

Release Notes

Contents

<i>System Compatibility</i>	1
<i>Enhancements in Email Security 8.0</i>	3
<i>Known Issues</i>	13
<i>Resolved Issues</i>	13
<i>Upgrading to Email Security 8.0</i>	14
<i>Related Technical Documentation</i>	17

System Compatibility

For Appliances

Dell SonicWALL Email Security 8.0 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 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 8.0 is supported on systems that meet the following requirements:

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



Note: Dell SonicWALL Email Security 8.0 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
 - Hard Disk: Additional 160 GB minimum. Recommended installation on a separate drive. Your storage needs are based on your mail volume, quarantine size, archived data, and auditing settings.

Release Notes

For Virtual Appliances

When installed as a Virtual Appliance, Dell SonicWALL Email Security 8.0 is supported on systems that meet the following requirements:

- VMware Platforms:
 - ESX 5.1 and newer
- 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

Release Notes

Enhancements in Email Security 8.0

The following is a list of new enhancements made to features in the Dell SonicWALL Email Security 8.0 release:

- **Encryption Service**

The Encryption Service feature works in tandem with Dell SonicWALL Email Security as a Software-as-a-Service (SaaS), which provides secure mail delivery solutions. The mail messages that have [SECURE] as part of the Subject will be encrypted and securely delivered to the recipient via the Encryption SaaS.

The Encryption Service works with both outbound and inbound email messages. The Encryption Service must first be licensed through the **System > License Management** page. The administrator then will enable the default policy filter that enables sending secure mail via the Encryption Service. After adding the necessary sender domains and public IP addresses, the administrator can then add users that are licensed to use Encryption Service.

The screenshot shows the 'License Management' page in the SonicWALL interface. The page title is 'License Management' and it includes a breadcrumb 'System / License Management'. Below the title, there is a link to 'Check system status under Reports & Monitoring'. The main content area is titled 'Manage Licenses' and contains a section for 'Email Encryption Service Subscription'. This section includes several input fields: 'Email Encryption Service Activation Keys, separated by comma:' (a large text area highlighted with a yellow border), 'Data Center nearest to you:' (a dropdown menu), 'Company Name:' (a text field), 'Admin Email Address:' (a text field with a 'What is this?' link), and 'Auto Sender Domains, separated by comma:' (a large text area with a 'What is this?' link). A 'Submit' button is located below these fields. At the bottom left, there is a 'Return to License Summary' button, and at the bottom right, there is a 'Test Connectivity' button. In the top right corner of the 'Manage Licenses' section, there are labels for 'Serial number:', 'Authentication Code:', and 'Model Number:'.

Release Notes

The Encryption Service also supports Whitelist IP Addresses.

Whitelist IP Address

Enter list of public IP address which is responsible to deliver mail outside your organization:

Separate entries with a <CR> Example:
10.1.1.1
10.1.1.2

Enter list of public IP address and its associated domain which is responsible to receive mails directly from Encryption Service: (If not specified, MXRecord will be used to deliver mails to the organization):

Separate entries with a <CR> Example:
engr.example.com 10.1.1.1
corp.example.com 10.1.1.2

- **Send Secure Mail Button**

The **Downloads** page on your Email Security solution provides a link for the “Send Secure” button for Microsoft Outlook. This button allows you to send Secure Mail messages using the Encryption Service. To install, simply click the link compatible with your version of Outlook.

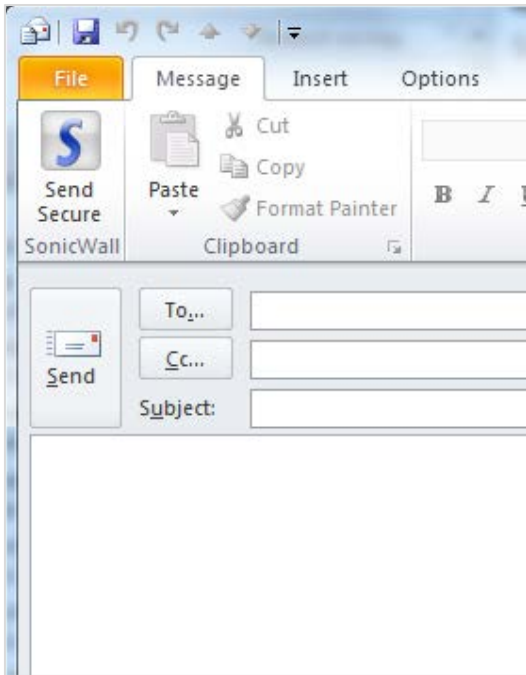
Downloads

To enhance your spam-blocking experience with a component on your desktop, select one of the following to download and install:

