SonicWall™ Email Security 9.0.4

Release Notes

August 2017

These release notes provide information about the SonicWall™ Email Security 9.0.4 release.

Topics:

- About Email Security
- Features and Enhancements
- Resolved Issues
- Known Issues
- Product Licensing
- Upgrade and Installation Instructions
- SonicWall Support

About Email Security

Email Security provides a flexible solution to protect email from spam, phishing, and viruses, and it extends Email Security to a new family of appliances. Email Security 9.0.4 is a patch that enhances performance through support for the new McAfee 5900 AV scan engine and resolves known issues found in previous releases. Refer to Features and Enhancements for more information.

Email Security 9.0.4 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 platforms. See the following sections for detailed requirements:

- Supported Appliance Platforms
- Software Requirements
- Virtual Appliance Requirements
- System Requirements for the Junk Button
- System Requirements for the SendSecure Button

Supported Appliance Platforms

Email Security 9.0.4 firmware is supported on the following SonicWall appliances:

- Email Security 3300
- Email Security 4300
- Email Security 8300
- Email Security Appliance 5000
- Email Security Appliance 7000
- Email Security Appliance 9000

Software Requirements

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

Requirements	Definitions
Processor	Intel Pentium: P4 or compatible CPU
Memory	8 GB of RAM
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 2012 R2 (64-bit) Microsoft Hyper-V Server 2012 (64-bit) Windows Server 2012 R2 (64 bit) Windows Server 2012 (64 bit) Windows Server 2008 R2 (64 bit) with Service Pack 1 Windows Small Business Server (SBS) 2011 (64-bit) with Service Pack 2

Virtual Appliance Requirements

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

> **IMPORTANT:** Because Email Security 9.0.4 is a 64-bit implementation and versions prior to 9.0 are 32-bit, SonicWall recommends a fresh deployment for Email Security 9.0 or later for Virtual Appliance deployments.

Requirements	Definition
Processor	1 CPU, can be expanded to 8 CPU
Memory	8 GB of RAM, can be expanded to 64 GB
Hard Disk Space	160 GB thick-provisioned hard disk space
VMware Platforms	ESXi 5.5 and newer

> **NOTE:** The default allocation for the OVA image of the Email Security Virtual Appliance is 160 GB on the virtual disk. Beginning with version 8.3, Email Security supports disk resizing, but once the disk space has been expanded, it cannot be reduced back to a smaller size.

System Requirements for the Junk Button

The Junk Button is supported on the following platforms:

Solution	Platforms	OS
Junk Button, 32-bit	Outlook 2010, 32 bit	Windows 7
	Outlook 2013, 32 bit	Windows 8.1
	Outlook 2016, 32 bi5	Windows 10
Junk Button, 64-bit	Outlook 2010, 64 bit	Windows 7
	Outlook 2013, 64 bit	Windows 8.1
	Outlook 2016, 64 bit	Windows 10

System Requirements for the SendSecure Button

The Send-Secure Button is supported on the following platforms:

Secure Button Client	OS	Outlook Version
SecureMailTaggingSetup32	Window 7, 32 bit	Microsoft Outlook 2010, 32 bit
	Window 8.1, 32 bit	Microsoft Outlook 2013, 32 bit
	Window 10, 32 bit	Microsoft Outlook 2016, 32 bit
SecureMailTaggingSetup64	Window 7, 64bit	Microsoft Outlook 2010, 64 bit
	Window 8.1, 64 bit	Microsoft Outlook 2013, 64 bit
	Window 10, 64 bit	Microsoft Outlook 2016, 64 bit

Features and Enhancements

Email Security 9.0.4 corrects the issues listed in Resolved Issues. It was also enhanced with the new McAfee 5900 AV scan engine. The following describes the changes made to Email Security 9.0 to the improve protection from spam, phishing, and viruses:

- Updated Email Security Appliances
- Capture ATP Integration
- Office 365 Support
- Improved Anti-Virus Offerings

Updated Email Security Appliances

The Email Security Appliances (ESA) have been refreshed with the release of Email Security 9.0. Appliance functionality focuses on:

- Effectively scanning inbound and outbound email
- Providing multi-layer protection
- Managing compliance and encryption

Refer to the *SonicWall Email Security Appliance 5000/7000/9000* for more information about the appliances.

Capture ATP Integration

Capture Advanced Threat Protection (Capture ATP) is a cloud-based service that analyzes various types of content for malicious behavior, and this function is being extended to Email Security beginning with version 9.0. It work similar to the anti-virus engines already integrated into Email Security and does the following:

- Scan suspected messages.
- Render a verdict about the message.
- Take action based on what the administrator configures for that verdict.

