Dell™ SonicWALL™ Email Security 8.3.2

Release Notes

October 2016

These release notes provide information about the Dell™ SonicWALL™ Email Security 8.3.2 release:

About Email Security 8.3.2

Email Security 8.3.2 provides a flexible solution to protect email from spam, phishing, and viruses. The fixes included in this release resolve some reported vulnerabilities. Refer to Resolved issues for more information.

Email Security 8.3.2 is supported 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 appliances

Email Security 8.3 firmware is supported on the following SonicWALL appliances:

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

Software requirements

When installed as software, SonicWALL Email Security 8.3 is supported on systems that meet the following requirements:

Requirement	Definition
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 auditing 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 8.3.2 is supported on systems that meet the following requirements:

Requirement	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

w

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

Resolved issues

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

Email Encryption

Resolved Issue	Issue ID
Email Security reports an error when trying to communicate with Encryption Service. Occurred only when using Encryption Services on the Windows version of Email Security.	178170

Install, Update & Upgrade

Resolved Issue	Issue ID
A MySQL vulnerability was identified and corrected. Occurred when updating the Windows version of Email Security.	178173

Security and Compliance

Resolved Issue	Issue ID
An upload capability can be abused to retrieve files from the host. The vulnerability exists when a certain set of conditions exist for uploading files.	177413
Arbitrary files can be deleted. Occurs if someone with proper authentication makes the system believe a proper delete function is being requested.	177381
Remote commands can be executed by substituting values in certain config files. Occurs if someone with proper authentication substitutes an executable string in certain fields of a config file.	177368
Sensitive information may be exposed. Occurs if someone with proper authentication opts to leverage a vulnerability to download sensitive files.	177362
A flaw in a limiting mechanism allows a patient attacker to be able to inject packets into client/server session. Can occur when a certain rate limit is reached on a long lived connection.	176725

Known issues

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

Administration

Known Issue	Issue ID
Redirecting access from HTTP to HTTPS fails Occurs after restoring the system from a snapshot. The following options must be manually enabled after the snapshot restore to get the redirect to work again: **Enable HTTPS (SSL) access on port** and **Redirect access from HTTP to HTTPS**.	177431
Branding packages that are not in use at the time of the Email Security upgrade are not updated with the UI element changes. When a customer has multiple branding packages defined, only the branding package that is active and applied gets updated during the upgrade. The other packages are not updated and are missing required CSS files, causing the branding to break if any of them were applied. Download the package from the web site, make the required changes within the payload, and upload it again. Once the upload is completed, select this package and select **Apply**. New settings are enforced after that.	173630

Product licensing

SonicWALL Email Security appliances must be registered on MySonicWALL to enable full functionality and the benefits of SonicWALL security services, firmware updates, and technical support.

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

- **Node/Users:** Indicates the number of users to which the license applies.
- **Email Security:** Base license that comes with the software and enables basic components. It allows the use of basic policy filters.
- **Email Protection (Anti-Spam and Anti-Phishing):** This license 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 Cyren:** Provides updates for Cyren 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 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.
- **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 Security Transition:** One-time upgrade from the trial-type, limited-term base key to the perpetual key. For new installations, it is displayed as "Perpetual" to start with.

Upgrade and installation instructions

The following sections describe how to prepare for upgrading by backing up the current environment on an Email Security appliance, how to upgrade firmware on an existing Email Security appliance, how to upgrade software on an existing Email Security Software installation, and how to find information about installing Email Security as a Virtual Appliance.