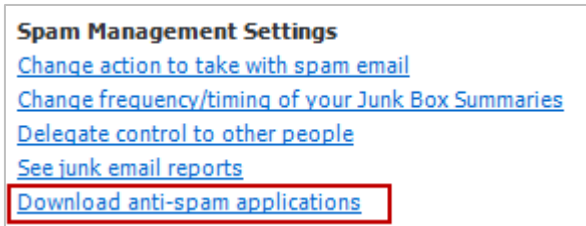
- Provides “Junk” and “Unjunk” buttons so you can quickly teach Email Security what you want and don’t want
[Anti-Spam Desktop for Outlook \(32-bit\) and Outlook Express \(trial version\) on Windows \(32-bit\)](#)
[Anti-Spam Desktop for Outlook \(32-bit\) and Outlook Express \(trial version\) on Windows \(64-bit\)](#)
[Anti-Spam Desktop for Outlook \(64-bit\) and Outlook Express \(trial version\) on Windows \(64-bit\)](#)
- Provides a “Junk” button so you can quickly teach Email Security what you don’t want
[Junk Button for Outlook \(32-bit\)](#)
[Junk Button for Outlook \(64-bit\)](#)
- Provides a “Send Secure” button so you can send mails via Encryption Service
[Send Secure button for Outlook \(32-bit\)](#)
[Send Secure button for Outlook \(64-bit\)](#)

Release Notes

The “Send Secure” button displays on your Outlook program where the “Send” button previously was located.



You can also access the **Downloads** page by clicking the **Download Anti-Spam Applications** link from your Junk Box Summary messages:



- **Allowed IP Address Support**

Enter a list of public IP addresses that are responsible for delivering outgoing mail recognized as secure. Then, enter the IP address and any associated domain that is responsible for receiving incoming mail messages from the Encryption Service. Note that if no inbound addresses are specified, the MX Records are used instead to deliver mail messages to your organization.

Release Notes

Allowed IP Address

Enter list of public IP address which is responsible to deliver mail outside your organization:

Separate entries with a <CR> Example:
10.1.1.1
10.1.1.2

Enter list of public IP addresses and the associated domains of your organization which are responsible to receive mails directly from Encryption Service: (If not specified, MXRecord will be used to deliver mails to the organization):

Separate entries with a <CR> Example:
enr.example.com 10.1.1.1
corp.example.com 10.1.1.2

- **DMARC Policy Enforcement**

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a policy that works in tandem with the SPF and DKIM features to fully authenticate incoming and outgoing email messages. Navigate to the **Anti-Spoofing > Inbound** tab to configure settings for DMARC Policy Enforcement for incoming messages. By default, the DMARC feature is enabled. You can specify the exact domain names to exclude from DMARC Policy Enforcement. The DMARC feature also allows you to specify domains for Incoming and Outgoing message reports. If you choose to configure Incoming/Outgoing reports, you can view the results on the **Reports & Monitoring > DMARC Reporting** page.

DMARC Settings

Enable DMARC Policy Enforcement for incoming messages

Exclude these domains (Do not enforce DMARC Policy for these domains)

(Separate multiple domains with a comma)

DMARC Incoming report settings :

Process DMARC incoming reports for these domains

Domains	RUA Email Address	Settings
No Data Available		

DMARC Outgoing report settings :

Domains	Sender Email Id	Additional Information (if any)	Settings
No Data Available			

- **DMARC Reporting**

The **Reports & Monitoring > DMARC Reporting** page allows you to generate various DMARC reports. Navigate to the **Reports & Monitoring > DMARC Reporting > Configure Known Networks** page to add server groups and IP addresses to be generated in the selected reports. Known Networks are considered IP addresses owned by Email Security servers, and IP addresses not owned are considered Unknown Networks.

Release Notes

Reports & Monitoring / DMARC Reporting /

DMARC Reports

Generate Dmarc Report

Dmarc Reports can be displayed by date range and/or filters

Select Date Range
(1) Last Day is the number of days before latest date imported data. (2) start/end date are limited by real data

Last 1 day Start Date End Date

Set Filters
(1) Filter button: creates new filter or changes saved filter. (2) opening filter window at one time to create multiple conditions. (3) click on arrow icon to open the filter or delete it.

