



SonicWall® Email Security 10.0.25

Release Notes

September 2023

This release notes provide information about the SonicWall® Email Security 10.0.25 release. The Software Requirements and Virtual Appliance Requirements are also updated to support the newer and more advanced software releases. Administrators should review and change their Email Security system configurations as per the new requirements to optimize security and performance.

- [About Email Security](#)
- [Managing Firmware Downgrades](#)
- [Features and Enhancements](#)
- [Features and Enhancements](#)
- [Known Issues](#)
- [Product Licensing](#)
- [Upgrade and Installation Instructions](#)
- [SonicWall Support](#)

About Email Security

Email Security 10.0 protects email from advanced email threats such as targeted phishing attacks, ransomware, business email compromise, fraud, spam, and viruses. Email Security 10.0.25 version provides fixes for the issues identified in the [Features and Enhancements](#) section.

Email Security is supported as firmware on SonicWall Email Security appliances, as a software installation on Windows Server systems, and as a Virtual Appliance on VMware ESXi platform and on Hyper-V platform. Email Security is also offered as a hosted service. See the following sections for detailed requirements:

- [Supported Platforms](#)
- [Software Requirements](#)
- [Virtual Appliance Requirements](#)
- [Required Application Ports](#)

Supported Platforms

Email Security 10.0.25 firmware is supported on the following SonicWall appliances:

- Email Security Appliance 5000
- Email Security Appliance 5050
- Email Security Appliance 7000
- Email Security Appliance 7050
- Email Security Appliance 9000

Software Requirements

When installed as software, SonicWall Email Security is supported on systems that meet the following requirements:

Requirements	Definitions
Processor	Intel 64 or AMD64 with x86 instruction set, 8 cores
Memory	16 GB of RAM minimum 32 GB of RAM recommended
Hard Disk Space	Additional 160 GB minimum Recommend installation on a separate drive. Your storage needs are based on your mail volume, quarantine size, archived data, and audit settings.
Operating System	Microsoft Hyper-V Server 2019 Microsoft Hyper-V Server 2016 Microsoft Hyper-V Server 2012 R2 Microsoft Hyper-V Server 2012 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012
Network File System (NFS) 4.1 version	Provides protocol support to take advantage of clustered server deployments, including the ability to provide scalable parallel access to files distributed among multiple servers.

Virtual Appliance Requirements

VMware ESXi Platform

When installed as a Virtual Appliance using VMware platform, SonicWall Email Security is supported on systems that meet the following requirements:

Requirement	Definition
Processor	Intel 64 or AMD64 with x86 instruction set, 8 cores Can be expanded to 64 cores
Memory	16 GB of RAM minimum 32 GB of RAM recommended Can be expanded to 64 GB

Requirement	Definition
Hard Disk Space	160 GB thick provisioned hard disk space
VMware Platforms	ESXi 7.0

Hyper-V Platform

When installed as a Virtual Appliance using Hyper-V platform, SonicWall Email Security is supported on systems that meet the following requirements:

Requirement	Definition
Processor	Intel 64 or AMD64 with x86 instruction set, 8 cores Can be expanded to 64 cores
Memory	16 GB of RAM minimum 32 GB of RAM recommended Can be expanded to 64 GB
Hard Disk Space	160 GB thick provisioned hard disk space
Hyper-V Platforms	Microsoft Hyper-V Server 2019 Microsoft Hyper-V Server 2016

Required Application Ports

Email Security requires that certain ports be left open to operate correctly.

Service	Port Number
HTTP	80
HTTPS	443
Junk Replication	2599
Replicator	51212
SMTP	25

Managing Firmware Downgrades

IMPORTANT: Please review the SonicWall Product Lifecycle page to see the list of supported firmware versions. Downgrades to any firmware versions who are past their support discontinued date are not supported.

For firmware downgrade from Email Security 10.0.25, only 10.0.19 or later versions are supported, you should follow the usual firmware downgrade steps.

IMPORTANT: If you downgrade to an older version of Email Security, you could be exposed to vulnerabilities that the most recent 10.0.25 protects you from.

Features and Enhancements

The following is a list of new feature enhancements added in Email Security 10.0.25:

- Multi-threading for mlqueue to improve processing of quarantine data.

Resolved Issues

There are no resolved issues in this release.

Known Issues

There are no known issues in this release.

Product Licensing

SonicWall Email Security components must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at <https://www.mysonicwall.com/>.

