Dell™ SonicWALL™ Email Security 8.3

Release Notes

June 2016

These release notes provide information about the Dell SonicWALL™ Email Security 8.3 release:

About Email Security 8.3

Email Security 8.3 provides a flexible solution to protect email from spam, phishing, and viruses. In addition to fixing a number of known issues from previous releases, the new features for this release include:

- User interface changes
- Effectiveness enhancements
- Connection management
- SMTP authentication support
- Encryption strength for TLS over SMTP
- Backup and restore
- Reporting enhancements
- Audit and Junk Box user interface
- MTA Queue Management
- New Monitor Configure feature
- Policy feature enhancements
- Finnish language support

See New features and Resolved issues for more information. This release includes all features and resolved issues from earlier Email Security 8.2.x releases.

Email Security 8.3 is supported on Dell SonicWALL Email Security appliances, as a software installation on Windows Server systems, and as a Virtual Appliance on VMware ESX/ESXi platforms.

See the following sections for detailed requirements:

- Supported appliances
- Software requirements
- Virtual Appliance requirements

Supported appliances

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

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

Software requirements

When installed as software, Dell 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)

NOTE: Email Security 8.3 software is *not* supported on Windows running on VMware. Only the Email Security Virtual Appliance is supported on VMware platforms.

Virtual Appliance requirements

When installed as a Virtual Appliance, Dell SonicWALL Email Security 8.3 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	ESX 5.1 and newer ESXi 5.1 and newer

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.

New features

The following subsections summarize the new features for the Email Security 8.3 release:

- User interface changes
- Effectiveness enhancements
- Connection management
- SMTP authentication support
- Encryption strength for TLS over SMTP
- Backup and restore
- Reporting enhancements
- Audit and Junk Box user interface
- MTA Queue Management
- New Monitor Configure feature
- Policy feature enhancements
- Finnish language support

User interface changes

The look and feel of the user interface for Email Security 8.3 has been updated. Very little functionality has changed, but the elements that make up the interface have a cleaner appearance. The following summarizes the changes:

- Removed all icons from the navigation.
- Removed the **Assist** link.
- Changed background and font colors.
- Removed many box and border elements.
- Changed the appearance of tabs to buttons.

- Changed the searching and filtering navigation controls for **Audit Trail**, **Auditing > Messages**, and **Junk Box Management > Junk Box**. Refer to Audit and Junk Box user interface for more information on these changes.

Effectiveness enhancements

To improve the effectiveness of Email Security 8.3, a new spam detection engine was developed. It utilizes the following features:

- Expanded the number of thumbprint types that can now be queried at the one-minute update interval. Previously, these thumbprints had a minimum query frequency of five minutes.
- Changed the format of the IP address thumbprint. This thumbprint now supports CIDR range notation. This reduces the size required to store these thumbprints in the local database.
- Retrained the Adversarial Bayesian model for better spam catch rate and lower false positive incidences.
- Added a new machine learning model. While similar in some respects to our Adversarial Bayesian technique, this new technique uses a Support Vector Machine approach to identifying spam. These two techniques complement each other with the ability to catch spam that the other may miss.

Connection management

Several connection management features were added or enhanced for Email Security 8.3:

- Delayed connection management
- Enhanced Allowed List
- Auditing connections

Delayed connection management

In Email Security 8.3, the system administrator can opt to delay how long a malicious connection stays connected. Rather than immediately dropping the connection, the goal is to maintain the connection long enough to find out who the sender or recipients are. Once this information is known, the connection is dropped. Delayed connection management applies to IP Reputation, Greylisting, the Deferred List, and the Blocked List.

This feature also allows administrators to develop an *Allowed List* of senders that overrides the application's judgments. That way mail from senders on the Allowed List will be delivered even it comes from an IP address with a known issue.

Delayed connection management can be configured under **System > Connection Management**. Scroll towards the bottom of the page to the segment titled **Delayed Connection Management** and set the timing for rejected connections. The default is to drop the connection as soon as possible so delaying the dropped connections must be actively enabled and changes applied. The option to manually edit the IP address list is in the same area of the page.

Enhanced Allowed List

The Connection Management function (**System > Connection Management**) was enhanced so emails addresses and domains can be added to the Allowed List. Select **Edit Allowed List** at the bottom of the page and enter sender domain and email addresses as needed.