Filter

Apply Filter

Select Report

- DMARC Statistic Report
- DMARC Master Detail Report
- Source IP Aggregation Report
- Provider Aggregation Report
- Source IP And Provider Aggregation Report

- **DKIM for Outbound Email**

Dell SonicWALL now supports DKIM for outbound email messages. Domain Keys Identified Mail (DKIM) uses a secure digital signature to verify the domain name of the email message, which is then validated by the recipient of the message. Outbound email messages now include DKIM signatures added to the headers of the messages.

To configure the settings for DKIM Outbound Signatures, navigate to the **Anti-Spoofing > Outbound** tab, and click **Add Configuration** button in the **DKIM Signature Configurations** section.

Release Notes

The screenshot shows the 'DKIM outbound configuration' settings in the SonicWALL interface. At the top left is the Dell SonicWALL logo and the title 'DKIM outbound configuration'. At the top right is a 'Close' button. The main heading is 'Settings for DKIM Signature :'. Below this, there is a checkbox for 'Enable signature on outbound email' which is checked. A yellow note box contains the text: 'Note: DKIM TXT record should be added to the domain's DNS before enabling DKIM configuration.' The configuration fields include: 'Domain' (text input), 'Identity of Signer' (text input with a checked 'Same as domain' checkbox), 'Selector' (text input), and 'List of Header fields for Signing' (checkbox for 'Sign all standard headers' which is checked, followed by a text area for header fields with a help icon and the text 'Separate multiple headers with a colon Example - from:to:subject'). Below these is the section 'Generate public-private key pair for DKIM Signing:', which includes a 'Key size' dropdown set to '1024', a 'Generate key pair' button, and two large text areas for 'Public key' and 'Private key', each with a help icon. At the bottom left are 'Save' and 'Cancel' buttons.

- **Smart Host Routing Using Multiple IPs**

The Smart Host Routing feature now includes options to use round-robin or failover mode to route mail to multiple destination servers. This feature is currently supported on the inbound path dialog only. You can configure the Smart Host Routing settings by navigating to the **System > Network Architecture > Server Configuration** page and clicking **Add Path**.

Release Notes

This is an MTA. Route email using SmartHost to destination server:
[What is this?](#)

With the following **EXCEPTIONS**:
These domains should use MX record routing.

These domains should route email using SmartHost in Round-Robin mode to the following multiple IP addresses or hostnames:

Destination host name or IP Port

Separate domains with a <CR>. Example:
example.com
example.net

Separate the domain and IP address with a space. Separate IP address with a comma. Separate entries with a <CR>. Examples:
enr.example.com 10.1.1.2,10.1.1.3,10.1.1.4
sales.example.com 10.1.1.1

- **Export Address Book**

The Export Address Book option for Global Administrators and OU Administrators is now available. Navigate to the **Anti-Spam > Address Books** page. Click the **Export** button. The available address book is exported to your local system as a .txt file.

Anti-Spam /

Address Books

Allowed Blocked

Administration - Corporate

Use this page to allow or block people, companies, or mailing lists from sending you email. The final list shown is a compilation of allowed and blocked senders from your organization's lists and lists provided by default.

Search

People Companies Lists IPs

<input type="checkbox"/>	Address	Type	Address Source
<input type="checkbox"/>	sonicwall.com	Companies	

Release Notes

- **'Likely Spoof Judgment' Inbound Policy**

A 'Likely Spoof Judgment' Inbound policy is now supported on the **Policy & Compliance > Filters** page. Select the **Inbound** tab and the Add New Filter dialog box displays. For **Select**, choose the **Likely Spoof Judgment** option from the drop down list. You can then select the specific **Matching** field for likely spoof judgment.

The screenshot shows the 'Add New Filter' dialog box in SonicWALL. The dialog is titled 'Add New Filter' and has a 'Dell SonicWALL' logo. It contains several sections: 'Enable this filter:' with a checked checkbox; 'If All of these conditions are met:' with a dropdown menu set to 'All'; 'Select:' with a dropdown menu set to 'Likely Spoof Judgment'; 'Matching:' with a dropdown menu showing a list of options including 'SPF Pass', 'SPF Soft Fail', 'SPF Hard Fail', 'DKIM Pass', 'DKIM Fail', 'DMARC Aligned', and 'DMARC Unaligned', with 'SPF Pass' selected; 'Search value:' with an empty text field; 'Use dictionary:' with a dropdown menu set to 'Financial Terms (SonicWALL) - 1.0'; 'Use record ID:' with a dropdown menu set to 'Social Security Number'; 'Match case' checkbox; 'Intelligent attachment matching' checkbox; 'Disguised text identification' checkbox; 'Perform the following actions:' section with 'Action:' dropdown set to 'Store in Junk Box' and a checked checkbox for 'Stop processing policy filters'.

