Vulnerable SonicOS LDAP Configurations

First, determine IF SonicOS **User > Settings** is configured to use LDAP authentication AND any usernames in Microsoft Active Directory /LDAP directories are members of SonicWALL Administrator groups (locally or in LDAP directories). IF it is determined that LDAP is **NOT** enabled in SonicOS **User > Settings**, then you may stop here.

The **SonicwallLDAPAdminUserChk.vbs** script can be used to help diagnose configurations, as it examines a SonicOS configuration (.exp file) and determines if SonicOS **User > Settings** is enabled AND if any LDAP usernames in Active Directory are members of the SonicWALL administrator groups (“SonicWALL Administrators”, “Limited Administrators”, “SonicWALL Read-Only Admins”, “Guest Administrators”). The script is available at:

<https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminUserChk.zip>.

IF it is determined that LDAP is enabled in SonicOS **User > Settings**, but there are NO SonicWALL administrator usernames found in the AD / LDAP directory, then you may stop here (however, upgrading the firmware is suggested as a precautionary measure against creating a potentially vulnerable LDAP configuration in the future).

 **Note:** The **SonicwallLDAPAdminUserChk.vbs** script only searches in the LDAP directory and makes no changes to any objects in it. Also see appendix for script usage example.

To use the **SonicwallLDAPAdminUserChk.vbs** script:

1. Log into the Microsoft Active Directory Domain Controller or into another PC in the domain using a domain account with sufficient privileges to search Active Directory.
2. Download the zip archive containing the **SonicwallLDAPAdminUserChk.vbs** script from: <https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminUserChk.zip>. Save it in a convenient location and unzip it to extract the script.
3. Log into SonicOS and use System > Settings to export settings (.exp file).
4. Run the script to check IF the SonicOS **User > Settings** is configured to use LDAP and if the Active Directory LDAP configuration contains any usernames which are members of the SonicWALL administrator groups. The command is:

```
cscript SonicwallLDAPAdminUserChk.vbs settings-file.exp
```

where *settings-file.exp* is replaced by the name of the SonicOS settings file exported from the appliance. If the script reports any of the following, then no further action is necessary:

***The firewall is not configured to use LDAP for user authentication***

***No LDAP server is configured in the firewall settings***

***No SonicWALL administrator users were found in the directory***

If the script reports **<Number of> SonicWALL administrator users were found in the directory**, then proceed with the next steps of immediately upgrading firmware or immediately making configuration changes to disable these accounts.

# Dell SonicWALL Service Bulletin

## Upgrading SonicOS Firmware (Recommended)

IF SonicOS is configured to use Microsoft Active Directory / LDAP authentication AND any AD/LDAP usernames are members of the SonicWALL Administrator groups (locally or in LDAP directories), THEN it is critical to immediately upgrade to the recommended firmware versions listed above OR immediately apply the configuration remediation. See [Determining Vulnerable SonicOS LDAP Configurations](#) above for diagnosis. To upgrade firmware:



**Note:** For upgrading SonicOS via GMS, please refer to the [Using GMS to Upgrade Firmware](#) section below. Also, see [Dell SonicWALL GMS Web Services Vulnerability](#) for instructions to patch GMS Web Services.

## Obtaining the Recommended SonicOS Firmware Version

To obtain the 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 <https://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 recommended firmware to your computer, click the link for the firmware version listed in table above. You can download the Release Notes and other associated files in the same way.

## Creating a System Backup and Exporting Settings

1. In the System > Settings page, click **Create Backup**. SonicOS takes a “snapshot” of your current configuration settings and firmware\*, and makes it the new System Backup. Clicking **Create Backup** overwrites the existing System Backup, if any. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file for backup purposes, click **Export Settings**. A popup window displays the name of the saved file.

\* Certain SonicWALL appliances do not support saving firmware with system backups using the **Create Backup** button.

## Upgrading the SonicOS Firmware and Exporting Settings

1. On the System > Settings page, click **Upload New Firmware**.
2. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it will display in the Firmware Management table.
3. On the System > Settings page, click the Boot icon in the row for **Uploaded Firmware - New!**
4. In the confirmation dialog box, click **OK**. The appliance restarts and then displays the login page. No further action is required (issue resolved). For backup purposes, repeat the step [Creating a System Backup and Exporting Settings](#) above.

# Dell SonicWALL Service Bulletin

## Remediation via SonicOS Configuration and LDAP/AD Configuration (If Not Upgrading SonicOS Firmware Immediately)

IF SonicOS is configured to use Microsoft Active Directory / LDAP authentication AND any AD/LDAP usernames are members of the SonicWALL administrator groups (locally or in LDAP directories), THEN it is critical to immediately upgrade to the recommended firmware versions listed above OR immediately apply the configuration remediation. See [Determining Vulnerable SonicOS LDAP Configurations](#) above for diagnosis.

