Release Notes

Email Security

Dell SonicWALL Email Security 7.4.5

Contents

System Compatibility

For Appliances

Dell SonicWALL Email Security 7.4.5 firmware is supported on the following appliances:

- Dell SonicWALL Email Security 200
- Dell SonicWALL Email Security 300
- Dell SonicWALL Email Security 400
- Dell SonicWALL Email Security 500
- Dell SonicWALL Email Security 3300
- Dell SonicWALL Email Security 4300
- Dell SonicWALL Email Security 6000
- Dell SonicWALL Email Security 8000
- Dell SonicWALL Email Security 8300

For Software

When installed as software, Dell SonicWALL Email Security 7.4.5 is supported on systems that meet the following requirements:

- Operating Systems:
  - Windows Server 2008
  - Windows Server 2008, R2 (64-bit)
  - Windows Server 2012 (64-bit)
  - SBS 2011 (64-bit)

  Note: Dell SonicWALL Email Security 7.4.5 Software is *not* supported on Windows running on VMware. Use the Email Security Virtual Appliance on VMware platforms.

- Hardware Requirements:
  - Intel Pentium: P4 or compatible CPU
  - 4 GB of RAM strongly recommended
  - Hard Disk: Additional 80 GB minimum. Recommended installation on a separate drive. Your storage needs are based on your mail volume, quarantine size, archived data, and auditing settings.

For Virtual Appliances

When installed as a Virtual Appliance, Dell SonicWALL Email Security 7.4.5 is supported on systems that meet the following requirements:

- VMware Platforms:
  - ESXi 4.0 Update 1 (Build 208167 and newer)
  - ESX 4.0 Update 1 (Build 208167 and newer)
  - ESX 5.1
- Hardware Resource Requirements:
  - 160 GB thick provisioned hard disk space

    Note: The OVA image for the Dell SonicWALL Email Security Appliance specifically allocates 160 GB on the virtual disk and cannot be altered.
  - 4 GB RAM
  - 1 CPU

Enhancements in Email Security 7.4.5

The following is a list of new enhancements made to features in the Dell SonicWALL Email Security 7.4.5 release:

- **Address Book Import**
  The **Anti-Spam, Anti-Phishing** > **Address Books** page now allows users to import an address book with multiple addresses. The imported file must follow specific formatting requirements in order to successfully import into the Email Security solution.
- **Domain Keys Identified Mail (DKIM)**
  Dell SonicWALL Email Security now supports DKIM verification of inbound email messages. DKIM uses a secure digital signature to verify that the sender of a message is who it claims to be and that the contents of the message have not been altered in transit. A valid DKIM signature is a strong indicator of a message's authenticity, while an invalid DKIM signature is a strong indicator that the sender is attempting to fake his identity.
- **HTML Support for Outbound Reports**
  Email Security allows you to optionally download data reports in CSV or HTML format. Custom reports can also be created by specifying a time period for the data.
- **User Lockout Feature**
  Administrators have the option to enable a user lockout feature, which locks out user accounts if the number of unsuccessful attempts to login is reached.
- **Maria DB Support**
  Maria DB 5.5.32 now supports all Email Security platforms (including Windows 32 and 64-bit), replacing MySQL services.

Resolved Issues

The following are resolved issues in the Dell SonicWALL Email Security 7.4.5 release.

	Symptom	Condition
138429	TLS is not enforced when the "Require the destination server to support StartTLS" checkbox is enabled.	Occurs when the "Require the destination server to support StartTLS" feature is enabled and the path is configured to route emails using MX routing or MX routing with exceptions. TLS is not enforced and is allowing email messages. With this feature enabled, TLS should be rejecting or bouncing email messages.
135553	Email Security resets the outbound connection with 20+ recipients.	Occurs due to an obscure combination of conditions, including a large number of recipients in a message. The Email Security Gateway fails to deliver a message, and the sender receives an SMTP error response ("421 4.4.1 Service unavailable, error interacting with downstream server") and a log record warning ("Downstream response does not appear to be SMTP").
132821	Special characters in the Username (for example, the German Umlaut) are not recognized and prevent user from logging in.	Occurs when using special characters from languages other than English in the Username. For example, logging in with the name "Stöckmann" results in an incorrect username, but "Stoeckmann" results in a successful login.
132675	The OU Admin is unable to view or unlock a corresponding OU User that has been locked out of Email Security after unsuccessful login attempts.	Occurs when a user enters the wrong login credentials five times and, as a result, is locked out of Email Security. The corresponding OU Admin is unable to view the locked out user, nor is the Admin able to unlock the user.
132670	Help Desk Users are unable to view the Auditing Page to manage Auditing Data.	Occurs when a user assigned with a Help Desk Role attempts to view Auditing Data. In order for the Help Desk Role to be able to view Auditing data, the Global Administrator must enable the "Allow audit view to Help Desk Users" checkbox.
131153	Users are unable to log in if the name attribute is set to CN and the login name includes a space (i.e. "John Doe").	Occurs when upgrading to Email Security 7.4.3. If the login name attribute is set to CN and users attempt to log in with a name that includes a space, the user receives an "Invalid Username or Password" error; however, the WebUI log does not display the error. **Workaround:** Change the user login name attribute to UID and login with a username that does not contain a space.
130582	The SMTP log does not record the source IP of a spam message if it is an IPv6 address, and results in a "Permanent Error" message.	Occurs when there are IPv6 terms in the SPF record. Instead of recording the occurrence in the SMTP log, the SPF judgment renders a "Permanent Error" message.
130356	A user is not inheriting Group Junk Summary Delivery settings.	Occurs when disabling global settings and enabling Junk Summary Delivery only for a group. The specified members of the group are unable to receive the Junk Box Summary.