- **Drag-and-Drop Policy Filter**

The **Policy & Compliance > Filters** page allows you to select any filter from the list and 'drag and drop' it into a different position on the list.

- **IPv6 Support**

Dell SonicWALL Email Security now supports IPv6 configuration.

- **System Diagnostics Enhancements**

Dell SonicWALL Email Security supports the following categories for diagnostics on the **System > Diagnostics** page:

- Run SMTP Test for specific Host or IP
- Query DNS for A Record of the specified Host
- Query DNS for MX Record of the specified Host
- Query DNS for SPF Policy for the specified Host
- Query DNS for DMARC Policy of the specified Host
- Query DNS for DKIM Policy of the specified Host
- Ping the specified Host or IP
- Connect to the specified Host

Release Notes

The screenshot shows the 'System Diagnostics' interface. At the top, it says 'System / Diagnostics'. Below that is a 'System Diagnostics' section with a form titled 'Select Category, Input SMTP Hostname/IP'. The form has four input fields: 'Diagnostics Category' (a dropdown menu), 'SMTP Hostname/IP', 'Port', and 'Alternate DNS Server IP (optional)'. The dropdown menu is open, showing several options: 'Run SMTP Test for specified Host or IP', 'Run SMTP Test for specified Host or IP', 'Query DNS for A record of the specified Host', 'Query DNS for MX Record of the specified Host', 'Query DNS for SPF Policy of the specified Host', 'Query DNS for DMARC Policy of the specified Host', 'Query DNS for DKIM Policy of the specified Host', 'Ping the specified Host or IP', and 'Connect to the specified Host'. The 'Ping the specified Host or IP' option is highlighted in blue. To the right of the 'SMTP Hostname/IP' field, there is a note: '(Default port is 25 unless specify)'. A 'Go' button is located to the right of the 'Alternate DNS Server IP' field.

- **Per Domain TLS Support**

Administrators are now able to configure per-domain and per-path Transport Layer Security (TLS). This allows the administrator to specify domains for which upstream or downstream TLS is mandatory.

- **SPF UI Enhancements**

Sender Policy Framework (SPF) is an email validation system designed to prevent email spam by detecting email spoofing by verifying sender IP addresses. SPF records, which are published in the DNS records, contain descriptions of the attributes of valid IP addresses. SPF is then able to validate against these records if a mail message is sent from an authorized source. If a message does not register as an authorized source, the message 'fails.' You can configure the actions against messages that 'fail.'

There are two types of SPF Fails:

SPF SoftFail - If the email message from a domain originates from an IP address outside of the IP range defined in the SPF record for the domain, the message is accepted, but marked.

SPF HardFail - If an email message from a domain originates from an IP address outside of the IP range defined in the SPF record for the domain, the message is rejected.

The **Anti-Spoofing > Inbound** tab allows you to configure setting for SPF Hard Fail and SPF Soft Fail. The SPF enhancements now include configuring the actions for SPF Hard Fail and adding domain(s) for this specific fail. For SPF Soft Fails, you can configure Ignore Allow Lists.

Release Notes

Anti-Spoofing

Inbound Outbound

SPF Settings ?

Enable SPF validation for incoming messages

On hard fail

Ignore allow lists

Action for messages marked as **SPF hard fail**:

No action

Permanently delete

Reject with SMTP error code 550

Store in Junk Box (recommended for most configurations)

Send to

Tag with added to the subject

Add X-Header: X- :

Domain specific SPF settings

Sender Domain	Ignore allow lists	SPF Action	Settings
No Data Available			

On soft fail

Ignore allow lists

Release Notes

Known Issues

The following are Known Issues in the Email Security 8.0 release:

	Symptom	Condition
143722	IPv4 must be configured on Ethernet 1 port before IPv6 addresses can be added.	Occurs when adding an IPv6 alias for the Ethernet1 port on the Host Configuration page. The Web UI will display that the alias has been successfully added. However, upon scrolling to the Network Settings section shows that all the fields are greyed out and nothing has been configured. Workaround: Enter an unused IPv4 address.
143432	Diagnostics page does not support IPv6.	Occurs when attempting to use IPv6 addresses on the Diagnostics page.