If not upgrading SonicOS firmware immediately, you can address the LDAP vulnerabilities by quickly performing the following configuration remediation steps on your firewall and, if required, on the Microsoft Active Directory server:

1. Export your SonicOS configuration settings to save the original LDAP usernames with SonicWALL administrator group memberships (to be optionally restored after firmware upgrade).
2. Apply the SonicOS and Active Directory/LDAP configuration remediation (described in two parts below) to remove LDAP usernames as members of SonicWALL administrator groups (configured in SonicOS locally and, if present, on Microsoft Active Directory /LDAP servers).
3. Create a system backup and export configuration settings (now with LDAP usernames NOT having SonicWALL administrative group membership). *Do not overwrite the configuration file saved in step 1.*
4. Later, upgrade the firewall to the recommended SonicOS firmware version, and add back LDAP usernames as members of SonicWALL administrator groups (optionally importing the configuration settings that were saved in step 1).



**Note:** *The SonicOS configuration remediation removes Web and SSH management access from any AD/LDAP username accounts with SonicWALL administrative rights, and therefore afterwards you will log into your firewall with local-only admin accounts (ie: non-LDAP usernames) for all administrative tasks. Note that local-only admin accounts can be created temporarily for any LDAP username which previously had SonicWALL administrative rights (by creating a non-LDAP username with SonicWALL administrative rights). See the [Optionally Create Temporary Local Administrators](#) section below.*

To apply the SonicOS and Microsoft Active Directory / LDAP configuration remediation, follow the steps below:

- On your firewall (part 1 of 2):
- On your Microsoft Active Directory / LDAP Domain Controller (part 2 of 2):

# Dell SonicWALL Service Bulletin

## On your firewall (part 1 of 2):

1. Log into SonicOS using the built-in admin account.
2. Navigate to System > Settings.

The screenshot shows the SonicOS Settings page. The left sidebar contains a navigation menu with categories like System, Network, and Firewall. The main content area is titled 'System / Settings'. At the top, there are 'Accept' and 'Cancel' buttons. Below that, there are buttons for 'Import Settings...', 'Export Settings...', and 'Send Diagnostic Reports to Support'. The 'Firmware Management' section includes a note: 'Note: Backup Settings were created FRI JUN 20 11:47:11 2014 from version SonicOS Enhanced 6.1.1.6-21n'. A table lists the following:

Firmware Image	Version
Current Firmware	SonicOS Enhanced 6.1.1.7-24n
Current Firmware with Factory Default Settings	SonicOS Enhanced 6.1.1.7-24n
System Backup	SonicOS Enhanced 6.1.1.6-21n

At the bottom of the Firmware Management section, there are buttons for 'Upload New Firmware...' and 'Create Backup...'.

3. Click **Export Settings** to save a copy of your SonicOS configuration settings on your management computer. This backs up your current LDAP usernames and administrator group memberships (to be optionally restored after firmware upgrade).
4. Navigate to Users > Local Groups.

The screenshot shows the SonicOS Users / Local Groups page. The left sidebar contains a navigation menu with categories like VPN, SSL VPN, Virtual Assist, and Users. The main content area is titled 'Users / Local Groups'. At the top right, there is a 'Mode: Configuration' indicator. Below that, there is a table with the following columns: #, Name, Bypass content filters, Guest Services, Admin, Comment, VPN Access, and Configure. The table contains 10 rows of data:

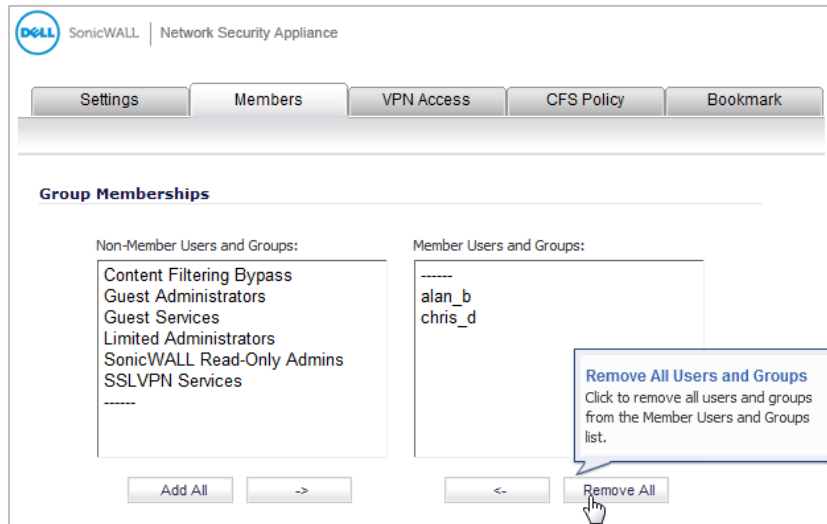
#	Name	Bypass content filters	Guest Services	Admin	Comment	VPN Access	Configure
1	Everyone						
2	Trusted Users						
3	Content Filtering Bypass	✓					
4	Limited Administrators			Ltd.			
5	SonicWALL Administrators			Full			
6	SonicWALL Read-Only Admins			Rd-Only			
7	Guest Services		✓				
8	Guest Administrators			Guest			
9	SSLVPN Services						
10	Content Filtering Override						

At the bottom of the table, there are buttons for 'Add Group...', 'Delete', and 'Delete All'.

