SonicWall® Email Security 9.2 Virtual Appliance

Getting Started Guide

SONICWALL®

Contents

1

Introduction

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying the SonicWall® Email Security 9.2 Virtual Appliance on a server on your network.

SonicWall Email Security provides effective, high-performance and easy-to-use inbound and outbound email threat protection. Ideal for the small to medium size business, this self-running, self-updating software delivers powerful protection against spam, virus and phishing attacks in addition to preventing leaks of confidential information. Combining anti-spam, anti-phishing, content filtering, policy management and content compliance capabilities in a single seamlessly integrated solution, SonicWall Email Security provides powerful protection without complexity.

The SonicWall Email Security Virtual Appliance allows for the secure and easy deployment of SonicWall Email Security solution within a virtual environment.

NOTE: SonicWall TotalSecure Email provides complete protection from spam, virus attacks and phishing. Without TotalSecure Email, to use the spam and phishing protection provided by SonicWall Email Security, you must have a subscription to SonicWall Email Protection and Dynamic Support. If you need to purchase a subscription, contact your SonicWall vendor.

The SonicWall Email Security Virtual Appliance provides the following benefits:

- **Scalability and Redundancy:**
  - Multiple virtual machines can be deployed as a single system, enabling specialization, scalability, and redundancy.
- **Operational Ease:**
  - Users can virtualize their entire environment and deploy multiple machines within a single server or across multiple servers.
- **Product Versatility:**
  - SonicWall Email Security Virtual Appliance is compatible with other SonicWall Email Security platforms (Windows Software/Appliance Hardware) as a stand-alone (All-In-One), control center, or remote analyzer.
- **Security:**
  - SonicWall Email Security Virtual Appliance provides an optimized, non-tamperable software and hardware architecture.

    NOTE: For SonicWall Email Security documentation, refer to the *SonicWall Email Security 9.2 Administration Guide*. This and other documentation are available at: http://www.sonicwall.com/us/Support.html

Please read this entire *Getting Started Guide* before setting up your SonicWall Email Security virtual appliance and note that an updated version of this guide may exist. For SonicWall Email Security documentation, refer to the *SonicWall Email Security 9.2 Administration Guide*. This and other documentation are available on SonicWall's Support Website:

https://www.sonicwall.com/en-us/support

Topics:

What You Need to Begin

- A computer to use as a management station for initial configuration of SonicWall Email Security
- An Internet connection
- An Internet browser

  NOTE: SonicWall Email Security requires the latest Chrome, Firefox, or Edge browser.

Supported VMware Platforms

The elements of basic VMware structure must be implemented prior to deploying theSonicWall Email Security Virtual Appliance. SonicWall Email SecurityVirtual Appliance runs on the following VMware platforms:

- ESXi 5.5 and newer

You can use the following client applications to import the image and configure the virtual settings:

- **VMware vSphere** – Provides infrastructure and application services in a graphical user interface for ESXi, included with ESXi. Provides Thick provisioning when deploying SonicWall Email Security Virtual Appliance.
- **VMware vCenter Server** – Centrally manages multiple VMware ESXi environments. Provides Thick provisioning when deploying SonicWall Email Security Virtual Appliance.

System Requirements

The following hardware resources are the minimum requirements for the SonicWall Email Security Virtual Appliance:

- Additional 160 GB minimum

  NOTE: The OVA image for the SonicWall Email Security Virtual Appliance specifically allocates 80 GB on the virtual disk and cannot be altered.

- 8GB of RAM
- Processor: 2 Core Processor (minimum); 4 Core Processor (recommended)

HTTPS Connectivity to License Manager

Email Security products communicate with the SonicWall License Manager servers using the default HTTPS port. The Upstream firewalls in the network where this Email Security system is deployed must allow HTTPS communication on port 443 that is initiated from the 9.2 upgrade process.

> **NOTE:** To test connectivity in SonicWall Email Security 9.2, click the **Test Connectivity to SonicWall** button on the **System > License Management** page in the user interface. If the test fails, check your firewall to be sure that outbound HTTPS communication is allowed.

Files for Installation

You will use different files for a fresh installation than when updating to a newer version. For more information see:

- New Deployment Files on page 5
- Updater File on page 5

New Deployment Files

SonicWall Email Security Virtual Appliance is available for download from http://www.mysonicwall.com. For a fresh install, the Open Virtual Appliance (OVA) file with the following file name format is available for import and deployment to your ESXi server:

- ES_VM64_XX_XXXX.ova

  > **NOTE:** Do not rename the OVA files.