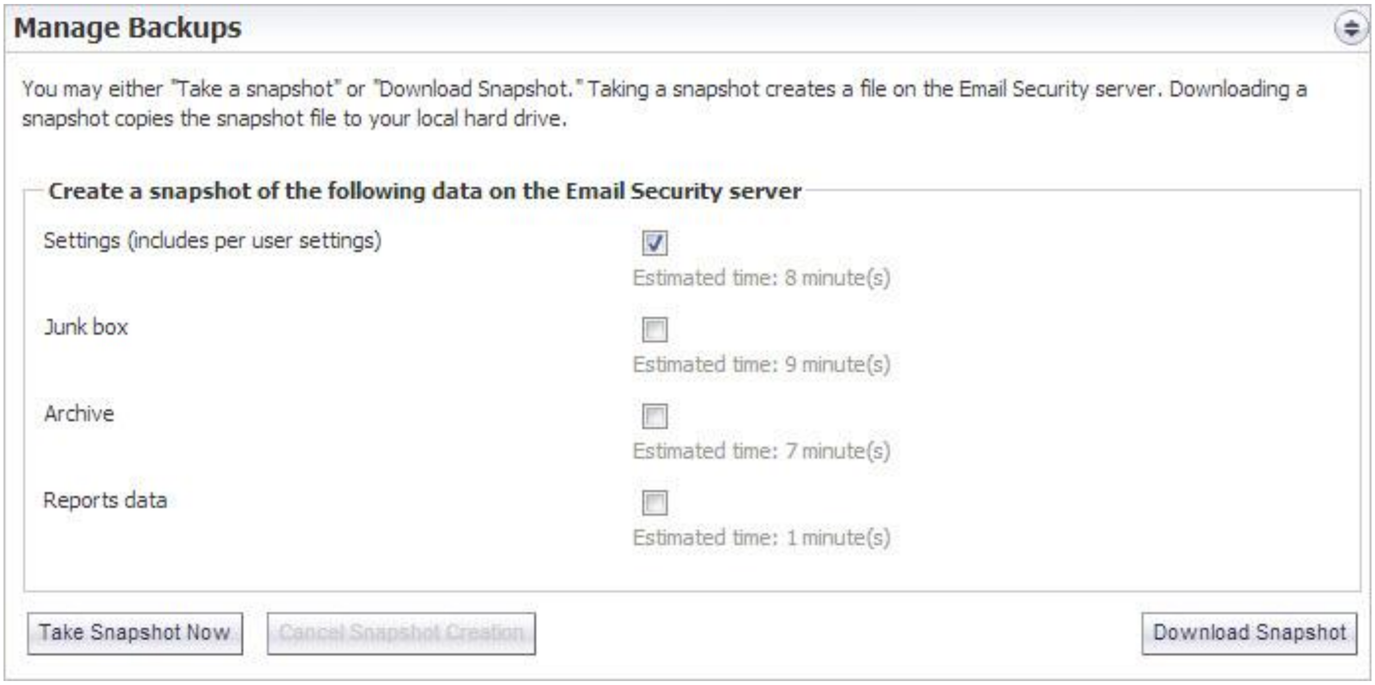
Upgrading to Email Security 7.4.5

The following procedures are for upgrading an existing Email Security appliance or software installation, or for installing the Email Security Virtual Appliance.