Backing up your existing environment

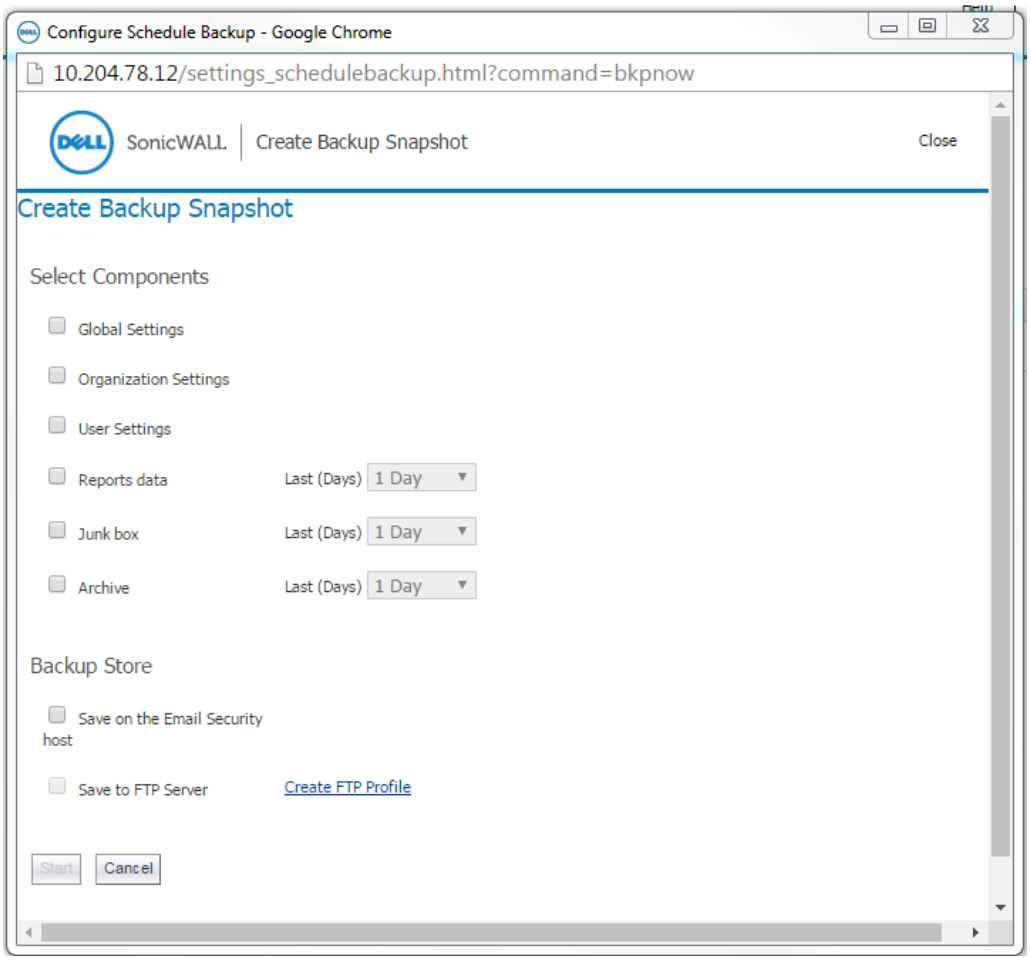
Before you upgrade your appliance firmware, you should back up your existing environment. This allows you to restore it if you decide to change back for some reason. Your backup should include the settings files, including User Settings. Choose the backup process appropriate for your version of software:

Backing up an 8.3 environment

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 Select **Backup Now** on the **Schedule Backup** page.



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.