> ⓘ **NOTE:** All three ant-virus options (McAfee, Kaspersky, and Cyren) and Capture ATP need to be licensed as part of Total Secure bundles, to use Capture functionality.

Unlike the anti-virus engines that check against malware signatures stored locally, messages for Capture ATP are uploaded to the back end cloud servers for analysis. These messages are typically advanced threats that evade identification by traditional static filters. They need to be identified by their behavior, and thus need to be run in a highly instrumented environment. Capture ATP accepts a broad range of file types to analyze.

To engage Capture ATP:

1. Inbound email is first scanned by the other anti-virus plug-ins.
    - If a threat is detected, then the appropriate action is taken (discard, junk, tag, etc.).
    - If the service is enabled, all the anti-virus plug-ins return a *no threat* result, and the message contains an eligible attachment, the email is sent to Capture ATP for analysis.
2. The attachment is uploaded to the Capture server and quarantined in the Capture Box.
3. Capture ATP performs the analysis and returns a verdict.
4. Further analysis is performed and Email Security applies the appropriate action based on the final disposition of the message.

Capture ATP status and settings can be managed through the **Capture** command on the user interface. For details, refer to the *Email Security 9.0 Administration Guide*.

Office 365 Support

Beginning with the 9.0 release, organizations that use Office 365 for email can now route their email through their Hosted Email Security (HES) to get added protection for their messages. A path can be created based on both the sender domain and the source IP address so outbound mail from ISPs can be scanned while still maintaining the privacy of the IPS customer.

> ⓘ **NOTE:** Office 365 is supported only for Hosted Email Security; it is not supported for the on-premise products.

Customers are strictly limited to one ISP as the source for one outbound path. If a customer wants a second ISP that customer must configure a second path. Similarly, no IP addresses outside of the ISP-owned range are allowed on a shared-IP path. Only one path can handle email for a particular sender domain.

Because upstream TLS must be negotiated before the path is selected, weak ciphers are not allowed.

Improved Anti-Virus Offerings

Email Security improved its core virus filtering capability with improved Kaspersky, Cyren and McAfee filtering engines. Email Security integrated the Kaspersky 8.5 Anti-Virus DAT and scan engine, the Cyren 5.4.25 AV scan engine, and the McAfee 5900 AV scan engine into the Email Security gateway and backend servers. All utilize 64-bit specific data for both Windows and Linux platforms. All engines provide improved scanning and filtering to detect malicious content.

Resolved Issues

This section provides a list of resolved issues for the 9.0.4 patch.

Administration

Resolved issue	Issue ID
Email Security locks a user's Active Directory account. Occurs after one failed login attempt.	180949

Email Encryption

Resolved issue	Issue ID
Mail coming from SonicWall Encryption (DataMotion) servers may get blocked. Can occur if the SPF records for the encryption service hosting servers (Azure cloud) are not set correctly. IP addresses for the Azure servers were added to the predefined dictionaries which are used in the predefined policies.	190542

Known Issues

This section provides a list of known issues for the 9.0.4 patch.

Administration

Known issue	Issue ID
Impacts versions 9.0.0 thru 9.0.3: Appliances and virtual appliances using a remotely mounted (CIFS) data directory become unresponsive for SMTP, SSH and HTTP(S) connection. Occurs if a CIFS mount point goes offline. The SMTP, SSH and HTTP(S) connections revert to a responsive state when the remote CIFS share becomes available again. No manual intervention is required to restore full functionality.	183343

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 comes with several modules that must be licensed separately. For maximum effectiveness, all modules are recommended. The following licenses are available:

- **Email Protection (Anti-Spam and Anti-Phishing):** Additional license that protects against email spam and phishing attacks.
- **Email Anti-Virus (McAfee and SonicWall Time Zero):** Provides updates for McAfee anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
- **Email Anti-Virus (Kaspersky and SonicWall Time Zero):** Provides updates for Kaspersky anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
- **Email Anti-Virus (SonicWall Grid A/V and SonicWall Time Zero):** Provides updates for SonicWall Grid anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.

- **Email Anti-Virus Cyren:** Provides updates for Cyren anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
- **Email Encryption Service:** License for encryption features enabling the secure exchange of sensitive and confidential information. It includes predefined dictionaries to ensure proper protection.
- **Email Compliance Subscription:** License for compliance features. It includes predefined polices for easy compliance, allows multiple governance policies, identifies email for compliance policy enforcement, and provides compliance reporting and monitoring.
- **Capture for Email Security:** Provides analysis of threats by examining their behavior in a managed environment.