Open SSL 1.0.1g Issue

Issue	Condition
A small number of vendors may fail to accept default TLS connections from OpenSSL 1.0.1g.	Dell SonicWALL Email Security 8.0 uses the most recent OpenSSL 1.0.1g to initiate TLS connections when delivering email in MTA mode. When such a TLS connection is initiated to connect to a small number of vendor solutions, their solution may fail to accept the default connection. This might result in failure of mail delivery when mandatory TLS is configured and a clear text delivery when an opportunistic TLS is setup. Recipients experiencing this issue should refer to their vendor for the latest update on this issue.

Resolved Issues

The following are Resolved Issues in the Email Security 8.0 release:

	Symptom	Condition
141299	Tomcat does not start after downgrading Email Security to a pre-Email Security 7.4.6 version.	Occurs when downgrading Email Security 8.0 to a release earlier than Email Security 7.4.6. After the downgrade, Tomcat will not start and its log will show duplicate 8.0 ciphers. Email Security 8.0 only supports downgrading to Email Security 7.4.6. Workaround: Manually delete the 8.0 ciphers tag using a text editor.

Release Notes

Upgrading to Email Security 8.0

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.....	14
Upgrading Your Existing Dell SonicWALL Email Security Firmware	15
Upgrading Your Existing Dell SonicWALL Email Security Software	15
Installing the Dell SonicWALL Email Security Virtual Appliance	16

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.

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. 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

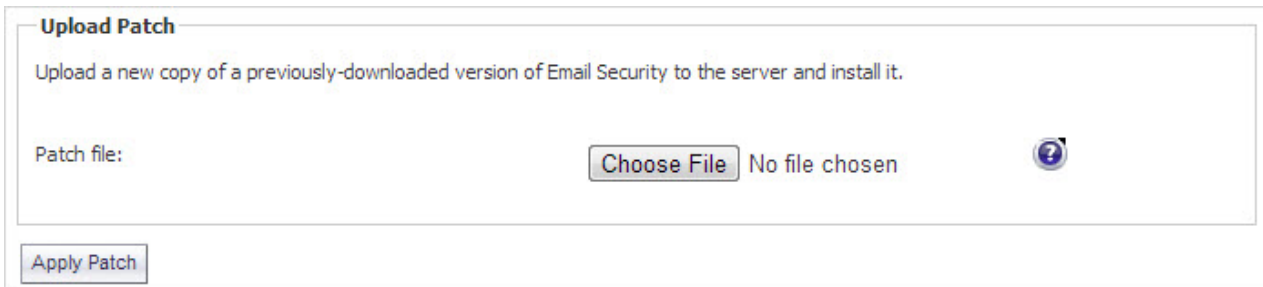
Release Notes

Upgrading Your Existing Dell SonicWALL Email Security Firmware

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

 **Note:** Upgrading your existing installation to Dell SonicWALL Email Security Software 8.0 is supported only if you are running previous versions on a 64-bit Windows operating systems, which are listed under the 'System Compatibility' section of this document. Dell SonicWALL Email Security 8.0 is not supported for 32-bit operating systems.

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



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.

Release Notes

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 8.0 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

Release Notes

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>

The screenshot shows the Dell SonicWALL Support website interface. At the top, there is a navigation bar with the Dell logo, 'SonicWALL' brand name, and menu items: 'Products', 'Solutions', 'How to Buy', 'Support', 'Sign In', and 'Register'. A search bar is located on the right. Below the navigation bar, a 'Where am I?' breadcrumb trail is visible. The main content area is titled 'Product Support' and features a large banner for 'Email Security Appliances and Software' with an image of SonicWALL hardware. A sidebar on the left contains a 'Support' menu with various categories, including 'Email Security Appliances and Software' which is currently selected. Below the banner, there are tabs for 'Support Documents' and 'Knowledge Base'. The 'Support Documents' section is active and displays a list of 'Product Guides' with filters for 'List View Options' and 'Categories'. The 'Product Guides' list includes titles like 'SonicWALL Hosted Email Security Quick Start Guide' and 'SonicWALL Email Security 7.3 Appliance Administrator's Guide'. Below this, there is a 'Technical Notes' section with one item: 'SonicWALL Anti-Spam Desktop 6.3.1 Release Notes'.

Last updated: 4/22/2014