# Dell SonicWALL Service Bulletin

Perform steps *a*, *b*, and *c* for each of the four SonicWALL Administrator groups: “SonicWALL Administrators”, “Limited Administrators”, “SonicWALL Read-Only Admins”, “Guest Administrators”:

- a) Click the Configure button in the row for the administrator group.
- b) In the Edit Group window, on the **Members** tab, do one of the following:
  - Remove all Active Directory / LDAP usernames by selecting the member(s) and clicking the left arrow button.
  - If all members are Active Directory / LDAP usernames, click **Remove All**.



- c) Click **OK** to apply the change and return to the Users > Local Groups page.

## *Optionally Create Temporary Local Administrators*

The SonicOS configuration remediation removes Web and SSH management access from any AD/LDAP username accounts with SonicWALL administrative rights, therefore local-only admin accounts may be created temporarily for any LDAP username which previously had SonicWALL administrative rights (by creating a non-LDAP username with SonicWALL administrative rights; for example, create the username “johnsmith\_sonicwall” and add this username as a member of the local group “SonicWALL Administrators”).

These steps are:

1. Log into SonicOS using the built-in **admin** account.
2. Navigate to Users > Local Users.
3. Click **Add User**.
4. On the **Settings** tab, in the **Name** field, type in the new local username, ensuring the username is NOT an AD/LDAP username. For example, if you have an LDAP username, *johnsmith*, type in an unlikely AD/LDAP username like *johnsmith\_sonicwall*.
5. In the **Password** field, type in a password for this local user.
6. In the **Confirm Password** field, type in the password again.

# Dell SonicWALL Service Bulletin

7. On the **Groups** tab, select the appropriate SonicWALL administrator group:
  - *Limited Administrators*
  - *SonicWALL Administrators*
  - *SonicWALL Read-Only Admins*
  - *Guest Administrators*
8. Click the right arrow button to move the selected group into the **Member Of** list.
9. Click **OK**.
10. Inform the SonicWALL admin user of their revised local username/credentials.

After the firmware is upgraded, you can import the previously saved configuration settings to the firewall causing these temporary local accounts to be removed and restoring the previously configured AD/LDAP usernames.

## On your Microsoft Active Directory / LDAP Domain Controller (part 2 of 2):

Use either of the following methods presented in this section:

- *Manual method* - appropriate for either Active Directory or other types of LDAP servers
- *Scripted method* - only for Microsoft Active Directory servers

### **Manual method:**

IF SonicWALL administrator group names (shown in the table below) are present in your Active Directory or LDAP configuration, THEN simply rename these groups to disable them from being used by SonicOS to authenticate administrators.

1. Log into the Domain Controller as the domain administrator.
2. Do one of the following:
  - On an Active Directory server, open **Active Directory Users and Computers**.
  - On any other type of LDAP server, open an appropriate update utility or application.
3. Locate all instances of the SonicOS administrator groups and rename the administrator groups by prefixing each with an underbar “\_”.

<b>SonicWALL Administrator Group Name:</b>	<b>Disable by Renaming to:</b>
<i>Limited Administrators</i>	<i>_Limited Administrators</i>
<i>SonicWALL Administrators</i>	<i>_SonicWALL Administrators</i>
<i>SonicWALL Read-Only Admins</i>	<i>_SonicWALL Read-Only Admins</i>
<i>Guest Administrators</i>	<i>_Guest Administrators</i>

4. Save and apply the changes.



# Dell SonicWALL Service Bulletin

## Scripted method (Active Directory Only):

### Checking –

Use the *SonicwallLDAPAdminUserChk.vbs* script to determine if any LDAP usernames in Active Directory are members of the SonicWALL administrator groups (“SonicWALL Administrators”, “Limited Administrators”, “SonicWALL Read-Only Admins”, “Guest Administrators”). The script is available at:

<https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminUserChk.zip>.



**Note:** This script only searches in the LDAP directory. It makes no changes to any objects in it.

To use the *SonicwallLDAPAdminUserChk.vbs* script:

1. Log into the Microsoft Active Directory Domain Controller or into another PC in the domain using a domain account with sufficient privileges to search Active Directory.
2. Download the zip archive containing the *SonicwallLDAPAdminUserChk.vbs* script from: <https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminUserChk.zip>. Save it in a convenient location and unzip it to extract the script.
3. Log into SonicOS and use System > Settings to export settings (.exp file).
4. Run the script to check if the Active Directory configuration contains any usernames which are members of the SonicWALL administrator groups. The command is:

```
cscript SonicwallLDAPAdminUserChk.vbs settings-file.exp
```

where *settings-file.exp* is replaced by the name of the settings file exported from the appliance. If the script reports any of the following, then no further configuration action is necessary:

***The firewall is not configured to use LDAP for user authentication***

***No LDAP server is configured in the firewall settings***

***No SonicWALL administrator users were found in the directory***

If the script reports **<Number of> SonicWALL administrator users were found in the directory**, then proceed with the next steps of immediately upgrading firmware or immediately making configuration changes to disable these accounts.