Updater File

For updating the version of an existing Email Security Virtual Appliance, a file with the following file name format is available from MySonicWall:

- es-X.X.X.XXXX-linux-updater-Haswell-der-signed.sh

  > **NOTE:** Do not rename the updater file.

The es-X.X.X.XXXX-linux-updater-Haswell-der-signed.sh file is uploaded to the Upload Patch section of the **MANAGE | Firmware Update** page on the appliance management interface of your existing SonicWall Email Security deployment.

Users already running SonicWall Email Security 200 to 8000 appliances will need to use the Updater File. For more information, see Updating the Email Security Virtual Appliance on page 21.

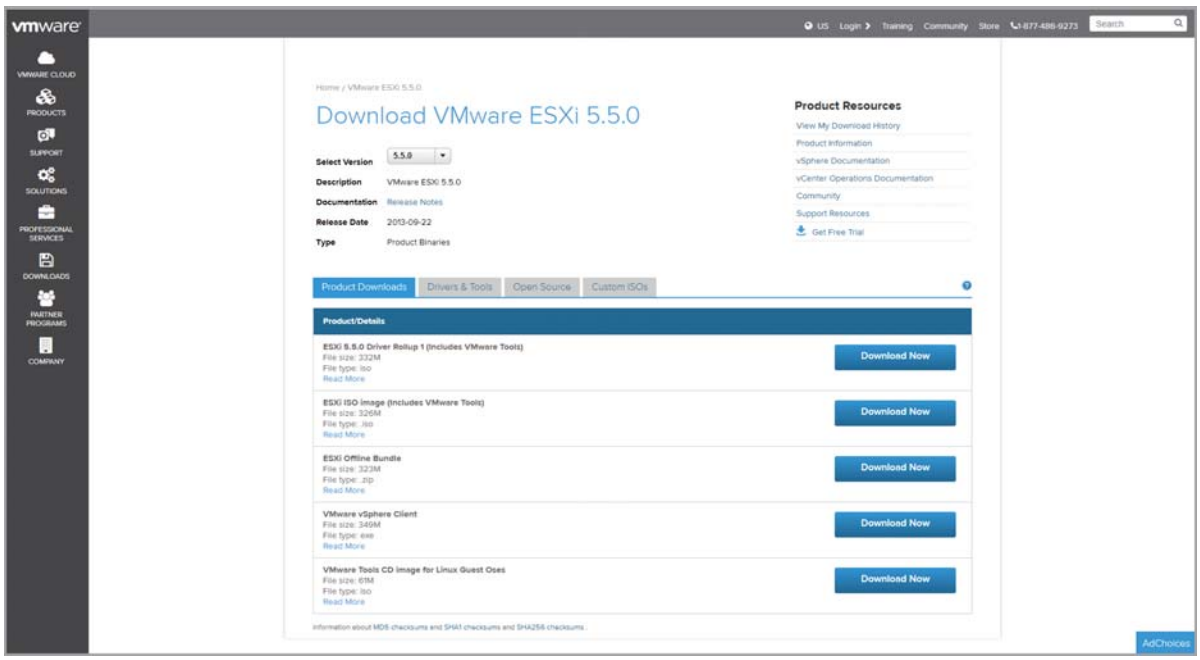
2

Installing the Virtual Appliance

SonicWall Email Security Virtual Appliance is installed by deploying an OVA file to your ESXi server. Each OVA file contains all software components related to SonicWall Email Security.

You can deploy the OVA files as needed for your SonicWall Email Security environment. SonicWall Email Security can be configured for a single server or in a distributed environment on multiple servers.

You can deploy an OVA file by using the vSphere or vCenter client, which comes with ESXi. For vSphere, point a browser to your ESXi server, scroll to VMware vSphere Client, and click on **Download Now**.



Topics:

About Thick Provisioning

Thick provisioning occurs when an OVA file is deployed on your ESXi server. This type of provisioning pre-allocates all the hard disk space for the virtual appliance.