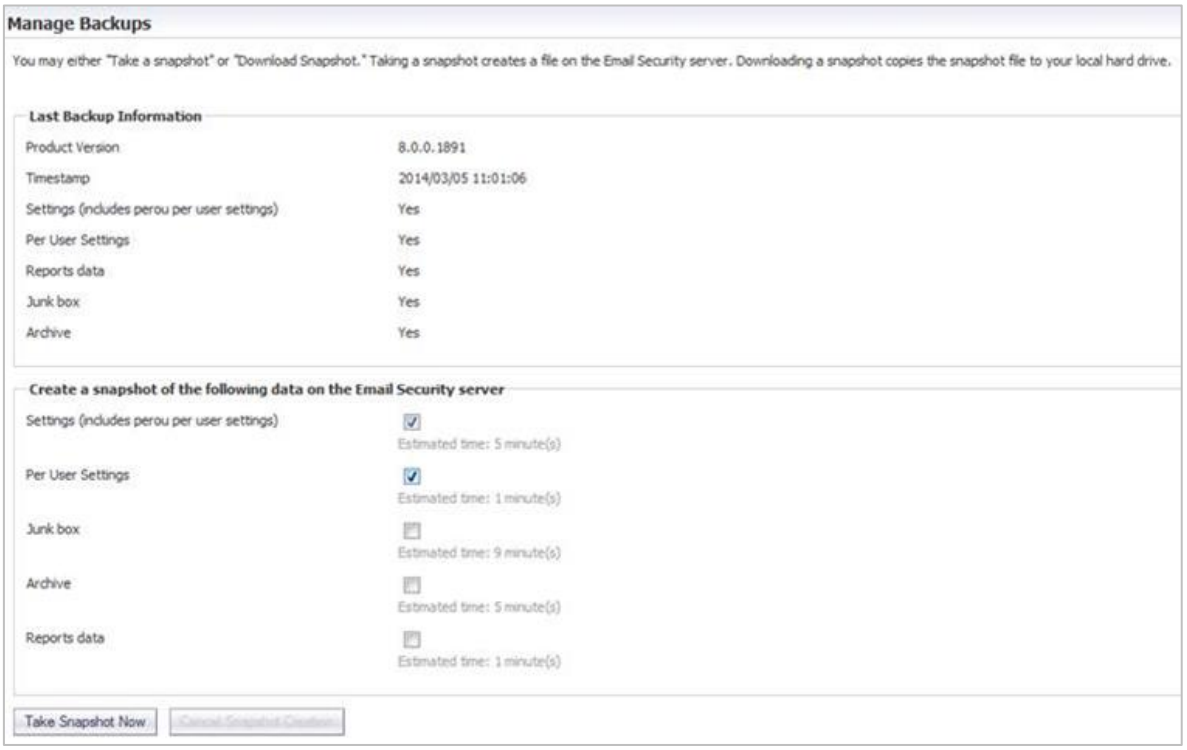
6 Click on **Start** to begin the backup. On the Schedule Backup page, messages report the status of the backups, and the task appears in the Backup Snapshots list on the **Manage Backups** page.

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. You 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.

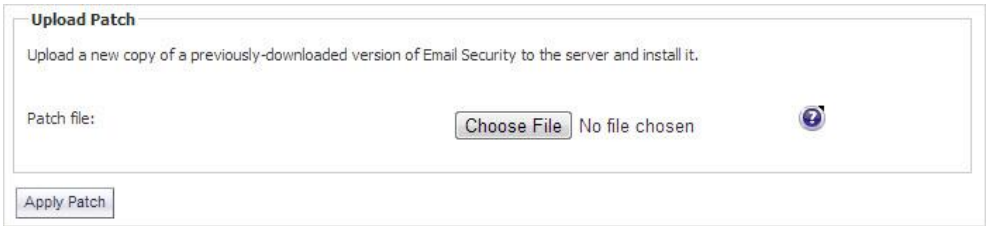
Upgrading your existing firmware

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**.

5 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 for ES8300 Appliances: 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 *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. 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.

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

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

5 Dell 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 Dell SonicWALL Email Security may be diminished without them. Asian language packs can be installed before or after Email Security Software installation.

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

NOTE: It is important that this folder is not scanned by an anti-virus engine.

7 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.

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

9 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. Dell SonicWALL recommends port **8080**. 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.

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

Installing the Virtual Appliance

For information about installing Dell SonicWALL Email Security as a Virtual Appliance, see the ***Dell SonicWALL Email Security Virtual Appliance Getting Started Guide***, available at:

https://support.software.dell.com/sonicwall-email-security/Virtual%20Appliance/release-notes-guides

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit http://www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to http://support.software.dell.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to http://software.dell.com/trials.
- View how-to videos
- Engage in community discussions

Legend

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.

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

Last updated: 10/3/2016

232-003123-00 Rev B