Release Notes

Email Security

Dell SonicWALL Email Security 7.3.6 Software Release Notes

Contents

System Compatibility

Dell SonicWALL Email Security 7.3.6 Software is supported on systems with the following:

Operating Systems

- Windows Server 2003, SP2
- Windows Server 2008

Note: Dell SonicWALL Email Security 7.3.6 Software is currently not supported on Windows running on VMWare.

Hardware Requirements

- Intel Pentium: Celeron, P4 or compatible CPU
- Additional 2 GB of RAM strongly recommended (1GB additional RAM minimum)
- Hard Disk: Additional 40GB minimum. Recommended installation on a separate drive. Your storage needs are based on your mail volume, quarantine size, archived data, and auditing settings.

HTTPS ***Connectivity to Dell SonicWALL License Manager***

Email Security products running version 6.0 and above communicate with the Dell SonicWALL License Manager servers using the default HTTPS port. The Upstream firewalls in the network where this Email Security system is deployed must allow HTTPS communication on port 443 that is initiated from the 7.3.6 upgrade process.

Note: To test connectivity in Dell SonicWALL Email Security 7.3.6, click the **Test Connectivity to Dell SonicWALL** button on the **System** > **License Management** page in the user interface. If the test fails, check your firewall to be sure that outbound HTTPS communication is allowed.

Enhancements

The following is a list of new enhancements made to features in the Dell SonicWALL Email Security 7.3.6 Software release:

- **McAfee Incremental Updates**
  McAfee Incremental Updates significantly reduce the network bandwidth usage.
- **CLI Commands**
  New CLI commands introduced in Email Security 7.3.6 to force NAI updates (*forcemcafeeupdate* and *forcemcafeeupdatecancel*).
- **Network Path Functionality**
  New Network Pat functionality in Email Security 7.3.6 allows MTA to have “SmartHost with Exception” Routing option.
- **SNMP Service**
  SNMP Service has been upgraded with added support to Start, Stop, and Set Community Strings.
- **Self-Signed Certificates Support**
  Email Security 7.3.6 supports downloading Self-Signed Certificates from LDAP Servers over LDAPs.
- **PMTA Upgrade**
  Powerful Mail Transfer Agent (PMTA) is upgraded to version 4.0r2sb1 in Email Security 7.3.6.
- **Tomcat Upgrade**
  Tomcat is upgraded to version 6.0.35 in Email Security 7.3.6.
- **JRE Upgrade**
  Java Runtime Environment (JRE) is upgraded to version 1.6.0.30 in Email Security 7.3.6.
- **OpenSSL Upgrade**
  OpenSSL is upgraded to version 1.0.0e in Email Security 7.3.6.

Restrictions and Limitations

These are the known restrictions and limitations currently reported in the Dell SonicWALL Email Security 7.3.6 Software release:

	Symptom	**Condition**
95936	Auditing and Junk Box messages do not display after downgrading from Dell SonicWALL Email Security 7.3.5 to 7.2.4.	Occurs after a successful upload of the Dell SonicWALL Email Security 7.2.4 Der-signed patch. Upon logging into the appliance again, the user will receive a warning message, as well as no inbound messages in the Auditing and Junk Box screens. **Workaround:** Login to the command prompt. Go to the ‘\INSTALL’ directory, and run the command ‘mlfworkr.exe –rebuildsearchdb’. All messages will display in the Junkbox/Auditing UI.

Known Issues

These are the known issues currently reported in the Dell SonicWALL Email Security 7.3.6 Software release:

	Symptom	Condition
113931	On the Web User Interface, upgrading from Email Security 7.2.4 to 7.3.5 using the "sonicsigned_der_eg-7.3.5.6369-win_2k.exe" does not upgrade the JRE from version 1.5.0_15 to version 1.6.0_30. This only occurs on SBS 2008 systems.	Occurs when navigating to the **System > Advanced** page, browsing for the "sonicsigned_der_eg-7.3.5.6369-win_2k.exe" file, and clicking **Apply**. The system reboots, but does not upgrade the JRE version. Stop the Web server under **Administrative Tools > IIS Manager > Connections**, and go to Run Type services.msc. Restart Tomcat. When logging back in to the Email Security system, the User Interface does not display. **Workaround:** Before applying the patch from the Web User Interface, navigate to the **services.msc** panel. Go to the Tomcat properties. From the Log On tab, select the "Log on using these Credentials" option, and change the login to Admin Credentials. Restart the Tomcat service. Log back in to the Email Security service, and navigate to **System > Advanced** page. Browse for the "sonicsigned_der_eg-7.3.5.6369-win_2k.exe" file, and click **Apply**. The system reboots and successfully upgrades the JRE. Next, navigate to the **Start > Administrative Tools**, and open the IIS Manager to stop the Web server under Connections. Then, go to the Run Type services.msc, and restart the Tomcat service.
107341	Progress bars of the Junk Email Breakdown report are not aligned with each other.	Occurs when viewing the Junk Email Breakdown report on the Reports & Monitoring > Overview Reports page. The report should show bar charts aligned with number and percentage values.
106418	When Spam emails are sent to recipients in the To/Cc/Bcc fields, multiple instances of emails appear in the JunkBox.	Occurs when spam mail with the subject "MLFJUNK" is sent to recipients in each To/Cc/Bcc field. When the admin logs in to the Junk Box UI and selects all the messages, then clicks "Unjunk," the following email is sent to the same recipients: "[Junk released by User action]MLFJUNK".
95227	The Scheduled Backup process does not confirm the available disk space before initiating a backup zip file creation.	Occurs when attempting to schedule a backup. The Scheduled Backup process should estimate the space required for the backup before initializing a backup zip file creation.

Resolved Known Issues

These are the resolved known issues currently reported in the Dell SonicWALL Email Security 7.3.6 Software release:

	Symptom	Condition
112222 **120042**	Web UI cross-site scripting vulnerability found in Email Security 7.3.5 or earlier release builds.	The vulnerability may be exposed when attempting to access some of the Email Security administrative configuration pages using administrative credentials. To exploit this vulnerability, the attacker must have access to the web UI, which is typically only available on the local LAN. In addition, the attacker must have administrative credentials. The pages impacted are only accessible to the administrator, so it does not pose any risk to normal users accessing the web UI. The vulnerability also does not specifically target or impact message processing, anti-spam, anti-virus or policy and compliance protection. For these reasons the risk is considered low.
111245	The TLS implementation of the SMTP Proxy defaults to a large set of ciphers, including weak ciphers that are required by modern security compliance tests to be disabled.	The client side TLS request demanded the use of a weak cipher. Email Security always returns the strongest cipher that the client supports.
110710	The Flood Protection threshold is not being triggered by secondary aliases.	Occurs when flood sender sends more emails than the value specified in message threshold by the administrator. Flood protection threshold is not accounting for email aliases associated with the primary address.
110460	Customers with larger user lists and multiple RAs may get ‘User Map is Stale’ alerts.	Occurs when using large user maps in a split mode setup with multiple RAs. This may issue stale alerts because of an issue with replicating the data in a timely manner.
109769	The CA Certificate keystore in the Java Directory is empty with no certificates imported inside. LDAPs are also unable to work correctly because of dependence on the certificates.	Occurs when downloading certificates into the JRE directory. New certificates are not getting added to the CA Certs file in JRE directory.
109027	Tomcat allows the use of weak SSL ciphers, which is a potential security risk and does not comply with modern security compliance tests (PCI).	Occurs when conducting a PCI compliance scan on the Email Security system. The results show that the Email Security system does not comply with PCI standards.
108993	MTA routing needs a “SmartHost with Exceptions” routing option, where the exception domains use MX record routing.	Occurs when selecting MTA routing options for routing email using SmartHost to the destination server.
108152	The DSN template file path no longer displays in the PMTA config.dat after new changes are made to the MTA.	Occurs when new changes are made to the MTA. As a result, the MTA stops, and does not restart. **Workaround:** Add the DSN template file path manually in the PMTA configuration file.