Auditing connections

The Auditing function has been enhanced to include auditing the connections log. Go to **Auditing > Connections**. You can select **Settings** to define the auditing parameters for the connections log files. Other

options allow you to configure the contents of the data table and refresh the data. You can also sort the data (ascending and descending) by clicking on the heading or filter the data using the drop-down menus by each heading.

SMTP authentication support

The new SMTP authentication support for Email Security 8.3 can be used to protect the customer's infrastructure from unauthorized use. For example, requiring a user to authenticate before sending outbound email can prevent an open relay.

NOTE: Authentication does not protect the *contents* of the email; encryption should be used for that.

Three authentication scenarios are being supported:

- Client-side authentication
  The most common situation for client-side authentication is for those customers that run their outbound mail through an ISP. The ISP requires authentication to prevent an open relay. A single credential is used for all outbound mail that identified the Email Security system to the ISP.
- Server-side authentication
  On the server side, customers want to require some or all of the users to authenticate with the Email Security system before they are allowed to send outbound mail. For example, one may want to allow onsite employees to send email without authentication, but want a separate path for offsite employees who need to be authenticated. Server-side authentication might also be used to ensure that unauthorized users are not routing their email through our customers' appliances.
- EMS relaying authentication commands
  The customer wants to send mail through the Email Security system first and then through an external mail server. To prevent an open relay, the external mail server requires the original sender to authenticate before it accepts mail. This situation is not common, but it sometimes comes up when a small business unit is owned or acquired by a larger business. In this situation the Email Security system doesn't actually do any authentication, but relays the authentication commands downstream for the external mail server to do the authentication.

SMTP Authentication can be configured under **System > Network Architecture > Server Configuration** on either the inbound or outbound path. Select **Add Path** and scroll to the bottom of the page that pops up. Select **Configure Authentication**. On the next page define the authentication credentials and encryption requirements.

SMTP Authentication is supported only for outbound paths on HES, not on inbound paths. Also, only server-side and client-side authentication is supported on HES. Relaying authentication commands downstream will not be supported.

Encryption strength for TLS over SMTP

When TLS over SMTP is enabled, one of three levels of encryption strength can selected. Select **System > Network Architecture > Server Configuration.** Select **Add Path** on either the Inbound or Outbound Email Flow. Scroll to the bottom and select **Configure STARTTLS**. Define the TLS settings and choose the appropriate Cipher Strength.

Cipher Strength	Definition
Strong	American AES (128 bits or higher) and Japanese Camellia (128 bits or higher). This setting is not the default since it will not interoperate with Exchange 2003. This is the recommended setting when mandatory TLS is enabled on the same path.
Normal	In addition to the strong ciphers, supports the American Triple-DES (3DES) and South Korean SEED (128 bits) ciphers. This is the recommended setting for public-facing paths that must interoperate with older SMTP servers.
Weak	In addition to all strong and medium ciphers, the American RC4 (128 bits) cipher is supported, and Discrete Logarithm Ephemeral Diffie-Hellman (EDH) key exchange is supported when the proxy is acting as a client. In addition, the MD5 hash is allowed in the HMAC. *This setting should only be used when the only alternative is clear text.*

The complete set of ciphers for Email Security 8.3 is listed in the following table:

OpenSSL Cipher string Name	TLS	Key Exchange	Authenticator	Cipher	HMAC	PFS
Strong Ciphers						
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD	Yes
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD	Yes
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384	Yes
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384	Yes
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1	Yes
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1	Yes
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH/RSA	ECDH	AESGCM(256)	AEAD	
ECDH-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH/ECDSA	ECDH	AESGCM(256)	AEAD	
ECDH-RSA-AES256-SHA384	TLSv1.2	ECDH/RSA	ECDH	AES(256)	SHA384	
ECDH-ECDSA-AES256-SHA384	TLSv1.2	ECDH/ECDSA	ECDH	AES(256)	SHA384	
ECDH-RSA-AES256-SHA	SSLv3	ECDH/RSA	ECDH	AES(256)	SHA1	
ECDH-ECDSA-AES256-SHA	SSLv3	ECDH/ECDSA	ECDH	AES(256)	SHA1	