Email Security appliances are licensed through security service bundles and support services. The following options are available:

- **TotalSecure Email:** TotalSecure Email bundle includes Anti-Spam, Anti-Virus, Anti-Phishing, Anti-Spoofing, DLP and Compliance, Software Updates, and 24*7 Support.
- **Advanced TotalSecure Email:** Advanced TotalSecure Email bundle includes Anti-Spam, Anti-Virus, Anti-Phishing, Anti-Spoofing, DLP and Compliance, Capture Advanced Threat Protection (ATP) for zero-day malware, Time-of-Click URL protection, Software Updates, and 24*7 Support.
- **Email Encryption (add-on):** Email Encryption are add-on licenses which can be added to the TotalSecure or Advanced TotalSecure bundle. Email Encryption enables secure exchange of sensitive and confidential information.
- **Hardware Warranty:** Hardware Warranty needs to be separately licensed for the hardware appliances deployed as Remote Analyzer in split mode configuration.

Hosted Email Security (HES) is licensed through simplified bundles. The following are the options available:

- **Hosted Email Security Essentials:** Essentials bundle includes Anti-Spam, Anti-Virus, Anti-Phishing, Anti-Spoofing, DLP and Compliance, Email Continuity, Software Updates, and 24*7 Support.
- **Hosted Email Security Advanced:** Advanced bundle includes Anti-Spam, Anti-Virus, Anti-Phishing, Anti-Spoofing, DLP and Compliance, Email Continuity, Capture Advanced Threat Protection (ATP) for zero-day malware, Time-of-Click URL protection, Software Updates, and 24*7 Support.
- **Email Encryption (add-on):** Email Encryption are add-on licenses which can be added to the Essentials or Advanced bundle. Email Encryption enables secure exchange of sensitive and confidential information.

Upgrade and Installation Instructions

The following sections describe how to prepare for and upgrade or install your Email Security solution.

Topics:

- [Backing Up Your Existing Environment](#)
- [Firmware Upgrade Path](#)
- [Upgrading your Existing Firmware](#)
- [Upgrading your Existing Software](#)
- [Installing the Virtual Appliance](#)
- [Installing on the Hyper-V Platform](#)

Backing Up Your Existing Environment

Before you upgrade your appliance firmware, you should back up your existing environment. This allows you to restore it if you decide to change back for some reason. Your backup should include the settings files, including User Settings.

To back up your existing environment:

- 1 Log into the Email Security management interface using the **admin** account.
- 2 Go to **MANAGE | Backup/Restore > Schedule Backup**.
- 3 Click **Backup Now**.

The screenshot shows a 'Create Backup Snapshot' dialog box. At the top, it says 'SONICWALL™ | Create Backup Snapshot' with a 'Close' button. Below the title bar, the main heading is 'Create Backup Snapshot'. Under 'Select Components', there are checkboxes for 'Global Settings', 'Organization Settings', 'User Settings', 'Reports data', 'Junk box', and 'Archive'. To the right of 'Reports data', 'Junk box', and 'Archive' are 'Last (Days)' dropdown menus, all set to '1 Day'. Under 'Backup Store', there are two options: 'Save on the Email Security host' (unchecked) and 'Save to FTP Server' (unchecked) with a dropdown menu showing 'ftp'. At the bottom are 'Start' and 'Cancel' buttons.

- 4 On the **Create Backup Snapshot** page (shown above), select the components you want to backup. At a minimum, select **Global Settings**, **Organization Settings**, and **User Settings**.
- 5 Select whether you want the snapshot to be saved on the Email Security host or saved to an FTP server.

- 6 Click **Start** to begin the backup.

On the **Schedule Backup** page, messages report the status of the backups, and the task appears in the Backup Snapshots list on the **Manage Backups** page.

Firmware Upgrade Path

The upgrade path for Email Security Appliances is 9.0.x => 9.1.x => 9.2.x => 10.0.x. The following guidelines apply:

- 9.0.x (Upgrade to the latest version in the 9.0 branch which is 9.0.6)
- 9.1.x (Upgrade to the latest version in the 9.1 branch which is 9.1.3)
- 9.2.x (Upgrade to the latest version in the 9.2 branch which is 9.2.2)
- 10.0.x (Upgrade to the latest release in the 10.0.x branch which is 10.0.25)

