Release Notes

Email Security | **SonicWALL Email Security 7.2.4 Software**

System Compatibility

SonicWALL Email Security 7.2.4 Software is supported on systems with the following:

Operating Systems

- Windows 2003, SP2
- Windows 2008

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 SonicWALL License Manager

Email Security products running version 6.0 and above communicate with the 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 7.2.4 upgrade process.

 **Note**: To test connectivity in SonicWALL Email Security 7.2.4, click the **Test Connectivity to 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 enhancements made to features in the SonicWALL Email Security 7.2.4 Firmware release:

- **Enhanced Effectiveness**
  - **Greater Effectiveness** – with the ability to prevent up to 99.96%[1] of spam from reaching from users' mailboxes
  - **Upgraded Advanced IP Reputation Management** – with the ability to eliminate up to 98%[1] of the spam at the connection level, before it enters the network
  - **Enhanced protection** – against dangerous botnets and zombies, as well as Directory Harvest Attacks and Denial of Service Attacks
  - **Updated Anti-Virus Scan Engines** – Upgraded version of both the McAfee antivirus scan engine and Kaspersky antivirus scan engine.
    - **McAfee Virus Scan Engine –** The latest McAfee antivirus engine uses a newer, enhanced format that provides smaller, faster signature updates, improved bandwidth and better detection of the latest malware.
    - **Kaspersky Virus Scan Engine** – The latest Kaspersky antivirus engine delivers native multi-threading, a smaller disk footprint, faster analysis, and new types of scanning including detection of multipacked objects

[1] Results based upon internal testing conducted by SonicWALL in September 2009 using Email Security Release 7.2.1 operating on SonicWALL's corporate Email Security Gateway.

- **Improved Ease of Management:**
  - **New GMS Support** – Support for SonicWALL Global Management System (GMS) v6.0[2]
  - **New Syslog Support** – Full syslog support, with message level detail, to enable 3rd party monitoring and reporting tools
  - **New Windows Event Viewer Support** – for Windows software deployments
  - **Advance Search Capabilities** – New high-performance search capabilities for message retrieval, archiving, auditing and e-discovery
  - **Enhanced Junkbox, Audit, and Per-User Views** – Unlimited scalability for junkbox, audit and per-user views

- **Scalability Improvements**
  - **GRID Network Performance Optimization** -- Optimized anti-spam signatures and updates for faster distribution and improved performance
  - **High-Performance Connection Management** -- Higher throughput high-performance connection management for scalable performance during peak traffic loads (Windows Server Software ONLY)

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 SonicWALL Email Security versions 7.1.2 and lower). SonicWALL Email Security customers using McAfee antivirus will need to upgrade their email security firmware by February 28th, 2010.

SonicWALL strongly recommends customers running McAfee to upgrade to the latest 7.2.4 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**, 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 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, SonicWALL will offer customers the following upgrade path:

- Upgrade to SonicWALL's newest, latest firmware (version 7.2.4). In addition to the enhanced SonicWALL McAfee engine, firmware version 7.2.4 offers several significant enhancements, including best-in-class effectiveness, bandwidth improvement, improved ease of management and significant scalability improvements.

[2] SonicWALL GMS 6.0 is targeted for release in December 2009

Known Issues

These are the known issues currently reported in the SonicWALL Email Security 7.2.4 Software release:

	Symptom	Condition
93344	The user is unable to add LDAP users to the Per User Allowed/Blocked list.	Occurs when attempting to add an LDAP user to the Allowed or Blocked list from the Per User Address Book page after installing or upgrading the CASS 2.0 Junk Store to the 7.2.4 firmware. A success message displays, but upon verification, the LDAP user is not added to the list.
84935	After an upgrade, the user is alerted about resetting the SSL settings.	Occurs when upgrading the servers with the latest 7.2.1 firmware.
84585	When a group is deleted from the LDAP server, it is not removed from ES.	Occurs when attempting to delete a group from the LDAP after it has been added to the ES. The user will have to manually remove the group from the ES.

Resolved Issues

The following issues have been resolved in the SonicWALL Email Security 7.2.4 Software release:

	Symptom	Condition
90809	Plug-in threads cause SMTP to crash unless firmware is upgraded to latest firmware.	Occurs when the SMTP engine resources enter into race condition. The upgrade is highly recommended as it provides stability.
86793	ES 7.2.0 on Windows Server 2008 sends Asian Language pack alerts.	Occurs when ES 7.2.0 is installed on a server running Windows 2008. Alerts appear stating that Asian Language packs are missing. **Workaround:** Suppress critical alerts.
86230	User's name contains an apostrophe, causing a false DHA.	Occurs when upgrading to ES 7.2.0. The SMTP displays that the user is being discarded due to a false DHA. **Workaround:** Manually add the email addresses containing an apostrophe as a Global LDAP source. You can also configure the email addresses to be routed to different alias addresses.
85404	User is unable to search for emails based on the 'To' field after a Services restart.	Occurs after a Services restart. Initially, the user may perform a Simple/Advanced searched based on the 'To' field, and mail will be indexed and then appear under Auditing. However, after a Services restart, new mail is indexed and appears to be in Auditing. When performing a search again based on the 'To' field, the results do not display mail sent after the restart.
85089	User enters the time from the Web Interface, and the appliance automatically adds one hour.	Occurs when attempting to set the time from the Host Configuration> Data and Time screen. **Workaround:** Subtract one hour when entering time onto the appliance. You could also activate NTP on the Command Line Interface (CLI).
85037	RA sends a gateway smtp test over port 2599, and issues an alert every 15 minutes.	Occurs when monitoring the alerts in RA. After upgrading the CC/RA with the latest 7.2.0.2565 firmware and verifying in the mlfmonitor.log, the RA sends a gateway smtp test over its own port 2599. Instead, the smtp test should be sent on the CC's port 2599.

Upgrading to Email Security 7.2.4

Using the Full Installer method, follow these steps to upgrade from Email Security (5.0 and later) to Email Security 7.2.4.

Downloading SonicWALL Email Security 7.2.4

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.

Note: Reverting is allowed to version **7.0** only.

To back up your existing environment:

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

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.

If, after upgrading, you need to roll back to a previous version, go back to the Backup/Restore page and use the Manage Restores section to upload the snapshot you have stored.

Upgrading Your SonicWALL Email Security

Follow this procedure to upgrade your existing Email Security installation to version 7.2.4. 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 on, double-click the Email Security 7.2.1 installation file and then 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.
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. 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 SonicWALL Email Security may be diminished without them. Asian language packs can be installed before or after 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. 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.

Document part number: 232-001929-00 Rev A
Last updated: 9/7/2010