System Compatibility

SonicWALL Email Security 7.2.4 is supported on the following SonicWALL Email Security appliances:
- SonicWALL Email Security 200
- SonicWALL Email Security 300
- SonicWALL Email Security 400
- SonicWALL Email Security 500
- SonicWALL Email Security 3300
- SonicWALL Email Security 4300
- SonicWALL Email Security 6000
- SonicWALL Email Security 8000
- SonicWALL Email Security 8300

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

- **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)

---

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

SONICWALL®

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.

Known Issues

These are the known issues currently reported in the SonicWALL Email Security 7.2.4 Firmware 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 Firmware 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.
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 the Email Security Firmware

The following procedures are for upgrading an existing Email Security appliance.

Backing Up Your Existing Environment

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

1. Login to Email Security interface using the **admin** account
2. In the left navigation pane under **System**, choose **Backup/Restore**. You will see the Backup/Restore page:

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

If, after upgrading to 7.2.1, 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.
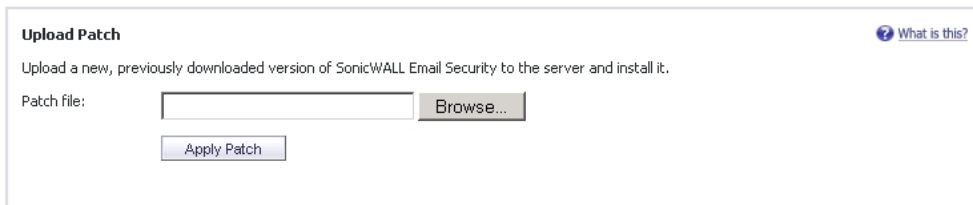
Note: Rollback is allowed to version **7.1** only.

Upgrading Your SonicWALL Email Security Firmware

Follow this procedure to upgrade your existing Email Security firmware.

1. Navigate to the System > Advanced page and scroll down to the **Upload Patch** section.

2. Click **Browse** to locate the Email Security Firmware file on your local file system, and then click **Apply Patch**.
3. As part of the upgrade process, the Email Security appliance will reboot. The upgrade process could take between 10-20 minutes. All the settings and data will be preserved.

⚠️ **NOTE for ES8300**
Your ES8300 is equipped with a battery backup unit on the RAID Controller Card, which allows the appliance to write volatile memory to disk in the event of a loss of power. This battery backup unit must be charged for 24 hours. When deploying your ES8300 appliance, follow the startup and registration instructions detailed in the Getting Started Guide, and then allow the battery backup in the unit to charge for 24 hours. If the battery is not fully charged, some RAID features are turned off, and the appliance performance is temporarily impaired until the battery is fully charged.

Document part number: 232-001928-00 Rev A
Last Updated: 9/7/2010

SONICWALL