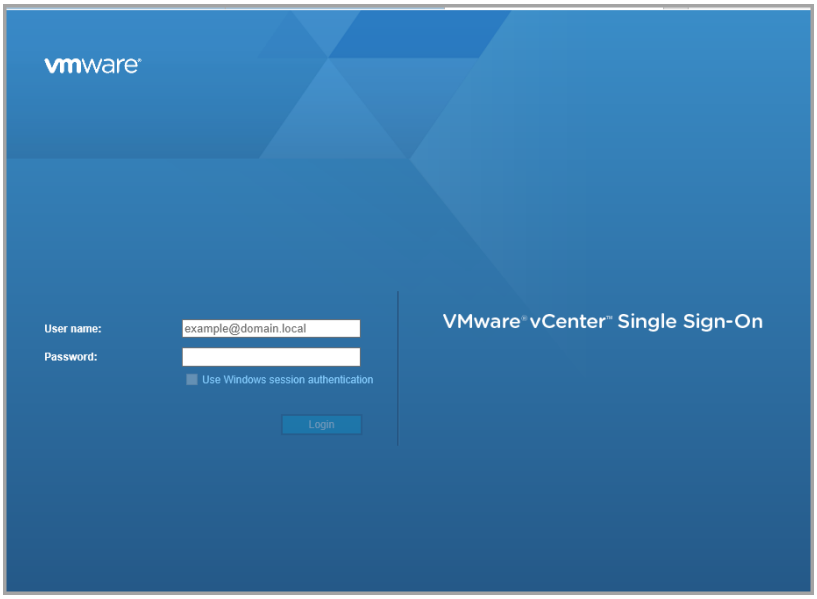
Installing with vSphere

To perform a fresh install of the SonicWall Email Security Virtual Appliance using the vSphere client, perform the following steps:

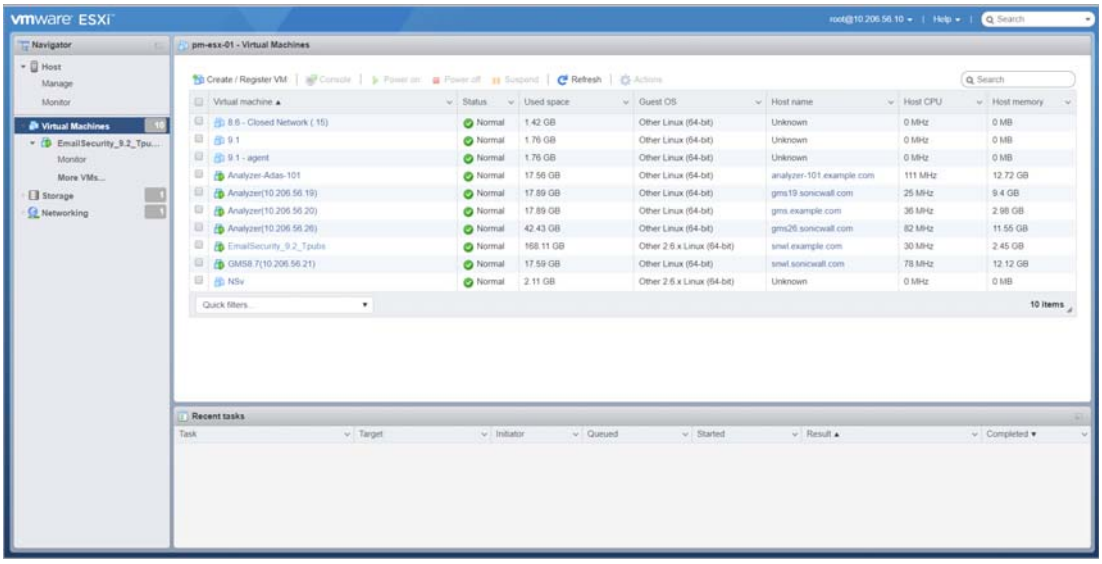
1 Download the es_vm_9.2 .x.xxxx.ova file from MySonicWall to a system that is accessible to your ESXi server.

NOTE: Do not rename the OVA files.

