SonicWall® Email Security

Release Notes

January 2018

These release notes provide information about theSonicWall® Email Security 9.1 release.

Topics:

About Email Security 9.1

Email Security 9.1 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.

Email Security 9.1 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. 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 9.1 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)

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

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

New Features and Enhancements

Email Security firmware has been updated with several new features and enhancements made to improve protection from spam, phishing and viruses and make administration easier.

- Email Continuity for Hosted Email Security
- MSP Management Support
- Improved Metadata Scanning for Attachments
- Enhanced User Interface
- RESTful API
- Performance Enhancements

Email Continuity for Hosted Email Security

SonicWall HES delivers Email Continuity against planned or unplanned downtime events, whether your email servers are on-premises, hybrid environments, or in the cloud. Continuity service is an add-on subscription that allows end users to compose and send new email, reply to existing email, and forward email using Email Continuity.

Email Continuity is automatically activated with the subscription. When an email outage occurs, the administrator is notified and users can access emails through the emergency inbox. During an outage SonicWall HES acts as the email server. All suspicious emails are quarantined and only safe email is stored in the **Email Continuity | Inbox**.

Once the primary email server is back online, any inbound email that was spooled is delivered to the downstream server. If licensed, 7 days of email remains in the **Email Continuity | Inbox** and continuity email is stored for 7 days.

MSP Management Support

This feature allows management of OUs in an on-prem setup for MSP customers in the way they are managed in the hosted version of Email Security. It introduces the concept of running the unit as an MSP and lets the customer manage individual OUs. The OUs are listed on the **Organizations** page (**System Setup | Users, Groups & Organizatins > Organizations** on the **MANAGE** view) for easy management.

Licenses for the OU for services like Encryption, Capture ATP, and DHA are inherited from the top level. The following features can be enabled for the on-prem OUs:

- Flood protection
- Zombie protection
- Connection management reports

NOTE: In the older Email Security versions, the OU admin role can only take limited actions on messages identified as spam, phishing attacks, or other threats.

Improved Metadata Scanning for Attachments

Support for scanning attachment content and matching details in meta data have been features in Email Security for a long time. However, the increasing number of attachment types prompted us to improve these features in 9.1. The goal of this feature is to empower attachment type identification and improve the attachment-name based filters without having to explicitly depend on opt-in for intelligent attachment matching.

We support dealing with attachments via following options when building policy filters:

- Scanning Attachment Contents
- Identifying attachment types
- Attachment name with intelligent attachment matching

Enhanced User Interface

The Email Security user interface adopted an enhanced menu structure that aligns commands under the key functions of **MONITOR**, **INVESTIGATE**, and **MANAGE**. The related commands on the left-hand menu are grouped under a divider labels for easier navigation. When you first log into your Email Security system, the **Dashboard** page on the **MONITOR** view is the default. The new interface structure is shown in the following table.

MONITOR

Dashboard

Event Summaries

- All Event Connections
- Anti-Spam
- Anti-Phishing
- Anti-Virus
- Anti-Spoof
- Directory Harvest
- Capture ATP

Policy & Compliance

- Policy
- Compliance
- Encryption

Appliance Health

- Live Monitor
- Performance Metrics
- LDAP Users

Current Status

- System Status
- MTA Status

INVESTIGATE

Junk Box

Email Continuity

- Inbox
- Outbox
- Sent

Logs

- Message Logs
- Connection Logs
- Capture ATP Logs

Tools

- Run DMARC Reports
- Audit Trail
- Diagnostics

MANAGE

Licenses Management

Firmware Update

▶Backup & Restore

Downloads

Policy & Compliance

- Filters
- Policy Groups
- ▶Compliance

System Setup

- ▶Server
- ▶Customization
- ▶Certificates
- ▶Users, Groups & Organizations
- ▶Network
- ▶Junk Box

Security Services

- ▶Anti-Spam
- Anti-Spoofing
- Anti-Phishing
- Anti-Virus
- Capture ATP
- Encryption Service
- Connection Management

Reporting

- Configure Known Networks
- Scheduled Reports

To toggle between the new interface and the old view of the interface, click the menu icon that appears in bottom left corner of the interface:

This toggle does not permanently retain the old view of the interface. To set the interface view permanently:

1 Navigate to **System Setup | Server > Administration** on the **MANAGE** view.

2 Scroll to **User Interface Preference** and make your selection. The default is the **Enhanced** (new) view.

3 Click **Apply Changes** to save the setting.

To see the table showing how the classic menu structure maps to the new enhanced menu structure, refer to the appendix provided in the administration guides.