OpenSSL Cipher string Name	TLS	Key Exchange	Authenticator	Cipher	HMAC	PFS
AES256-GCM-SHA384	TLSv1.2	RSA	RSA	AESGCM(256)	AEAD	
AES256-SHA256	TLSv1.2	RSA	RSA	AES(256)	SHA256	
AES256-SHA	SSLv3	RSA	RSA	AES(256)	SHA1	
CAMELLIA256-SHA	SSLv3	RSA	RSA	Camellia(256)	SHA1	
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD	Yes
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH	ECDSA	AESGCM(128)	AEAD	Yes
ECDHE-RSA-AES128-SHA256	TLSv1.2	ECDH	RSA	AES(128)	SHA256	Yes
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	ECDH	ECDSA	AES(128)	SHA256	Yes
ECDHE-RSA-AES128-SHA	SSLv3	ECDH	RSA	AES(128)	SHA1	Yes
ECDHE-ECDSA-AES128-SHA	SSLv3	ECDH	ECDSA	AES(128)	SHA1	Yes
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH/RSA	ECDH	AESGCM(128)	AEAD	
ECDH-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AESGCM(128)	AEAD	
ECDH-RSA-AES128-SHA256	TLSv1.2	ECDH/RSA	ECDH	AES(128)	SHA256	
ECDH-ECDSA-AES128-SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AES(128)	SHA256	
ECDH-RSA-AES128-SHA	SSLv3	ECDH/RSA	ECDH	AES(128)	SHA1	
ECDH-ECDSA-AES128-SHA	SSLv3	ECDH/ECDSA	ECDH	AES(128)	SHA1	
AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM(128)	AEAD	
AES128-SHA256	TLSv1.2	RSA	RSA	AES(128)	SHA256	
AES128-SHA	SSLv3	RSA	RSA	AES(128)	SHA1	
CAMELLIA128-SHA	SSLv3	RSA	RSA	Camellia(128)	SHA1	

OpenSSL Cipher string Name	TLS	Key Exchange	Authenticator	Cipher	HMAC	PFS
			Normal Ciphers			
SEED-SHA	SSLv3	RSA	RSA	SEED(128)	SHA1	
ECDHE-RSA-DES-CBC3-SHA	SSLv3	ECDH	RSA	3DES(168)	SHA1	Yes
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	ECDH	ECDSA	3DES(168)	SHA1	Yes
ECDH-RSA-DES-CBC3-SHA	SSLv3	ECDH/RSA	ECDH	3DES(168)	SHA1	
ECDH-ECDSA-DES-CBC3-SHA	SSLv3	ECDH/ECDSA	ECDH	3DES(168)	SHA1	
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168)	SHA1	
			Weak Ciphers			
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	DH	DSS	AESGCM(256)	AEAD	Yes
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM(256)	AEAD	Yes
DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES(256)	SHA256	Yes
DHE-DSS-AES256-SHA256	TLSv1.2	DH	DSS	AES(256)	SHA256	Yes
DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES(256)	SHAI1	Yes
DHE-DSS-AES256-SHA	SSLv3	DH	DSS	AES(256)	SHAI1	Yes
DHE-RSA-CAMELLIA256-SHA	SSLv3	DH	RSA	Camellia(256)	SHAI1	Yes
DHE-DSS-CAMELLIA256-SHA	SSLv3	DH	DSS	Camellia(256)	SHAI1	Yes
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	DH	DSS	AESGCM(128)	AEAD	Yes
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	DH	RSA	AESGCM(128)	AEAD	Yes
DHE-RSA-AES128-SHA256	TLSv1.2	DH	RSA	AES(128)	SHA256	Yes

OpenSSL Cipher string Name	TLS	Key Exchange	Authenticator	Cipher	HMAC	PFS
DHE-DSS-AES128-SHA256	TLSv1.2	DH	DSS	AES(128)	SHA256	Yes
DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES(128)	SHA1	Yes
DHE-DSS-AES128-SHA	SSLv3	DH	DSS	AES(128)	SHA1	Yes
DHE-RSA-SEED-SHA	SSLv3	DH	RSA	SEED(128)	SHA1	Yes
DHE-DSS-SEED-SHA	SSLv3	DH	DSS	SEED(128)	SHA1	Yes
DHE-RSA-CAMELLIA128-SHA	SSLv3	DH	RSA	Camellia(128)	SHA1	Yes
DHE-DSS-CAMELLIA128-SHA	SSLv3	DH	DSS	Camellia(128)	SHA1	Yes
ECDHE-RSA-RC4-SHA	SSLv3	ECDH	RSA	RC4(128)	SHA1	Yes
ECDHE-ECDSA-RC4-SHA	SSLv3	ECDH	ECDSA	RC4(128)	SHA1	Yes
ECDH-RSA-RC4-SHA	SSLv3	ECDH/RSA	ECDH	RC4(128)	SHA1	
ECDH-ECDSA-RC4-SHA	SSLv3	ECDH/ECDSA	ECDH	RC4(128)	SHA1	
RC4-SHA	SSLv3	RSA	RSA	RC4(128)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	RC4(128)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES(168)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES(168)	SHA1	

NOTE: TLS v1.2 Galois/Counter Mode (GCM), Authenticated Encryption with Associated Data (AEAD), and SHA-2 hashes are only available when the client uses TLS v1.2. All TSL v1 ciphers are available when the client uses TLS v1.2, except for RC4, which is always disabled with TLS v1.1 and above.