2 Log in to vCenter, or log in using vSphere client.

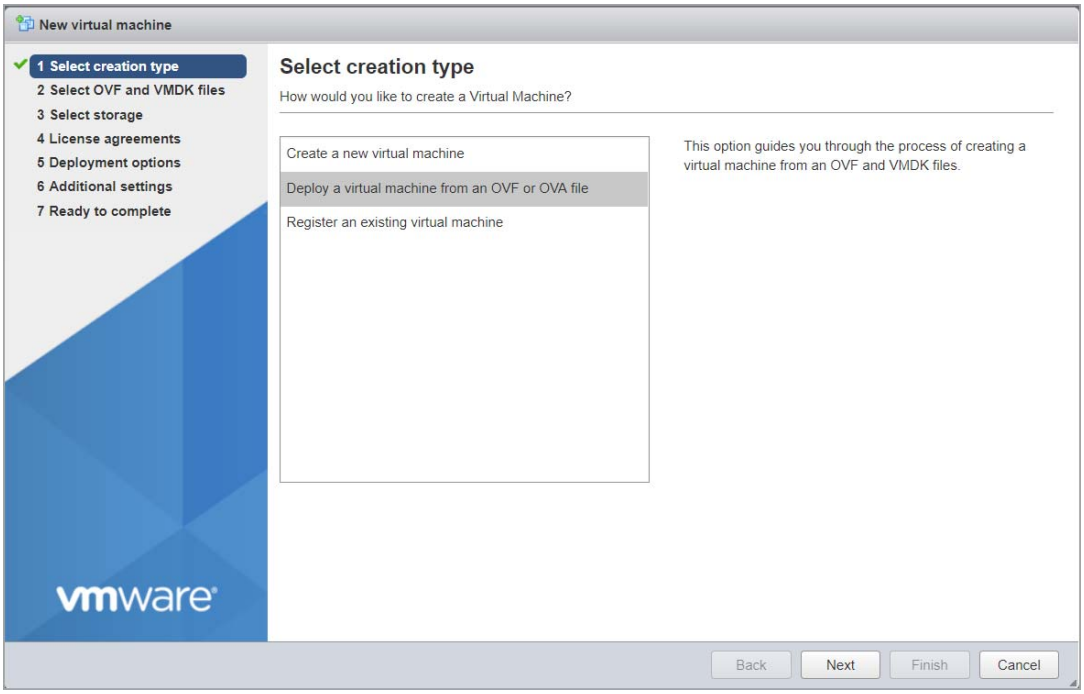


3 From the VMware ESXi **Virtual Machines** page, click **Create/Register VM**.



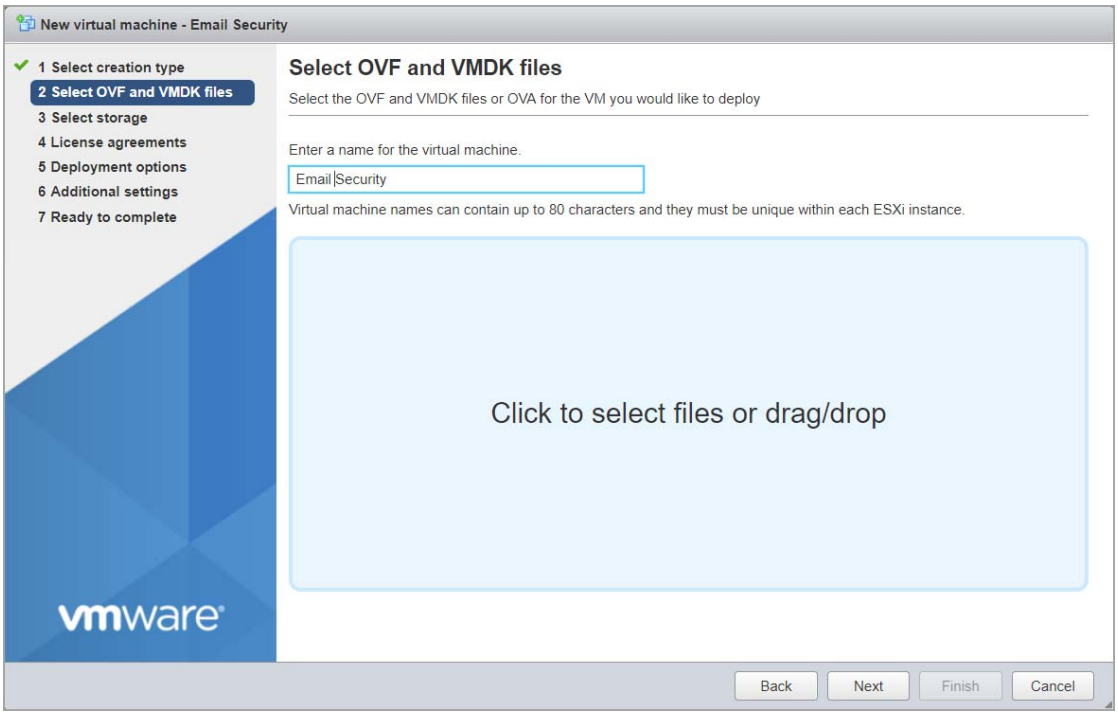
The **Select Creation Type** page displays in the **New Virtual Machine** wizard.