NOTE: Firmware version 9.2.x and newer are only supported on 64-bit platforms

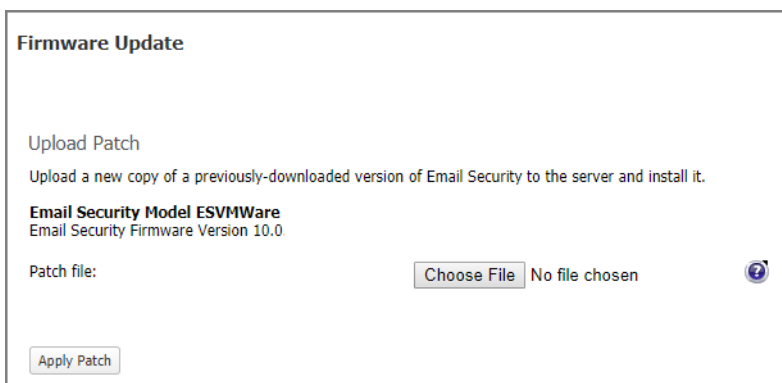
CAUTION: Skipping a version in the upgrade path will result in file corruption that may render the appliance unusable.

TIP: After every upgrade step, let the ES Appliance process mail for at least 30 minutes before completing the next step in the upgrade path.

Upgrading your Existing Firmware

To upgrade the existing firmware on an Email Security appliance:

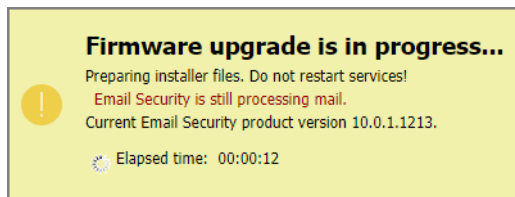
- 1 Log into your MySonicWall account and download the new Email Security firmware to your management computer.
- 2 Log into the Email Security management interface using the **admin** account.
- 3 Navigate to **MANAGE | Firmware Update**.
- 4 Click Choose File to locate the Email Security firmware on your local file system, and then click **Apply Patch**.



The screenshot shows the 'Firmware Update' page. It has a title 'Firmware Update' and a section 'Upload Patch' with the instruction 'Upload a new copy of a previously-downloaded version of Email Security to the server and install it.' Below this, it says 'Email Security Model ESVMWare' and 'Email Security Firmware Version 10.0'. There is a 'Patch file:' label, a 'Choose File' button, and the text 'No file chosen'. A help icon is to the right. At the bottom left is an 'Apply Patch' button.

- 5 Click **OK** in the popup dialog window that displays alerting you that when the installation is complete you are redirected to the Login page and the machine will be rebooted.

A yellow popup message displays telling you that the firmware upgrade is in progress.



IMPORTANT: As part of the upgrade process, the Email Security appliance reboots. The upgrade process could take between 10 and 20 minutes.

CAUTION: Your ESA 9000 appliance 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 ESA 9000 appliance, follow the startup and registration instructions detailed in the *Email Security Appliance 5000/7000/9000 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.

Upgrading your Existing Software

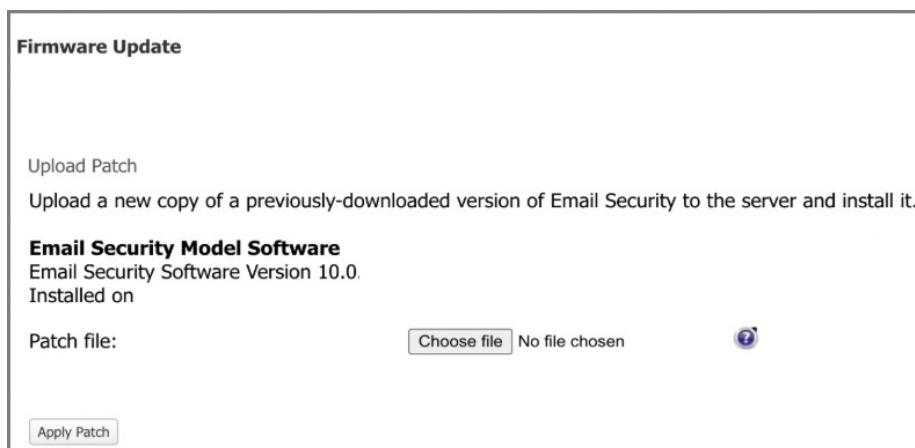
You can perform firmware upgrades when logged into Email Security as the administrator. The full installer for Email Security software includes installation of Apache Tomcat, the Java Runtime Environment (JRE), Firebird, and MySQL as well as the base Email Security software.

NOTE: SonicWall recommends that you use the signed update packages for software upgrades. Even though it has a .exe file type, the update package has to be run through the web interface rather than from the operating system.