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
- Upgrading Your Existing Firmware
- Upgrading Your Existing Software
- Installing the Virtual Appliance

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. Choose the backup process appropriate for your version of software:

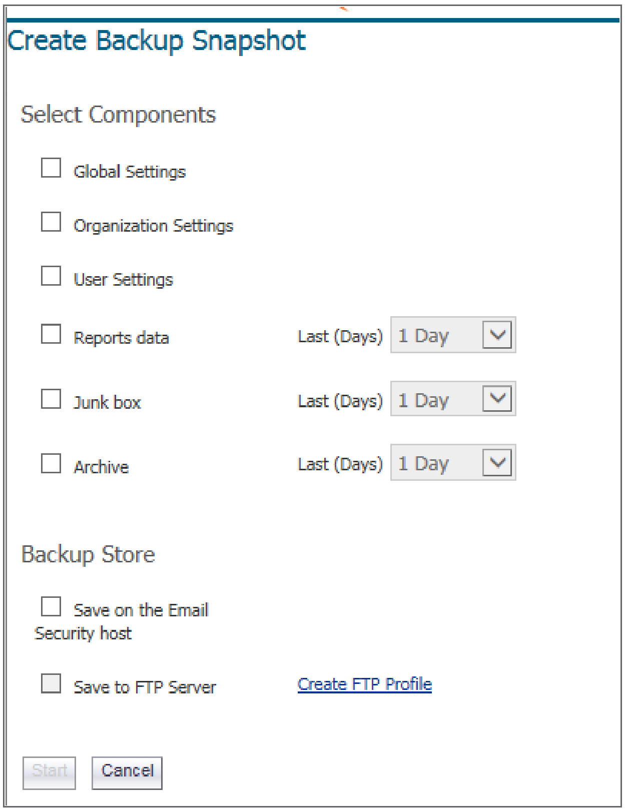
- Backing Up an 8.3 or Later Environment
- Backing Up a Pre-8.3 Environment

Backing Up an 8.3 or Later Environment

To back up your existing 8.3 or later version environment:

1. Log into the Email Security management interface using the **admin** account.
2. In the left navigation pane under **System**, choose **Backup/Restore > Schedule Backups**.

3 Click on **Backup Now** button.



Create Backup Snapshot

Select Components

□ Global Settings

□ Organization Settings

□ User Settings

□ Reports data Last (Days) 1 Day

□ Junk box Last (Days) 1 Day

□ Archive Last (Days) 1 Day

Backup Store

□ Save on the Email Security host

□ Save to FTP Server Create FTP Profile

Start Cancel

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.

ⓘ **NOTE:** If no FTP profiles have been defined for remote backups, the option to **Save to FTP Server** is not active. You can set up an FTP server profile by clicking on the link for **Create FTP Profile**.

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

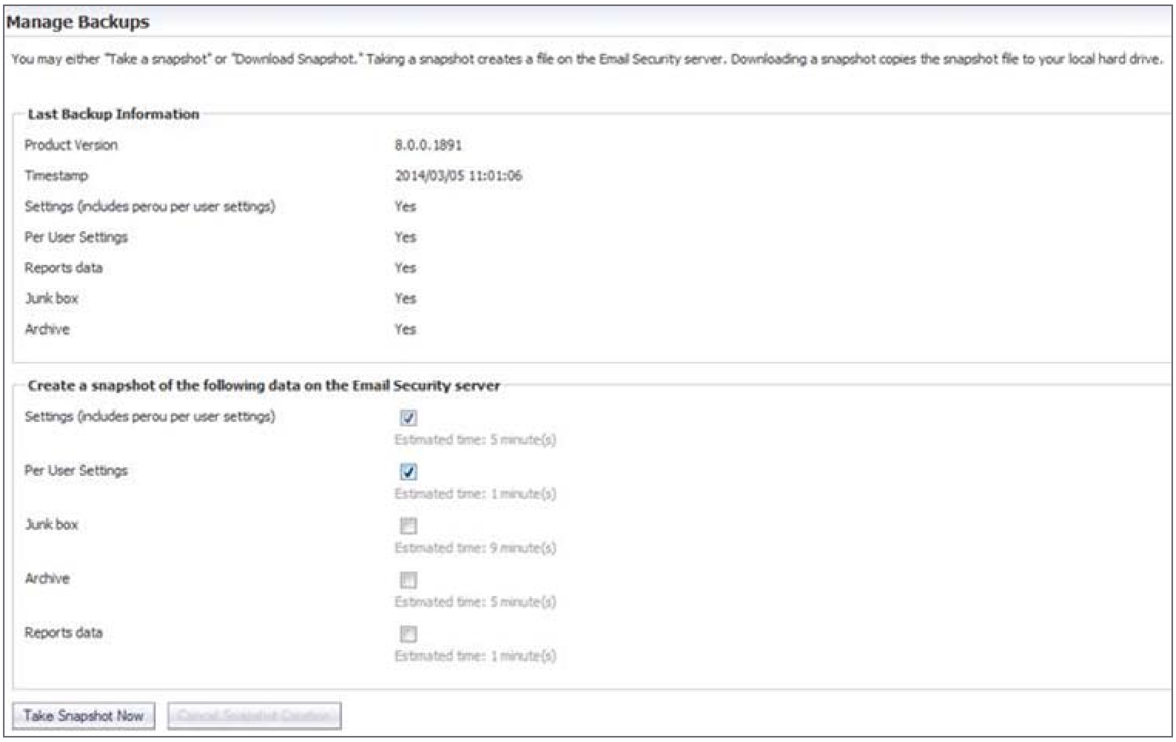
On the **Schedule Backup** page, messages report the status of the backups, and the task appears in the Backup Snapshots list on the **Manage Backups** page.