4 To begin the import process, click **Deploy a virtual machine from an OVF or OVA file.**



5 Click **Next.** The **Select OVF and VMDK files** page displays.

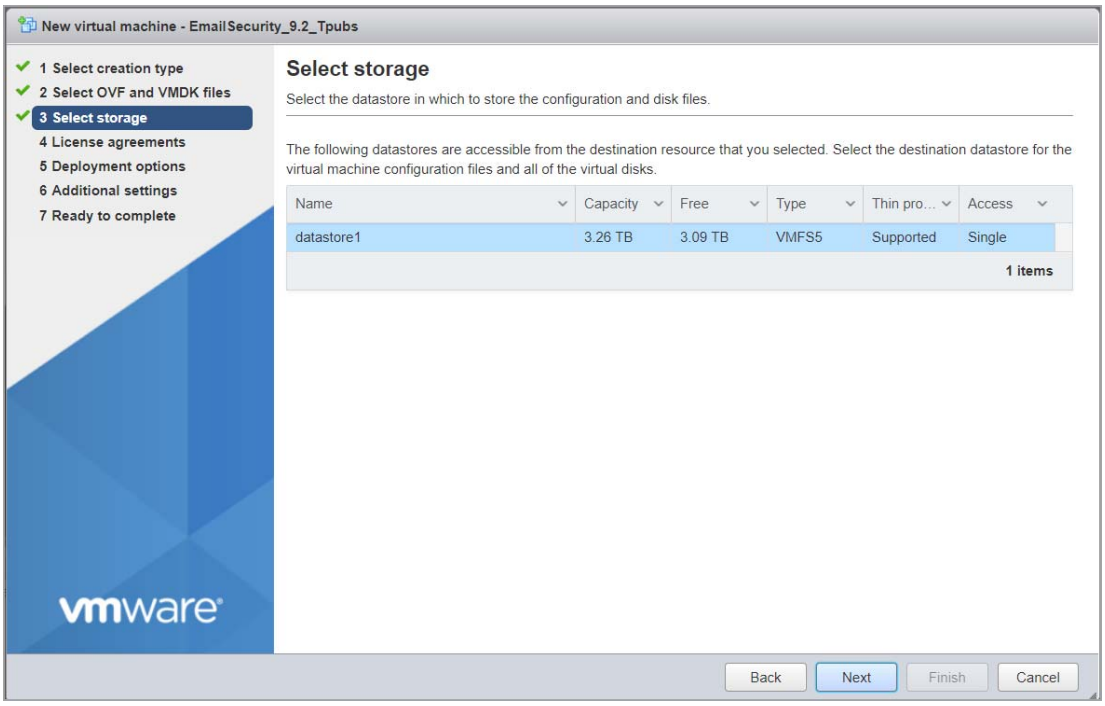
6 Type a descriptive friendly name for the virtual machine in the **Enter a name of the virtual machine** field.



7 Click on **Click to select files or drag/drop to select an OVA file** or drag and drop the OVA file into the drag and drop window.