RESTful API

A RESTful API (application programming interface) has been developed for Email Security. This allows customers to either script or build custom UI elements, in part or in full, to manage an Email Security unit if they don't want to use the default user interface shipped with the product. This may be especially useful to managed services providers (MSPs). The rest end-points are defined and can tested from the ES host by accessing https://<*eshostname*>/apidocs/docs.htm. The following features have REST endpoints defined for them:

- Authentication
- Capture
- Reports
- Branding
- Audit, Junkbox and Audit Trail
- Backup and Restore
- Anti-Virus
- Anti-Phishing/Fraud
- Anti-Spam

Performance Enhancements

A number of enhancements have been made to the Email Security application that can lead to improved performance or improved user experience.

- An updated McAfee engine provides improved scanning and filtering to detect malicious content. Added features are provided to manage anti-virus downloads more effectively.
- Spam classification has been refined and improved, including a new plugin that can better evaluate wither a given message is *good* or *spam*.
- The Kaspersky virus engine can be turned off. Navigate to **Security Services | Anti-Virus** on the **MANAGE** view. Scoll down to **Manages Virus Engines** and check the box next to **Disable Kaspersky**. Apply changes to save your settings.
- New country codes have been added to allow broader coverage and improve the effectiveness of categorizing threats.
- The ability to configure policy filters using address fields and **Reply-to** was added.
- Dynamic tags in **ends_with** conditions set on address fields is now supported.

Resolved Issues

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

Administration

Resolved issue	Issue ID
Group administrators can no longer see Junkbox contents of group members.	197685

Anti-Virus

Resolved issue	Issue ID
HES Capture in AMS is causing message delivery delays. May occur with attachments or without.	189401

Effectiveness

Resolved issue	Issue ID
English language messages are randomly being falsely identified as foreign languages resulting in them being identified as spam.	176140

Email Security on UTM

Resolved issue	Issue ID
CASS servers not accepting email after Mysql service crashed.	189643

Localization

Resolved issue	Issue ID
Capture ATP Exception changes value to decimals instead of filenames when language was changed to French.	194614

Organizations

Resolved issue	Issue ID
No junk box summaries.	191972

SMTP

Resolved issue	Issue ID
An archive bomb (highly compressed file with multiple layers of archives within it) attachment causes CPU to spike to 100% and stay there and the message never processes.	191544
HES customers cannot always save the setting to use O365 for outbound mail. Service cannot be used for outbound mail or Encryption Service.	186784

Known Issues

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

Administration

Known issue	Issue ID
Custom Branding settings applied to CC is not applied in RA	197504
When using **Quick Settings** on the **MANAGE | System Setup | Customization > Branding** page to customize new images for the logon backdrop, page header, and pop-up header, the new images do not get applied to the interface.	197435
Flood Protection experiences a 5- to 10-minute delay after updating Flood Protection settings.	195530
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

Reports

Known issue	Issue ID
When downloaded in pdf or JPEG format, performance metrics reports should show time information based on system time instead of GMT.	198393

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:

- **Nodes/Users:** Identifies the number of nodes or users that are licensed for this instance.
- **Email Security:** This is the primary license for Email Security.
- **Email Protection Subscription (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 Advanced Threat Protection:** Provides analysis of threats by examining their behavior in a managed environment.
- **Email Continuity:** Provides Email Continuity against planned or unplanned downtime events.

Upgrade and Installation Instructions

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

Topics:

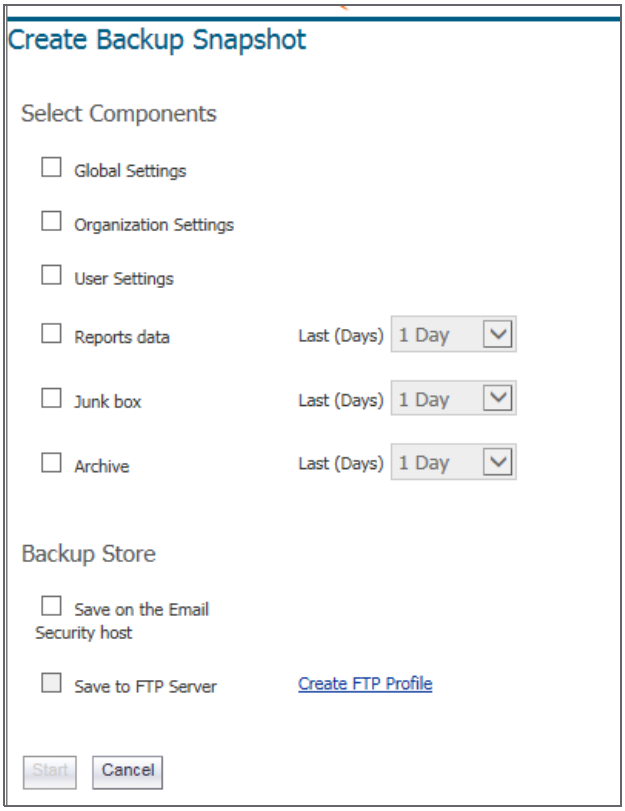
Backing Up Your Existing Environment

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 a Post-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.