100550	MTA services do not start and an error message displays in the config.dat file.	Occurs if the data directory is a UNC network path with spaces. The MTA does not start.
87748	The View button in the Junk Summary are not working for alias addresses, yet work fine for primary addresses. This is only seen when users are Global or non-LDAP users.	Occurs when clicking the View button for junk messages in the Junk Summary. The primary addresses that have aliases receiving junk for the aliases are unable to use the View button on the Junk Summary that was sent to the primary address. **Workaround:** Configure an LDAP server that returns no users. This creates the multi_ldap.xml with the necessary structure. You can also drop an empty multi_ldap.xml under $DATADIR$\. However, if you do this and decide to add an LDAP, this empty file will first have to be manually deleted.

Important Note for McAfee Anti-Virus Subscribers

Feature	Summary
Upgrade McAfee to Engine 5400	McAfee will be ending support for the anti-virus scan engine v5300 (running in Dell SonicWALL Email Security versions 7.1.2 and lower). Dell SonicWALL Email Security customers using McAfee antivirus will need to upgrade their email security firmware by February 28th, 2010.

Dell SonicWALL strongly recommends customers running McAfee to upgrade to the latest 7.3.6 firmware version.

McAfee has released an upgraded version of their anti-virus engine using a newer, enhanced format that provides smaller, faster signature updates, improved bandwidth, and better detection of the latest malware. As of **February 28, 2010**, Dell SonicWALL McAfee anti-virus engines in the firmware versions 7.1.2 and lower will no longer receive virus signature updates. Customers using McAfee anti-virus will begin to see degraded virus protection and will no longer be protected against the latest virus outbreaks.

Customers can simply upgrade their Dell SonicWALL Email Security firmware to receive the benefits of the McAfee upgrade. The impact will be largely transparent to administrators and end customers. To ease the transition, Dell SonicWALL will offer customers the following upgrade path:

- Upgrade to Dell SonicWALL's newest, latest firmware (version 7.3.6). In addition to the enhanced Dell SonicWALL McAfee engine, firmware version 7.3.6 offers several significant enhancements, including best-in-class effectiveness, bandwidth improvement, improved ease of management and significant scalability improvements.

Upgrading to Email Security 7.3.6

Using the Full Installer method, follow these steps to upgrade from Email Security (5.0 and later) to Email Security 7.3.6.

Downloading Dell SonicWALL Email Security 7.3.6

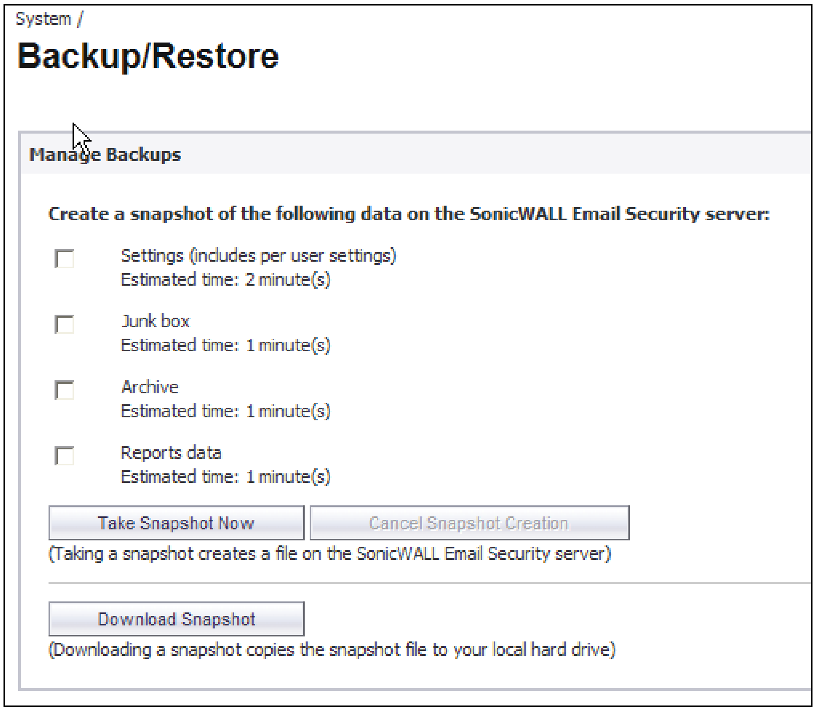
1. Log into your account at http://www.mysonicwall.com.
2. In the left navigation pane under **Downloads**, click **Download Center**.
3. In the **Activate Service – Software Download** dialog box, select a language from the **Select Language** drop-down list.
4. Select the checkbox to agree to the terms and conditions, and then click **Submit**.
5. In the **Download Center** screen, select **Email Security Software** from the **Type** drop-down list. If not already on this selection, the screen will refresh to show links to the available Email Security software versions and release notes.
6. Click the link for the version that you want and then select **Save** in the dialog box. Copy the downloaded binary to the Windows server running your Email Security application.