# Dell SonicWALL Service Bulletin

## Disabling –

Dell SonicWALL provides the *SonicwallLDAPAdminGroups.vbs* script to assist in disabling the SonicWALL administrator groups configured in Active Directory from being used by SonicOS to authenticate administrators. The script is available at:

<https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminGroups.zip>

The *SonicwallLDAPAdminGroups.vbs* script provides:

- **disable** option - disables the SonicWALL administrator groups that are configured in Active Directory.
- **enable** option - re-enables SonicWALL administrator groups previously disabled using the script's **disable** option. Use the **enable** option only after upgrading the firmware on your firewall (refer to the [Returning Your Active Directory / LDAP Server to Original Settings](#) section).

To use the *SonicwallLDAPAdminGroups.vbs* script:

1. Log into the Microsoft Active Directory Domain Controller or into another machine in the domain with sufficient privileges. The **disable** and **enable** options require that you log in using an account that has permissions to make changes in Active Directory.
2. Download the zip archive containing the *SonicwallLDAPAdminGroups.vbs* script from: <https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminGroups.zip>  
Save it in a convenient location and unzip it to extract the script.
3. Run the script to **disable** the SonicWALL administrator groups present in Active Directory from being used by SonicOS to authenticate administrators.
  - If running the script on the domain controller, the command is:


```
cscript SonicwallLDAPAdminGroups.vbs /disable
```
  - Otherwise:

```
cscript SonicwallLDAPAdminGroups.vbs /disable domain-controller
```

where *domain-controller* is replaced by the DNS name or IP address of the domain controller.
4. Confirm the *disable* action when prompted.
5. The SonicWALL administrator groups in Active Directory have now been renamed (by prefixing each SonicWALL administrator group name with underbar “\_”) which disables SonicOS from using Active Directory to authenticate administrators.
6. Once SonicOS firewalls using Active Directory have been upgraded to firmware versions that prevent the LDAP vulnerabilities, the script can be run with the **enable** option to easily restore the AD SonicWALL administrator group names, thus allowing SonicOS to utilize AD to authenticate administrators.

# Dell SonicWALL Service Bulletin

## Upgrading Firmware and Importing Original Settings (After Configuration Remediation Steps)

 **Note:** This section provides instructions in case you did not immediately upgrade SonicOS Firmware, and instead followed [Remediation via SonicOS Configuration and LDAP/AD Configuration](#), and are now upgrading SonicOS Firmware after having completed those steps.

If you are now ready to upgrade to the recommended firmware version, and if you followed the configuration remediation steps above, THEN, after upgrading, you may be able to import your original settings to reinstate your AD/LDAP usernames within administrative groups in SonicOS, and, if necessary, re-enable the SonicWALL administrator groups in the AD/LDAP server.

### Obtaining the Recommended SonicOS Firmware Version

To obtain the 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 <https://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 recommended firmware to your computer, click the link for the firmware version listed in table above. You can download the Release Notes and other associated files in the same way.

### Creating a System Backup and Exporting Your Settings

1. On the System > Settings page, click **Create Backup**. SonicOS takes a “snapshot” of your current configuration settings and firmware\*, and makes it the new System Backup. Clicking **Create Backup** overwrites the existing System Backup, if any. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file for backup purposes, click **Export Settings**. A popup window displays the name of the saved file.

\* Certain SonicWALL appliances do not support locally saved full system backups using the **Create Backup** button.

### Upgrading the SonicOS Firmware

1. On the System > Settings page, click **Upload New Firmware**.
2. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it will display in the Firmware Management table.
3. On the System > Settings page, click the Boot icon in the row for **Uploaded Firmware - New!**
4. In the confirmation dialog box, click **OK**. The appliance restarts and then displays the login page. Log in using the built-in **admin** account.

# Dell SonicWALL Service Bulletin

## Importing Your Original Configuration Settings to SonicOS

1. On the System > Settings page, click **Import Settings**.
2. Select the previously exported configuration file which contains the original AD/LDAP usernames and SonicWALL administrator groups settings.

## Returning Your Active Directory / LDAP Server to Original Settings (After Configuration Remediation Steps)

After upgrading your firewall to the firmware listed in the table at the beginning of this document, on your Active Directory / LDAP server, use one of the following methods:

### **Manual method:**

1. Log into the Domain Controller as the domain administrator.
2. Do one of the following:
  - On an Active Directory server, open **Active Directory Users and Computers**.
  - On any other type of LDAP server, open an appropriate update utility or application.
3. Locate all instances of the SonicWALL administrator groups and rename them to their original names by removing the underbar “\_”.

Temporary Remediation Group Name	Rename to Original:
<i>_Limited Administrators</i>	<i>Limited Administrators</i>
<i>_SonicWALL Administrators</i>	<i>SonicWALL Administrators</i>
<i>_SonicWALL Read-Only Admins</i>	<i>SonicWALL Read-Only Admins</i>
<i>_Guest Administrators</i>	<i>Guest Administrators</i>

4. Save and apply the changes.

### **Scripted method (Active Directory Only):**

Run the **SonicwallLDAPAdminGroups.vbs** script with the **enable** option to reinstate the SonicWALL administrator groups in Active Directory, and restore administrative rights for their group members.

1. Log into the Domain Controller or into another machine in the domain, using an account that has permissions to make changes in Active Directory.
2. Run the **SonicwallLDAPAdminGroups.vbs** script to re-enable administration by members of the SonicWALL administrators groups.
  - If running the script on the domain controller, the command is:

```
csript SonicwallLDAPAdminGroups.vbs /enable
```
  - Otherwise:


```
csript SonicwallLDAPAdminGroups.vbs /enable [domain-controller]
```

where *[domain-controller]* is replaced by the DNS name or IP address of the domain controller.
3. Confirm the *enable* action when prompted.

