

## SonicWall™ Email Security 9.0

### Release Notes

February 2017

These release notes provide information about the SonicWall™ Email Security 9.0 release.

Topics:

- [About Email Security 9.0](#)
- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Product Licensing](#)
- [Upgrade and Installation Instructions](#)
- [SonicWall Support](#)

## About Email Security 9.0

Email Security 9.0 provides a flexible solution to protect email from spam, phishing, and viruses. This release extends Email Security to a new family of appliances that takes advantage of 64-bit architecture. The new appliances are the ESA 5000, ESA 7000 and ESA 9000. New features were added and enhancements were made as well. Refer to [New Features and Enhancements](#) for more details.

**IMPORTANT:** Because Email Security 9.0 is a 64-bit implementation and prior versions are 32-bit, SonicWall recommends a fresh deployment for Email Security 9.0.

Email Security 9.0 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 Platforms](#)
- [Software Requirements](#)
- [Virtual Appliance Requirements](#)

## Supported Platforms

Email Security 9.0 firmware is supported on the following SonicWall appliances:

### 32-Bit Versions

- Email Security 3300
- Email Security 4300
- Email Security 8300

### 64-Bit Versions

- Email Security Appliance 5000
- Email Security Appliance 7000
- 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 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) Microsoft Hyper-V Server 2008(64-bit) Windows Server 2012 R2 (64 bit) Windows Server 2012 (64 bit) Windows Server 2008 R2 (64 bit) Windows Small Business Server (SBS) 2008 (64-bit)

## Virtual Appliance Requirements

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

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

## New Features and Enhancements

Email Security firmware has been updated to run on three new appliances that are being released concurrently. In addition, new features were added and enhancements made to improve protection from spam, phishing and viruses.

New features and enhancements include:

- [Updated Email Security Appliances](#)
- [Capture ATP Integration](#)
- [Office 365 Support](#)
- [Improved Anti-Virus Offerings](#)
- [Performance Enhancements](#)

# Updated Email Security Appliances

The Email Security Appliances (ESA) have been refreshed. They are built using 64-bit architecture, offering increased memory and the option for faster, detachable disk drives. Appliance functionality focuses on:


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

Refer to the *Email Security Appliance 5000 and Email Security Appliance 7000 Getting Started Guide* and the *Email Security Appliance 9000 Getting Started Guide* 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. 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 anti-virus options (McAfee, Kaspersky, and Cyren) and Capture ATP need to be licensed separately 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 policy based on the final disposition of the message.

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

## Office 365 Support

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 ISP 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 9.0 improved its core virus filtering capability with improved Kaspersky and Cyren filtering engines. Email Security integrated the Kaspersky 8.5 Anti-Virus DAT and scan engine and the Cyren 5.4.25 AV scan engine into the Email Security gateway and backend servers. Both utilizes 64-bit specific data for both Windows and Linux platforms. Both engines provide improved scanning and filtering to detect malicious content.

## Performance Enhancements

Improvements have been made to the Email Security application that can lead to an improved user experience. Some message attributes can be sent to SonicWall for analysis. These features, when combined with other data, can be used to identify and track new trends in spam and other junk mail. Those trends can be used to refine configurations and filtering.

Be aware, when opting to share this information, some of the message attributes may contain human-readable information. Information about the sender, recipient, subject or content is accessible by SonicWall. It is, however, very difficult to recover the entire message that corresponds to a specific set of attributes.

## Resolved Issues

This section provides a list of resolved issues in this release.

### Administration

Resolved issue	Issue ID
Internet Explorer 11 cannot see Junk Box contents or auditing. Occurs after firmware upgrade to 8.3.1/8.3.2 and when customer enables <b>Display intranet sites in compatibility view</b> option.	179297
A scheduled backup isn't saved to the specified FTP destination. Occurs after updating to 8.3.2 while making use of special characters in the FTP password.	178780
Outbound paths do not support more than a class C subnet. Occurs when customers tried to use Office 365.	170510
On HES system, the global user view setup seems to override the per OU user view setup. Occurs when defining the user download settings. After navigating away from the page and then coming back to view it, it doesn't retain the settings you initially defined.	166525
Auditing fails to reveal attachment information. Occurs when trying to get details about an attachment and archiving is disabled.	162534

### Anti-Spoofing

Resolved issue	Issue ID
DKIM check fails. Occurs for emails sent from AOL.com when DKIM is enabled.	148258

## Organizations

Resolved issue	Issue ID
Unjunked messages are failing. Occurs when trying to delivery to Office 365, via the backup SMTP server setting.	166489