IMPORTANT: As a part of the upgrade process, the Windows server does reboot. The upgrade process could take between 10 and 20 minutes. All settings and data are preserved.

To upgrade your existing Email Security software:

- 1 Log into your MySonicWall account and download the new Email Security Software updater package to your management system.
- 2 Log into Email Security using the **admin** account.
- 3 Navigate to **MANAGE | Firmware Update**.



- 4 Click **Choose File** to locate the Email Security software updater package on your local file system.
- 5 Click **Apply Patch**.

Installing the Virtual Appliance

SonicWall Email Security Virtual Appliance is installed by deploying an OVA file to your ESXi server. Each OVA file contains all software components related to SonicWall Email Security. Email Security can be configured for a single server or in a distributed environment on multiple servers.

Using the wizard for your virtual environment, install the `.ova` file.

- 1 Select the ESX server on which you want to deploy the virtual machine.
- 2 Choose the `.ova` file you want to install from the location where it is stored.
- 3 Set the virtual machine name and select the datastore.
- 4 Select the ESX resources to be used. The `.ova` file is validated.
- 5 Verify the template details for your installation.
- 6 Agree to the licensing.
- 7 Provision the storage for the virtual machine. The choices you make are validated for compatibility with Email Security.
- 8 Select the network interface to be assigned to the virtual machine.
- 9 Click **Finish** to complete the installation. A progress bar displays the status of the installation.
- 10 Select the instance of the virtual machine and power it on.
- 11 Open the virtual console and configure the IP address and the default route.
- 12 Launch a browser and enter the IP address of the virtual appliance.
- 13 Log in using the default credentials:
 - User = **admin**
 - Password = **password**
- 14 Enter the following setting when asked:
 - **Monitoring**—The email address of the mail server administrator who receives emergency alerts, the email of the MTA postmaster who will receive emergency alerts, and the name or IP address of the SMTP servers.
 - **Hostname**—A descriptive hostname for this SonicWall Email Security appliance.
 - **Networking**—The static IP address for this computer, including the Primary and Fallback DNS server IP addresses.
 - **Date and Time**—The system date and time, current time zone, and an option for automatically adjusting for Daylight Savings Time.
- 15 Click **Apply Settings** and the virtual appliance is rebooted.

Refer to the *Email Security Administration Guide* for more information on how to configure your virtual appliance.

Installing on the Hyper-V Platform

SonicWall Email Security virtual appliance is installed on Hyper-V platform by deploying an VHD file to Hyper-V server. Each VHD file contains all software components related to SonicWall Email Security. Email Security can be configured for a single server or in a distributed environment on multiple servers.

Using the wizard for your virtual environment,

- 1 Select the Hyper-V server on which you want to deploy the virtual machine.
- 2 Copy the Hyper-V build (.vhd) file to the respective Hyper-V server local directory.
- 3 Set the virtual machine name and select the datastore.
- 4 Select the resources to be used RAM, CPU and VLAN.
- 5 Verify the template details for your installation.
- 6 Choose the VHD(.vhd) file you want to install from the location where it is stored.
- 7 Click **Finish** to complete the installation. A progress bar displays the status of the installation.
- 8 Select the instance of the virtual machine and start.
- 9 Open the virtual console and configure the IP address and the default route. Use command:
 - "interface eth0 <ipaddress> <subnetmask>"
 - "route -add default -destination <gatewayip>"
- 10 Launch a browser and enter the IP address of the virtual appliance.
- 11 Agree to the licensing.
- 12 Log in using the default credentials:
 - User = **admin**
 - Password = **password**
- 13 Enter the following setting when asked:
 - **Monitoring**—The email address of the mail server administrator who receives emergency alerts, the email of the MTA postmaster who will receive emergency alerts, and the name or IP address of the SMTP servers.
 - **Hostname**—A descriptive hostname for this SonicWall Email Security appliance.
 - **Networking**— The static IP address for this computer, including the Primary and Fallback DNS server IP addresses.
 - **Date and Time**—The system date and time, current time zone, and an option for automatically adjusting for Daylight Savings Time.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum at <https://community.sonicwall.com/technology-and-support>
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

 **NOTE:** A NOTE icon indicates supporting information.

 **IMPORTANT:** An IMPORTANT icon indicates supporting information.

 **TIP:** A TIP icon indicates supporting information.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Email Security Release Notes
Updated - September 2023
Software Version - 10.0.25
232-006085-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.