NOTE: The changes from Release 8.2 to 8.3 are:

- All ciphers using less than 128-bit encryption (the former *weak* ciphers) have been removed and are no longer available.
- The RC4 cipher has been moved to the Weak cipher category
- The DHE authenticator has been moved to the Weak cipher category.
- 3DES is no longer included in the Strong cipher set; it is included in the Normal and Weak categories.

Backup and restore

The Backup and Restore function has been improved to allow more flexibility, ease of use and more granular chunks of data to be backed up. Large data will be broken up into multiple snapshots of less than 1 GB with each file being stored independently. The components that can be selected for a backup are:

- Global settings
- User settings
- Organization settings
- Archive
- Junk Box
- Reports database

The administrator has complete control over what to back up, when to do it, how often it is done, and where to store it. The backup can be created as an instant backup, or snapshot, of a selected component or scheduled at periodic intervals. A specific amount of disk space can also be allocated for the backups. Settings are always backed up in their entirety. The data can be stored locally or remotely on an FTP server.

NOTE: Backups cannot happen concurrently, so instant backups cannot be started if a scheduled backup is already in progress. Similarly, a backup cannot start while a restore is in progress.

Restores can only be started one snapshot at a time, but cannot be initiated if a backup is already in progress. A restore can fail if there is insufficient disk space to store the uploaded snapshot file or to extract it.

To access the backup and restore commands, select **System > Backup/Restore**:

- **Manage Backups**
  Allows you to backup snapshots, restore a snapshot file, manage settings and view backup and restore history.
- **Schedule Backups**
  Allows you to add a scheduled backup or do an instant backup.
- **FTP Profiles**
  Allows you to figure FTP profiles so that snapshot backups and scheduled backups can be stored on your FTP server.

IMPORTANT: After upgrading to Email Security 8.3, no pre-8.3 snapshots are listed in the user interface for restore. Customer should back up their system immediately after upgrade.

Reporting enhancements

A number of improvements were made in the Reporting & Monitoring function:

- User statistics reports
- Schedulable Dashboard Report
- Performance metrics reports

User statistics reports

New user statistics reports have been added to the reporting function. Go to **Reports & Monitoring > Reports > User Statistics** to see the following data:

- Domain Person vs. Group Email Addresses
- Domain Primary vs. Alias Email Addresses
- Organization Person vs. Group Email Addresses
- Organization Primary vs. Alias Email Addresses

Data can be shown in the form of a bar char or a table. The data is updated each hour for the current day and will remain in the database until it ages out. The age-out is based on what gets configured for Reports.

Schedulable Dashboard Report

The Dashboard Report is now one of the report options that can be scheduled:

1. Select **Reports & Monitoring > Scheduled Reports**.
2. Select **Add New Scheduled Report**.
3. In the Which Report field, select **Dashboard**.
4. Define the remaining parameters to schedule the dashboard report and save the settings.

Performance metrics reports

Under **Reports > Performance Metrics** you have the option of monitoring any of several system metrics by selecting from the list provided. You can select a graphical or table format to display the data. You can also enable or disable any of the processes by clicking on the legend at the bottom of each chart.

Audit and Junk Box user interface

The user interface for **Audit Trail**, **Auditing > Messages**, and **Junk Box Management > Junk Box** have been updated to be more intuitive and flexible for configuration and viewing. The new navigation and data configuration are summarized in the table below:

Action	Description
Adding or moving columns	Click on **Add Columns** and then check an option to include it in the table and uncheck it to remove it. Columns can be moved in the table by dragging-and-dropping to the desired location. Once the table is configured as you like, click on **Save View** to retain your settings.
Sorting	To sort a column, click on a column heading. A small arrowhead will appear in the heading area to indicate whether the data is sorted in ascending or descending order.
Filtering	Select the drop-down menu on a heading. Check the box by **Filtering** and enter the text string you want to search for. The data table shows immediate results. Click on **Clear Filters** to undo any filters you defined.
Simple search	Enter the search string in the text field at the top of the page, select the field to search in, and click on **Search**.
Advanced search	The advanced search function has been replaced by filtering (see above). You can filter on one or more headings to get as refined as needed.
Settings	The Settings button opens the settings page for that function.