## Performance and Stability

Resolved issue	Issue ID
The logs directory grew such that the virtual appliance began to run out of space. Occurred when the log files continued to be saved without any automatic purging of older files.	181937

## Policy and Compliance

Resolved issue	Issue ID
Alerts for approval box are being sent regardless of what the alert settings indicate. Occurs whenever a policy action sends an alert to the approval box.	178446
Attachment Type option looks like viable selection if Security Compliance subscription is not licensed even through it shouldn't be available. Occurs when trying to add a new filter. Security Compliance subscription is not licensed; the Attachment Type can be seen even though the drop down list is not populated.	172706
Only users with administrative rights can approve emails stored in the approval box. Customers requested that certain users, someone other than the administrator, be allowed to approve or reject emails in the approval box.	51222

## Reports

Resolved issue	Issue ID
Junk Summary was being delayed from the time set on the Junk Summary page. Occurred when systems rolled to the new year, requiring an update to the time zone information file.	181701

## SMTP

Resolved issue	Issue ID
Emails to Gmail stop processing until the next retry. Occurs when multiple emails are sent and a specific message—mailbox over quota—is received.	179988

# Known Issues

This section provides a list of known issues in this release.

## Administration

Known issue	Issue ID
Under certain conditions the appliance hangs. An alert isn't sent about the condition, and the user can't access the appliance. Occurs when a mount point is no longer reachable.	183343

## Install, Update and Upgrade

Known issue	Issue ID
<p>Apache Tomcat fails to come up on 32-bit virtual machine (VM) in larger configurations.</p> <p>Occurs when the VM has 8 GB of RAM and multi-core CPU. Calculating the heap size for a VM with 8 GB of RAM results in a heap size greater than 2 GB which can cause failure if the OS is not large-address aware.</p> <p><b>Workaround:</b> Execute the following CLI commands to limit the Tomcat memory allocation to 2 GB and restart the Tomcat service to restore Email Security's user interface.</p> <pre>SNWLCLI&gt;setsearchengine -memory 2048</pre> <pre>SNWLCLI&gt;restart tomcat</pre>	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 policies 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 Environment](#)
- [Backing Up a Pre-8.3 Environment](#)

### Backing Up an 8.3 Environment

*To back up your existing 8.3 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.

- 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)	<input checked="" type="checkbox"/>	Estimated time: 5 minute(s)
Per User Settings	<input checked="" type="checkbox"/>	Estimated time: 1 minute(s)
Junk box	<input type="checkbox"/>	Estimated time: 9 minute(s)
Archive	<input type="checkbox"/>	Estimated time: 5 minute(s)
Reports data	<input type="checkbox"/>	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.

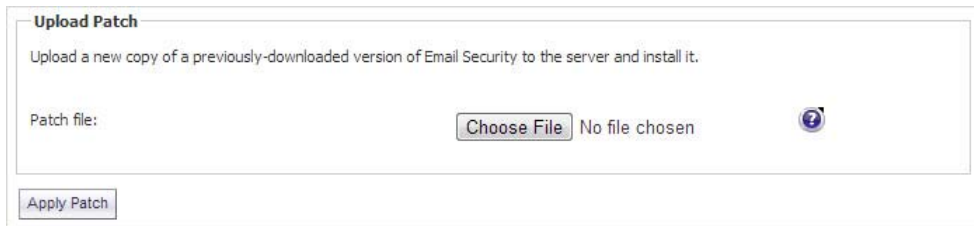
## Upgrading Your Existing Firmware

*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**.



- 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 10 to 20 minutes. 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.

### **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.

**NOTE:** Administrators must copy the installation file to the Email Security Server in order to run the installation file. Administrators cannot upgrade through the Web UI on Windows.

- 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://support.sonicwall.com/sonicwall-email-security/3300/technical-documents>

## SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support 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://support.sonicwall.com>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

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

Copyright © 2017 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

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/>.

The SonicWall End User Product Agreement (EUPA) can be viewed at <https://www.sonicwall.com/legal/eupa.aspx>. Select the language based on your geographic location to see the EUPA that applies to your region.

## 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.

SonicWall will provide a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, send your written request, along with a certified check or money order in the amount of US \$25.00 payable to "SonicWall Inc." to:

General Public License Source Code Request  
SonicWall Inc. Attn: Jennifer Anderson  
5455 Great America Parkway  
Santa Clara, CA 95054

Email Security Release Notes  
Updated - February 2017  
Software Version - 9.0  
232-003462-00 Rev A