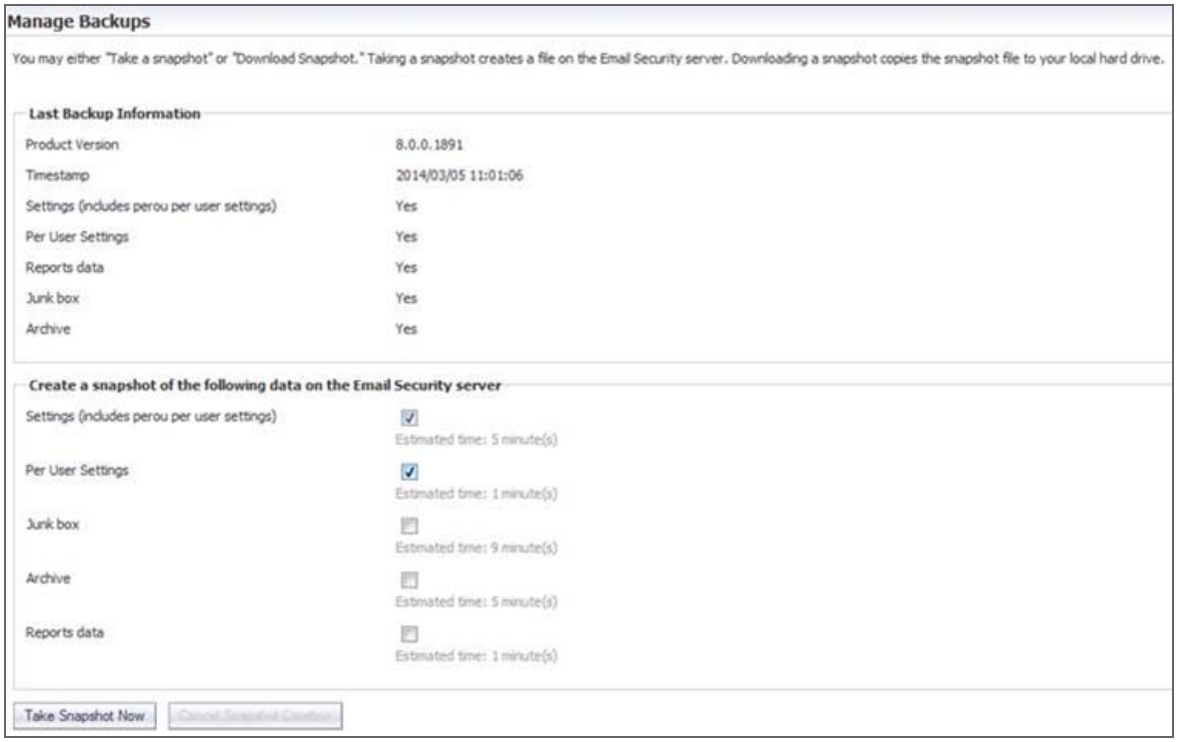
On the **Schedule Backup** page, messages report the status of the backups, and the task appears in the Backup Snapshots list on the **Manage Backups** page.

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**.



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.

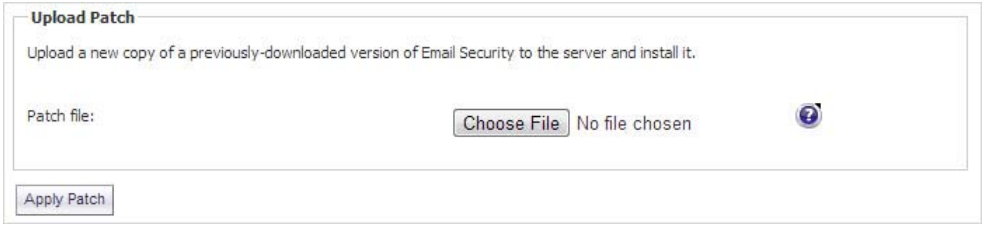
Upgrading Your Existing Firmware

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.

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.

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

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 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.

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.

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: 1/29/18

232-004189-00 Rev A