Backing Up Your Existing Environment on an Email Security Appliance

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. Login to Email Security interface using the **admin** account
2. In the left navigation pane under **System**, choose **Backup/Restore**. You will see the Backup/Restore page:



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.

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

Settings (includes per user settings) ☑ Estimated time: 8 minute(s)

Junk box □ Estimated time: 9 minute(s)

Archive □ Estimated time: 7 minute(s)

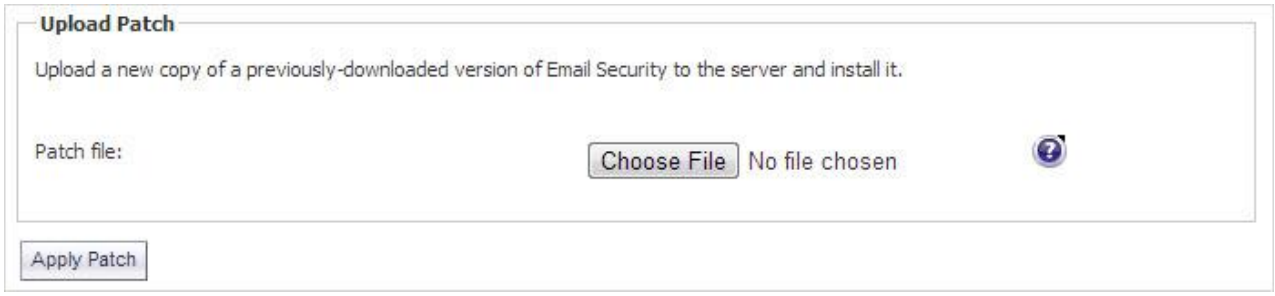
Reports data □ Estimated time: 1 minute(s)

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 Dell SonicWALL Email Security Firmware

Follow this procedure to upgrade your existing Email Security firmware on Email Security appliances.

1. Navigate to the **System** > **Advanced** page and scroll down to the **Upload Patch** section.



Upload Patch

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

Patch file: Choose File No file chosen

2. Click **Choose File** to locate the Email Security Firmware file on your local file system, and then click **Apply Patch**.
3. As part of the upgrade process, the Email Security appliance will reboot. The upgrade process could take between 10-20 minutes. All the settings and data will be preserved.

⚠ **NOTE for ES8300**

Your ES8300 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 Dell SonicWALL Email Security Software

Follow this procedure to upgrade your existing Email Security installation. The Full Installer includes installation of Apache Tomcat, the Java Runtime Environment (JRE), Firebird, and MySQL as well as the base Email Security software.

1. 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.

2. In the Welcome page of the installation wizard, click **Next**.
3. Read the License Agreement and then click **Next** to accept the agreement.
4. 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.

5. 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.

6. 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.
7. On the Start Installation page, click **Next**.
8. 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 appliance.
9. After the installation finishes, click **Finish** in the Installation Complete wizard. A browser window is displayed with links to the Email Security user interface and documentation.