Backing Up a Pre-8.3 Environment

To back up your existing environment if older than version 8.3:

1 Log into the Email Security management interface using the **admin** account.

2 In the left navigation pane under **System**, choose **Backup/Restore**.



Manage Backups

You may either "Take a snapshot" or "Download Snapshot." Taking a snapshot creates a file on the Email Security server. Downloading a snapshot copies the snapshot file to your local hard drive.

Last Backup Information

Product Version	8.0.0.1891
Timestamp	2014/03/05 11:01:06
Settings (includes perou per user settings)	Yes
Per User Settings	Yes
Reports data	Yes
Junk box	Yes
Archive	Yes

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

Settings (includes perou per user settings)	☑ Estimated time: 5 minute(s)
Per User Settings	☑ Estimated time: 1 minute(s)
Junk box	☐ Estimated time: 9 minute(s)
Archive	☐ Estimated time: 5 minute(s)
Reports data	☐ Estimated time: 1 minute(s)

3 Under the heading **Create a snapshot of the following data on the Email SEcurity Server,** select **Settings**.

4 Click **Take Snapshot Now** to create a snapshot.

5 Click **Download Snapshot** to save the snapshot to your local file system.

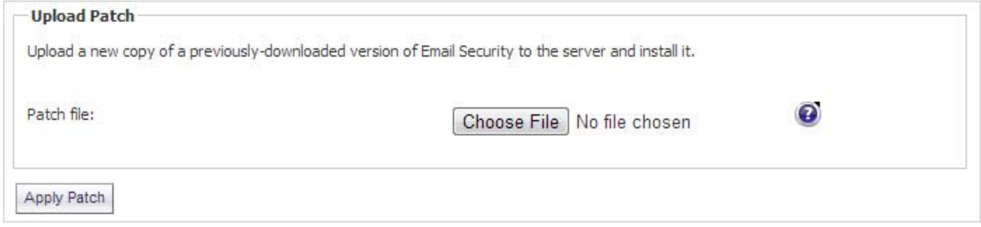
Upgrading Your Existing Firmware

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 the **System > Advanced** page and scroll down to the **Upload Patch** section, under **Miscellaneous Settings**.



Upload Patch

Upload a new copy of a previously-downloaded version of Email Security to the server and install it.

Patch file: No file chosen

4 Click **Choose File** to locate the Email Security firmware file on your local file system, and then click **Apply Patch**.

As part of the upgrade process, the Email Security appliance does reboot. The upgrade process could take quite a lot of time, depending on the size of your solution. All the settings and data are preserved.

△ CAUTION: **Your ES8300 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 ES8300 appliance, follow the startup and registration instructions detailed in the *ES8300 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

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:** Before upgrading Email Security on a Windows server, be sure the server has the latest updates and service packs installed.

To upgrade your existing Email Security installation:

1 Log into your MySonicWall account and download the new Email Security Software installation file to the server running Email Security.

2 On the server running Email Security, double-click the Email Security installation file.

3 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.

4 In the Welcome page of the installation wizard, click **Next**.

5 Read the License Agreement and then click **Next** to accept the agreement.

6 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 Email Security Software installation.

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

ⓘ **NOTE:** This folder should not be scanned by an anti-virus engine.

8 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.

9 On the Start Installation page, click **Next**.

10 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**.

11 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 management interface.

12 After the installation finishes, click **Finish** in the Installation Complete page. A browser window displays the links to the Email Security user interface and documentation.

Installing the Virtual Appliance

For information about installing SonicWall Email Security as a Virtual Appliance, see the ***Email Security Virtual Appliance Getting Started Guide***, available at: https://www.mysonicwall.com

SonicWall Support

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

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 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.

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/.

Legend

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

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

ⓘ **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 8/30/17

232-004052-00 Rev A