# Dell SonicWALL Service Bulletin

## Dell SonicWALL GMS Web Services Vulnerability

Dell SonicWALL has discovered an authentication vulnerability exposed when using GMS Web Services involving LDAP, Active Directory, and RADIUS authentication servers. This vulnerability is exposed only if you have GMS users in *LocalDomain* that use the above third party authentication servers for authentication and you use GMS Web Services (the iPhone App and ConnectWise Tool utilize GMS Web Services).

 **Note:** *GMS Web Browser UI and CLI, Analyzer, and ViewPoint based logins are not vulnerable. GMS Users created in domains other than LocalDomain are not vulnerable.*

## GMS Specific Versions to Upgrade

Platforms	Running these GMS Versions	Apply this Hotfix
GMS Windows / GMS Virtual Appliance / UMA EM5000	GMS 6.0, 7.0, 7.1, 7.2	Hotfix 150412


## GMS Remediation - Recommended Action

If you use Dell SonicWALL GMS to manage SonicWALL appliances, it is recommended to utilize GMS to immediately upgrade the firmware or make the necessary configuration remediation on the managed devices (see steps below). It is recommended to perform the *Immediate GMS Configuration Remediation* procedure first, and then follow the *Installing the GMS Hotfix* step after completing the recommended actions to the SonicWALL firewalls.

## Installing the GMS Hotfix

To download and install the Hotfix:

1. In a browser, log into MySonicWALL at <https://www.mysonicwall.com/>.
2. Download **Hotfix 150412** from the **Downloads > Download Center** page.
3. Log into the System Management Interface (*/appliance*) of your UMA or GMS system, then navigate to the **System > Settings** page.
4. Click the **Choose File** button, then select the Hotfix file.
5. Click the **Apply** button. The UMA or Virtual Appliance will automatically restart once the upgrade is completed. On a GMS Software (Windows) installation, you must explicitly reboot the system.

 **Note:** *This Hotfix must be applied to all systems in a GMS / UMA deployment.*

# Dell SonicWALL Service Bulletin

## Immediate GMS Configuration Remediation (Utilized Before Applying Hotfix)


The immediate remediation is to disable Web Services for any user who is using a third party authentication server.

1. In the GMS management interface, navigate to Console Panel > Management > Users.
2. On the **General** tab, select users who are authenticated with a third party authentication server.
3. On the **Action Permissions** tab, clear the **Use Web Services** checkbox.



The screenshot shows the 'Action Permissions' tab in the GMS management interface. The 'Use Web Services' checkbox is highlighted with a red box. The interface includes sections for Units, Views, Dashboard, and Others, each with various checkboxes for permissions. At the bottom, there are 'Update' and 'Reset' buttons.

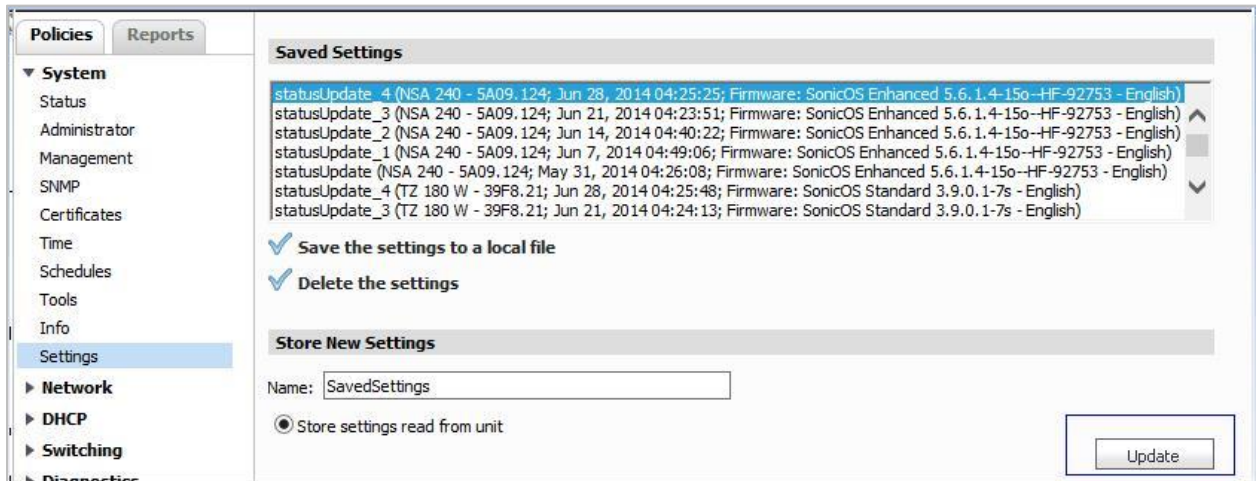
4. Click **Update**.

 **Note:** This operation can be done at the group level (**User Type**), in which case the changes at the group level for **Action Permissions** will be pushed to all users belonging to that **User Type**. By default, this checkbox is unchecked for all **User Types** for all **Domains**, except for the **Administrators** user type.