Backing Up Your Existing Environment

Before you upgrade your environment, you should back up your existing environment. This will enable you to restore it if you decide to revert the upgrade for some reason. Your backup should include the settings files, including the per user settings.

To back up your existing environment:

1. In the left navigation pane under **System**, choose **Backup/Restore**. You will see the Backup/Restore page:



System /

Backup/Restore

Manage Backups

Create a snapshot of the following data on the SonicWALL Email Security server:

☐ Settings (includes per user settings)
Estimated time: 2 minute(s)

☐ Junk box
Estimated time: 1 minute(s)

☐ Archive
Estimated time: 1 minute(s)

☐ Reports data
Estimated time: 1 minute(s)

(Taking a snapshot creates a file on the SonicWALL Email Security server)

(Downloading a snapshot copies the snapshot file to your local hard drive)

2. In the Manage Backups section, select **Settings**.
3. Click **Take Snapshot Now** to create a snapshot.
4. Click **Download Snapshot** to save the snapshot to your local file system.

Upgrading Your Dell SonicWALL Email Security

Follow this procedure to upgrade your existing Email Security installation to version 7.3.6. The Full Installer includes installation of Apache Tomcat, the Java Runtime Environment (JRE), and Firebird as well as the base Email Security software.

1. On the server running Email Security, double-click the Email Security 7.3.6 installation file. Click **Run** in the dialog box. If you do not have direct access to the server, use a remote desktop connection to connect to the server and run the installation file on the server.

   Note: Administrators must copy the installation file to the Email Security Server in order to run the installation file. Administrators will *not* be able to upgrade through the Web UI on Windows.

2. In the Welcome page of the installation wizard, click **Next**.
3. Read the License Agreement and then click **Next** to accept the agreement.
4. Dell SonicWALL recommends that Asian language packs be installed, and an alert is displayed if they are missing. To proceed with the Email Security installation and install Asian language packs later, click **Next**. To install Asian language packs prior to proceeding, click **Cancel**.

   Note: Installing Asian language packs is optional; however, the spam prevention capabilities of Dell SonicWALL Email Security may be diminished without them. Asian language packs can be installed before or after Dell SonicWALL Email Security Software installation.

5. On the Destination Folder page, click **Browse** to select an alternate folder, or click **Next** to accept the default location.

   Note: It is important that this folder is not scanned by an anti-virus engine.

6. On the Choose Data Folder page, click **Browse** to select an alternate folder, or click **Next** to accept the default location. If the data folder is on a different disk drive than the install directory, ensure that it has fast read/write access with less than 10 millisecond latency. You can test latency with the ping command.
7. On the Start Installation page, click **Next**.
8. If requested, allow the installation of Tomcat, Firebird, and the Java Runtime Environment (J2RE). If Tomcat is installed in this step, it prompts for the Apache Tomcat Web server port number. The default port is 80. If you are already running a Web server on port 80, you must change the port setting. Dell SonicWALL recommends port 8080. Click **Next** to continue.

   Note: You can change the port number and configure HTTPS access after installation by using the Server Configuration > User View Setup page of the Email Security appliance.

9. After the installation finishes, click **Finish** in the Installation Complete wizard. A browser window is displayed with links to the Email Security user interface and documentation.

Related Technical Documentation

For basic and advanced deployment examples, Dell SonicWALL documentation is available in the Dell SonicWALL Technical Documentation Online Library:

http://www.sonicwall.com/us/Support.html

Also, refer to the following related Knowledge Based articles:

How to Upgrade a Windows server in Split Mode Configuration

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=4891

How to Setup/Breakup Cluster Licensing for Email Security's Split-Configuration

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=5244

How to Recover a Non-Accessible Email Security Appliance

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=8486

How to Reset the Authentication for GUI Login Back to Default Credentials

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=5207

Last updated: 9/20/2012