MTA Queue Management

The interface for **Reports & Monitoring > MTA Status** has been updated so that customers are able to view and manage the MTA queue for each RA (remote analyzer) from the control center rather than having to log into each appliance separately. Administrators can see both the inbound and outbound paths. A detailed view is also provided so administrators can see any messages associated with a particular queue.

New Monitor Configure feature

A new configuration feature has been added to the **System > Monitoring** page. At the bottom of the page in the **Monitor Configure** section, you can adjust the **MTA Process Queue Size Alert**. Set the value and apply it. You can also apply the default value or revert to the prior value.

Policy feature enhancements

The Policy filters are typically defined by global administrators and OU administrators; however, group administrators and users may also use select filters for incoming traffic. See the following table for the updated filter list.

Policy Filter	Global Admin	OU Admin	Group Admin	User
Spam/Phishing Judgment	Available	In hosted version	Not available	Not available
Likely Spoof Judgment	Available	In hosted version	Not available	Not available
Address Book	Available	In hosted version	Not available	Not available
From	Available	Available	Available	Available
To/CC/Bcc	Available	Available	Available	Available
Subject	Available	Available	Available	Available
Body	Available	Available	Available	Available
Subject or Body	Available	Available	Available	Available
Subject, Body, or Attachment	Available	Available	Available	Available
Message Header	Available	Available	Available	Available
Attachment Name	Available	In hosted version	Not available	Not available
Attachment Contents	Available	In hosted version	Not available	Not available
Attachment Type	Available	In hosted version	Not available	Not available
Country Code	Available	Available	Available	Available

NOTE: User filters are not available on the outbound path.

In addition, when adding or editing a filter, support for the Not Equal condition has been added. The condition will appear as **is not** [something] in the Matching field on the Add New Filter page. Similar wording is used on the Edit Filter page, like **does not** or **without**, to show criteria that doesn't match the condition.

Finnish language support

Support for Finnish language has been incorporated. Go to **Anti-Spam > Languages**. Finnish appears in its alphabetical position, and you can choose to **Allow All** email in Finnish, **Block All** email in Finnish or have **No Opinion**.

Resolved issues

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

Administration

Resolved Issue	Issue ID
User logins sometimes fail after upgrading from 8.2.1 to 8.2.2. Occurs when the same user exists in multiple LDAP domains.	171324
Chinese characters in the GB2312 character set are displayed incorrectly in audit log. Occurs when clients include characters that are only allowed in the GB18030 character set in strings tagged as GB2312.	169959
Unencrypted passwords can be displayed on the LDAP configuration page. Occurs the administrator selects **Edit** on the **System > LDAP Configuration** page.	167687
Search terms in Auditing were not case sensitive in older versions but are in version 8.2. Occurs when searching **Auditing > Messages** and **Junk Box Management > Junk Box** when querying the From and To address.	167028
Only first page of data is exported by the **Export to cvs** on the **Auditing > Messages** page on either the Inbound or Outbound view. Occurs when clients include characters that are only allowed in the GB18030 character set in strings tagged as GB2312.	163544

Anti-Virus

Resolved Issue	Issue ID
Some macro viruses are not detected. Occurs when the Kaspersky heuristics option is not enabled. Note: This issue has been resolved in the Email Security Appliance builds. It is not yet available for Windows versions.	169950

Security and Compliance

Resolved Issue	Issue ID
Information leaks through cache-bank conflicts can be exploited through side channel attacks. Occurs when minute timing variations are observed, which can pinpoint a potential attack.	171398

Firmware

Resolved Issue	Issue ID
A method is needed to increase the storage space available on an Email Security Virtual Appliances. Occurs when data has grown to exceed the limit set at the time of creation.	164591

Known issues

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

Administration

Known Issue	Issue ID
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
If Arabic, Hebrew, or Portuguese are blocked, MS Outlook sometimes incorrectly encodes a message as Arabic or Hebrew under certain circumstances, and some English messages are incorrectly detected as Portuguese. Some spam email messages are seen in English with a background encoded in different character sets such as Cyrillic, Baltic, or Turkish. This is done by spammers to bypass the anti-spam mechanism that only scans for words in English. In general, unless used, Dell SonicWALL recommends that these character sets be excluded. Common languages such as Spanish and German are normally not blocked.	N/A