# Dell SonicWALL Service Bulletin

## Using GMS to Export Configuration Settings of Managed Firewalls

1. Log into GMS.
2. Select the Global, Group, or Unit level node.
3. In the Policies Panel > System > Settings screen, click **Update** in the *Store New Settings* section.



## Using GMS to Edit User Groups in the Managed Firewalls

If you have created groups with the same SonicOS administrator group names in your Active Directory or LDAP configuration, you can remove the members of these groups in SonicOS to prevent exploitation of the vulnerability.

This procedure takes a backup of the Firewall Configuration Settings and stores it in the GMS database.

1. In GMS, select the Global, Group, or Unit level node.  
If you added users to the affected SonicOS administrator groups at a global or group level node, you should apply the following steps at the corresponding node. This allows you to delete the administrator group members for multiple Firewalls at the same time.
2. Navigate to the Policies Panel > Users > Local Groups screen.

# Dell SonicWALL Service Bulletin

3. Perform steps *a*, *b*, and *c* for each of the four SonicWALL Administrator groups: “SonicWALL Administrators”, “Limited Administrators”, “SonicWALL Read-Only Admins”, “Guest Administrators”:

- a) Click the Configure button in the row for the administrator group.
- b) In the Edit Group window, on the **Members** tab, do one of the following:
  - Remove all Active Directory / LDAP usernames by selecting the member(s) and clicking the left arrow button.
  - If all members are Active Directory / LDAP usernames, click **Remove All**.



- c) Click **OK** to apply the change and return to the Users > Local Groups page.

## Obtaining the Recommended SonicOS Firmware Versions

To obtain the new SonicOS firmware image files for your managed firewalls:

1. In a browser on your management computer, log into your MySonicWALL account at <https://www.mysonicwall.com>.
2. Navigate to the **Downloads > Download Center** page.
3. For each managed firewall model, select the model in the **Software Type** drop-down list to display available firmware versions.
4. To download the recommended 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.