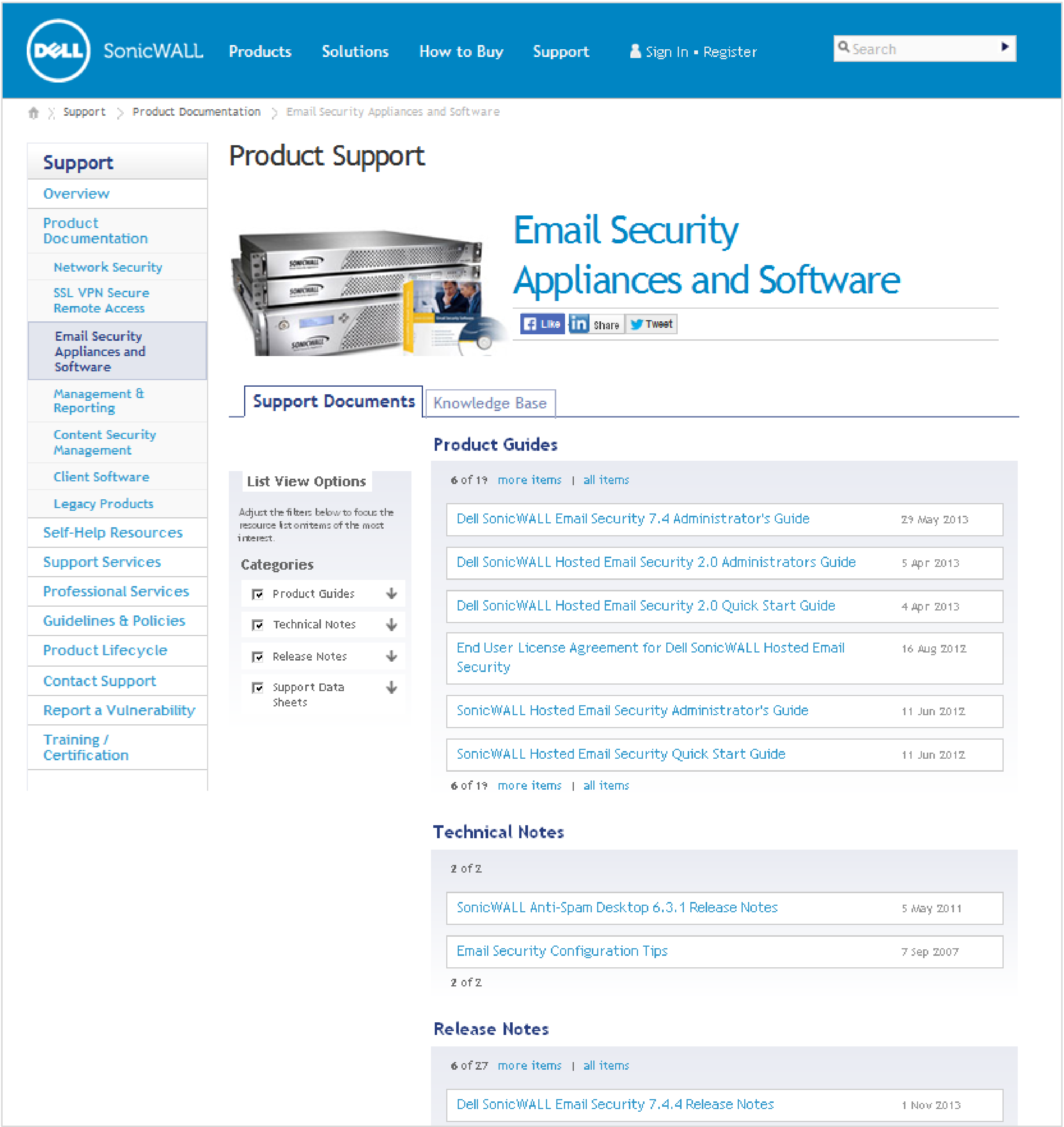
Installing the Dell SonicWALL Email Security Virtual Appliance

For information about installing Dell SonicWALL Email Security 7.4.5 as a Virtual Appliance, see the *Email Security Virtual Appliance Getting Started Guide*, available at:

http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=45

Related Technical Documentation

For basic and advanced deployment examples, Dell SonicWALL documentation is available in the Dell SonicWALL Technical Documentation Online Library: http://www.sonicwall.com/us/Support.html



SonicWALL Products Solutions How to Buy Support Sign In • Register Search

Support > Product Documentation > Email Security Appliances and Software

Support
- Overview
- Product Documentation
  - Network Security
  - SSL VPN Secure Remote Access
  - Email Security Appliances and Software
  - Management & Reporting
  - Content Security Management
  - Client Software
  - Legacy Products
- Self-Help Resources
- Support Services
- Professional Services
- Guidelines & Policies
- Product Lifecycle
- Contact Support
- Report a Vulnerability
- Training / Certification

Product Support

Email Security Appliances and Software

Like Share Tweet

Support Documents | Knowledge Base

List View Options

Adjust the filters below to focus the resource list oritems of the most interest.

Categories

☑ Product Guides

☑ Technical Notes

☑ Release Notes

☑ Support Data Sheets

Product Guides

6 of 19 more items | all items

Dell SonicWALL Email Security 7.4 Administrator's Guide	29 May 2013
Dell SonicWALL Hosted Email Security 2.0 Administrators Guide	5 Apr 2013
Dell SonicWALL Hosted Email Security 2.0 Quick Start Guide	4 Apr 2013
End User License Agreement for Dell SonicWALL Hosted Email Security	16 Aug 2012
SonicWALL Hosted Email Security Administrator's Guide	11 Jun 2012
SonicWALL Hosted Email Security Quick Start Guide	11 Jun 2012

6 of 19 more items | all items

Technical Notes

2 of 2

SonicWALL Anti-Spam Desktop 6.3.1 Release Notes	5 May 2011
Email Security Configuration Tips	7 Sep 2007

2 of 2

Release Notes

6 of 27 more items | all items

Dell SonicWALL Email Security 7.4.4 Release Notes	1 Nov 2013

Last updated: 12/6/2013