Product licensing

Dell SonicWALL Email Security appliances must be registered on MySonicWALL to enable full functionality and the benefits of Dell 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
- Upgrading your existing firmware
- Upgrading your existing software
- Installing the Virtual Appliance

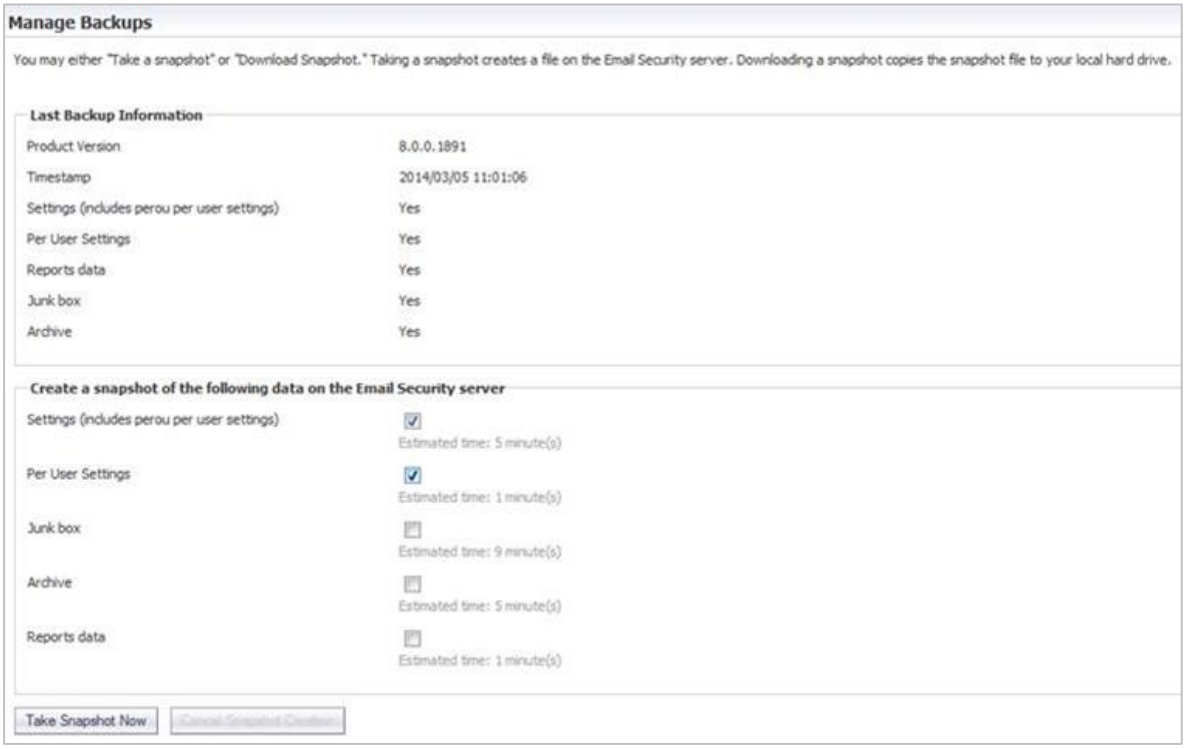
Backing up your existing environment

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

To back up your existing environment:

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

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

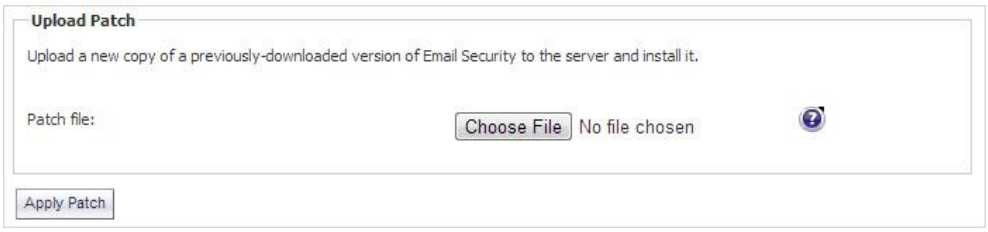
Upgrading your existing firmware

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 will reboot. The upgrade process could take 10 to 20 minutes. All the settings and data will be 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 will not be able to 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
- Chat with a support engineer

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: 6/23/2016

232-003295-00 Rev A