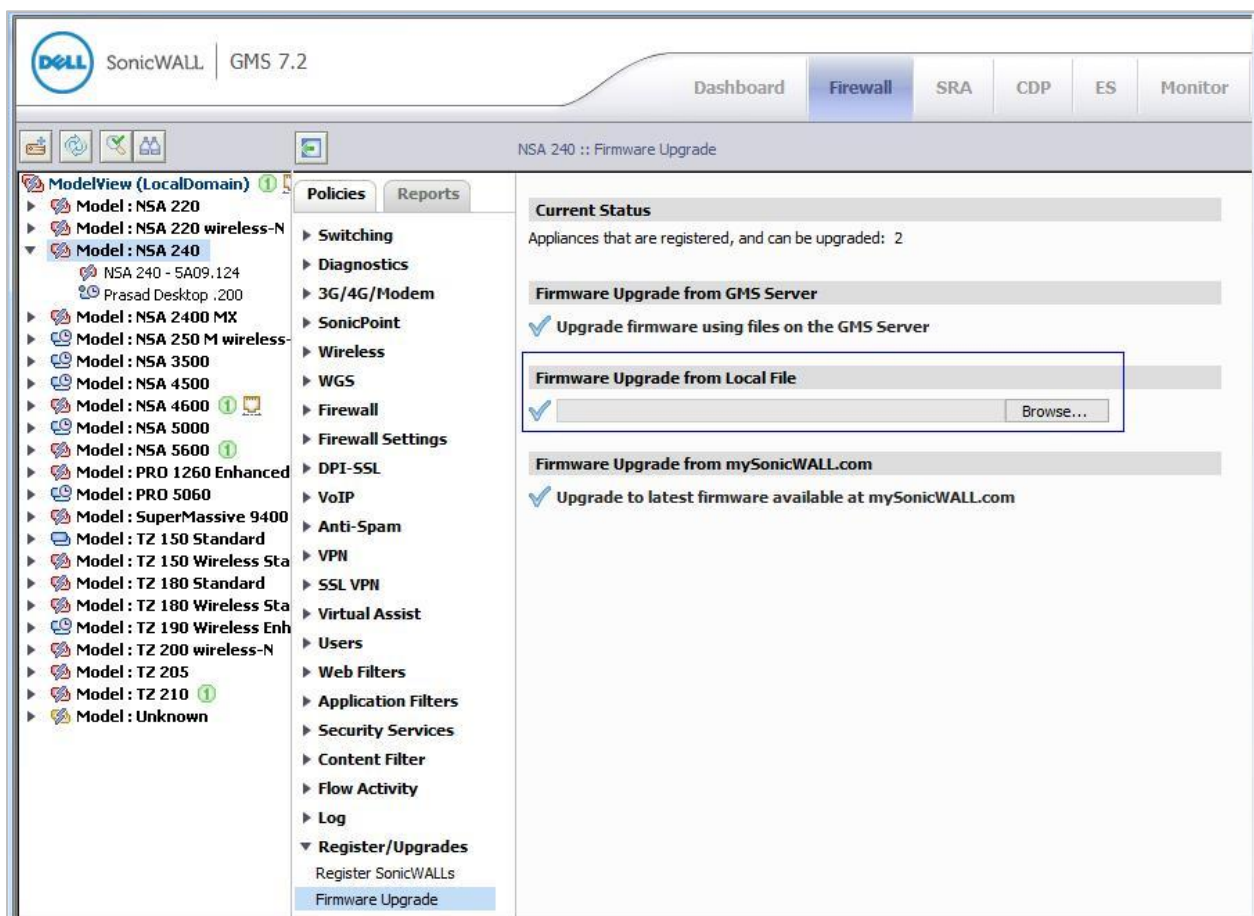


# Dell SonicWALL Service Bulletin

## Using GMS to Upgrade Firmware

While it is possible to upgrade the firmware of a managed firewall at the Unit level, it will be more efficient to perform the upgrade at the Group level.

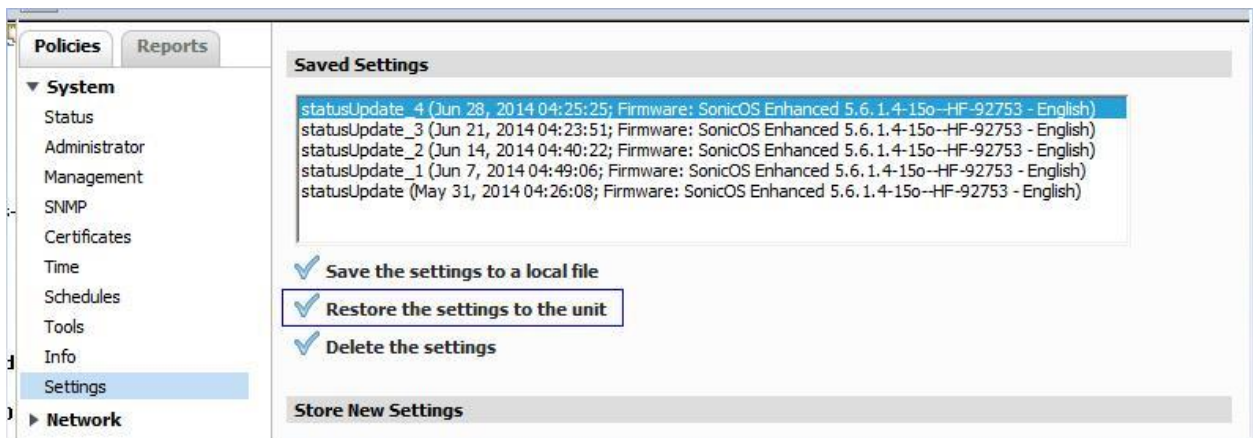
1. Log into the System Management Interface (*/appliance*) of your UMA or GMS system.
2. Set the TreeControl View to **Model View**.  
This organizes all managed firewalls by models, so that the same firmware can be applied at the group level where the group level node is a model name.
3. In the left pane, select a Model.
4. Under **Firmware Upgrade from Local File**, click **Browse**.
5. Select the firmware file for that Model that you downloaded from MySonicWALL.
6. Click the blue checkmark image on the left.



# Dell SonicWALL Service Bulletin

## Using GMS to Restore Configuration Settings of Managed Firewalls

1. Log into GMS.
2. In the TreeControl, select the Unit for which the Configuration Settings needs to be restored.
3. Navigate to the Policies Panel > System > Settings screen.
4. Select the first item in the **Saved Settings** list.
5. Click **Restore the settings to the unit**.
6. Select the next item in the **Saved Settings** list.
7. Click **Restore the settings to the unit**.
8. Repeat steps 6 & 7 until all settings have been restored.



# Dell SonicWALL Service Bulletin

## Appendix - SonicwallLDAPAdminUserChk / SonicwallLDAPAdminGroups

This section provides technical information about the command usage and options available in the following Visual Basic scripts, downloadable from the links below:

*SonicwallLDAPAdminUserChk.vbs:*

<https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminUserChk.zip>

*SonicwallLDAPAdminGroups.vbs:*

<https://software.sonicwall.com/UtilityTools/SonicwallLDAPAdminGroups.zip>

### SonicwallLDAPAdminUserChk.vbs Usage

=====

SonicwallLDAPAdminUserChk.vbs

Script to check if any user accounts exist in Active Directory that are set as administrative users for a Dell SonicWALL firewall, getting the latter information from a settings(.exp) file exported from the firewall.

SonicwallLDAPAdminUserChk can be run on the domain controller or from another machine in the domain. It can be run from any domain account that is able to make searches in Active Directory.

Note that this script only searches in the LDAP directory. It makes no changes to any objects in it.

Use 'cscript SonicwallLDAPAdminUserChk.vbs /help' for help.

Copyright (c) 2014, Dell SonicWALL Inc.

=====

Usage:

```
cscript SonicwallLDAPAdminUserChk.vbs [options] <file.exp>
cscript SonicwallLDAPAdminUserChk.vbs [options] /rerun
cscript SonicwallLDAPAdminUserChk.vbs /?
cscript SonicwallLDAPAdminUserChk.vbs /help
```

/rerun: Read the appliance user / user group configuration from the file that was that was saved on a previous run rather than reading from the .exp file again. For a re-run with the same firewall's configuration this is much quicker than re-reading and decoding the exported settings again.

/server: Specify the host name or IP address of the LDAP server on which to search. If this is not given, then SonicwallLDAPAdminUserChk will use the LDAP server that is configured on the firewall. If this is being run on the server itself, then you can specify it as 'localhost'.

/domain: The DNS name of the domain to search under. If a domain is not given, then SonicwallLDAPAdminUserChk will look it up in the directory's RootDSE (it should only be necessary to specify it should that fail for some reason).

/norefs: Search only under the domain on the server, ignoring any references to other servers. If this is not given, then the default is to search from the top of the forest and follow returned references to other domain controllers in it.

/subrefs: Search the domain on the server and its sub domains, but ignoring any references to higher level (parent) domain.

/verbose: Be more verbose in reporting what is found.



# Dell SonicWALL Service Bulletin

## *Usage Example for SonicwallLDAPAdminUserChk.vbs*

When you run the SonicwallLDAPAdminUserChk.vbs script, the output may be similar to the following example:

```
: cscript SonicwallLDAPAdminUserChk.vbs sonicwall.exp

Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Dell SonicWALL Administrative User Check Script Version 1.5

Reading the export file...
...
Decoding the export file (this may take a while)...
...

Found a local administrative user group: SW Admins
Found a local administrative user: john_smith
Found a local administrative user: bob_jones
Found a local administrative user: bob_local

An LDAP search will now be made to check if those users/groups exist in the
LDAP directory.
Press enter to continue

Searching under domain DN: DC=example,DC=com

Searching for the administrative users that were found in the firewall settings
Found 2 of the 3 users in the directory

Searching for the administrative groups that were found in the firewall
settings
Found group SW Admins
  - at CN=Sw Admins,CN=Users,DC=example,DC=com

Searching for users who are members of those groups
Found 1 user

Found administrative users set on the firewall and existing in the directory:
  - john_smith at CN=John Smith,OU=Users,OU=IT,OU=Domain
Users,DC=example,DC=com
  - bob_jones at CN=Bob Jones,OU=Users,OU=IT,OU=Domain Users,DC=example,DC=com

Found users in the directory set as administrative via groups on the firewall:
  - mary_joe at CN=Mary Joe,OU=Users,OU=IT,OU=Domain Users,DC=example,DC=com

3 Dell SonicWALL administrator users were found in the directory
```

# Dell SonicWALL Service Bulletin

## SonicwallLDAPAdminGroups.vbs Usage

=====

SonicwallLDAPAdminGroups.vbs

Script to rename the administrative user groups for the DELL SonicWALL firewall in Active Directory in order to temporarily disable management by LDAP-authenticated users by removing any firewall administrative rights that have been set there.

SonicwallLDAPAdminGroups can be run on the domain controller or from another machine in the domain. For the /check option it can normally be run from any domain account, for the /disable and /enable options it must be run from an account that has administrative rights to make changes in the directory.

Use 'cscript SonicwallLDAPAdminGroups.vbs /help' for help.

Copyright (c) 2014, DELL SonicWALL Inc.

=====

Usage:

```
cscript SonicwallLDAPAdminGroups.vbs /check [options] [server] [domain]
cscript SonicwallLDAPAdminGroups.vbs /disable [options] [server] [domain]
cscript SonicwallLDAPAdminGroups.vbs /enable [options] [server] [domain]
cscript SonicwallLDAPAdminGroups.vbs /?
cscript SonicwallLDAPAdminGroups.vbs /help
```

- /check: Check if any DELL SonicWALL administrative user groups exist in the directory on the server, and if so, if they have any members.
- /disable: Disable administration of DELL SonicWALL firewalls. The script will find all DELL SonicWALL administrative groups in the directory and rename them from '<name>' to '\_<name>', effectively removing all user administrative rights to DELL SonicWALL firewalls that have been set there. Note that it will not affect any administrative rights that are set on the firewalls.
- /enable: Re-enable administration of DELL SonicWALL firewalls. This will undo the effects of a previous run with /disable by finding all the previously renamed groups and restoring their correct names, hence restoring the DELL SonicWALL firewall administrative rights of their member users.
- /norefs: Search only under the domain on the local or given server, ignoring any references to other servers. If this is not given, then the default is to search from the top of the forest and follow returned references to other domain controllers in it.
- /subrefs: Search the domain on the local or given server and its sub domains, but ignoring any references to higher level (parent) domain.

SonicwallLDAPAdminGroups can be run on the domain controller or from another machine in the domain. For the /check option it can normally be run from any domain account, for the /disable and /enable options it must be run from an account that has administrative rights to make changes in the directory.

If running SonicwallLDAPAdminGroups on the machine where the directory is located, then server can be omitted, or it can be given as 'localhost' if the domain is to be specified. If the domain is not specified, then SonicwallLDAPAdminGroups will look it up in the directory's RootDSE (it should only be necessary to specify it should that fail for some reason).

Note that this script only renames the DELL SonicWALL administrative groups in the LDAP directory: SonicWALL Administrators, SonicWALL Read-Only Admins, Limited Administrators and Guest Administrators. It makes no other changes to them and in no way updates or renames any other objects in the directory.