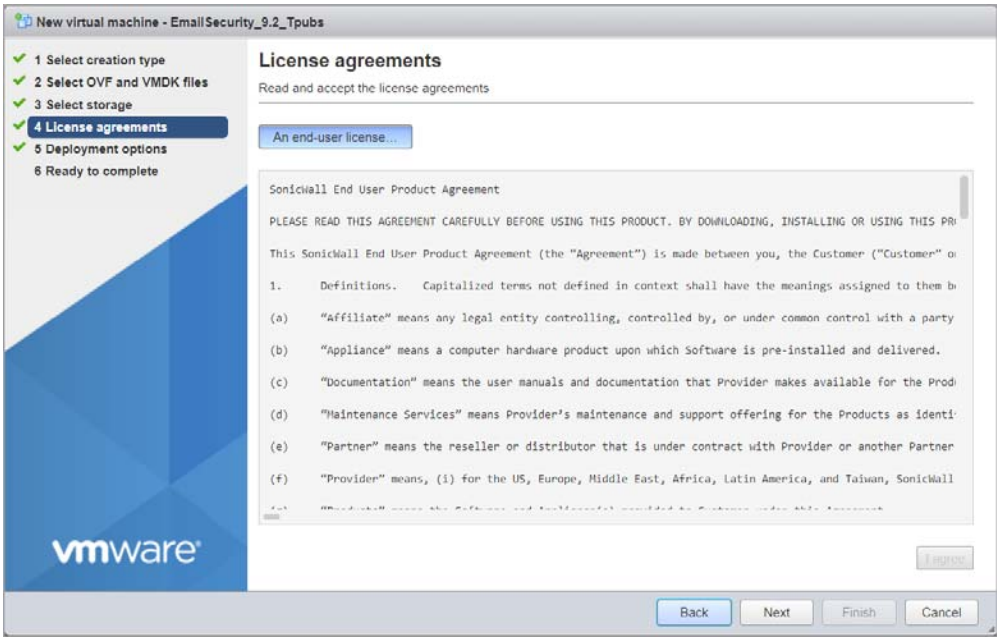
8 Click **Next.** The **Select storage** page displays.

9 Select the datastore in which to store the configuration and disk files.



10 Click **Next.** The **License Agreements** page displays.

11 Read and accept the license agreements then click **I agree**.



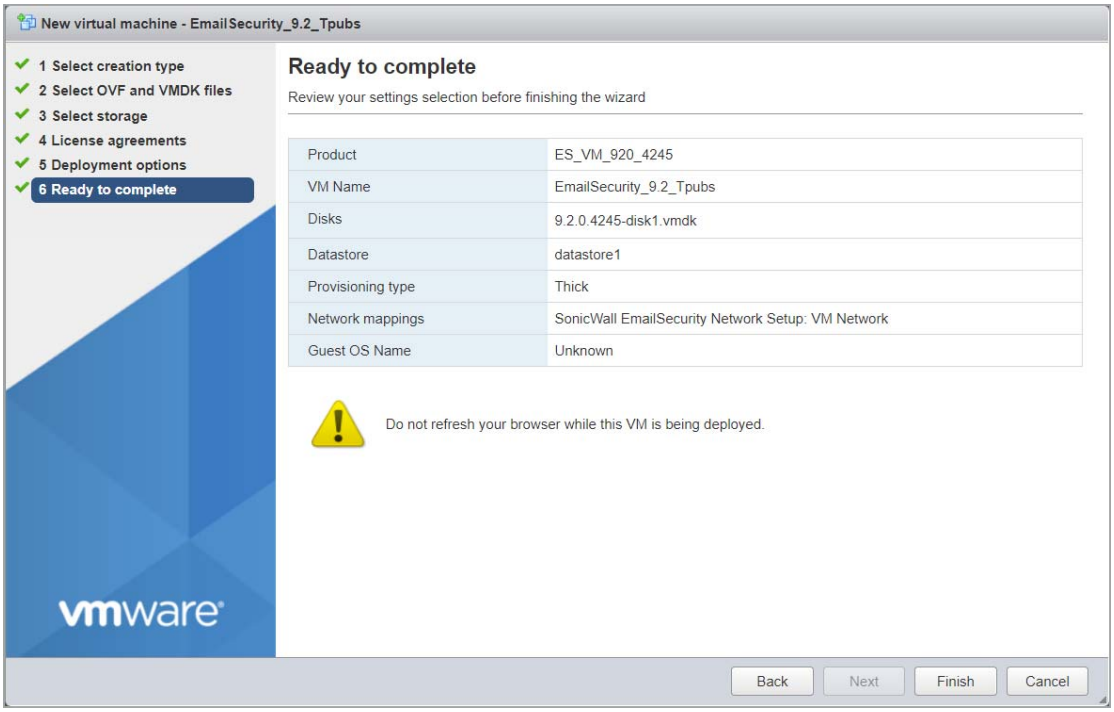
12 Click **Next**. The **Deployment options** page displays.

13 Select / Enter the following in the **Deployment options** page:

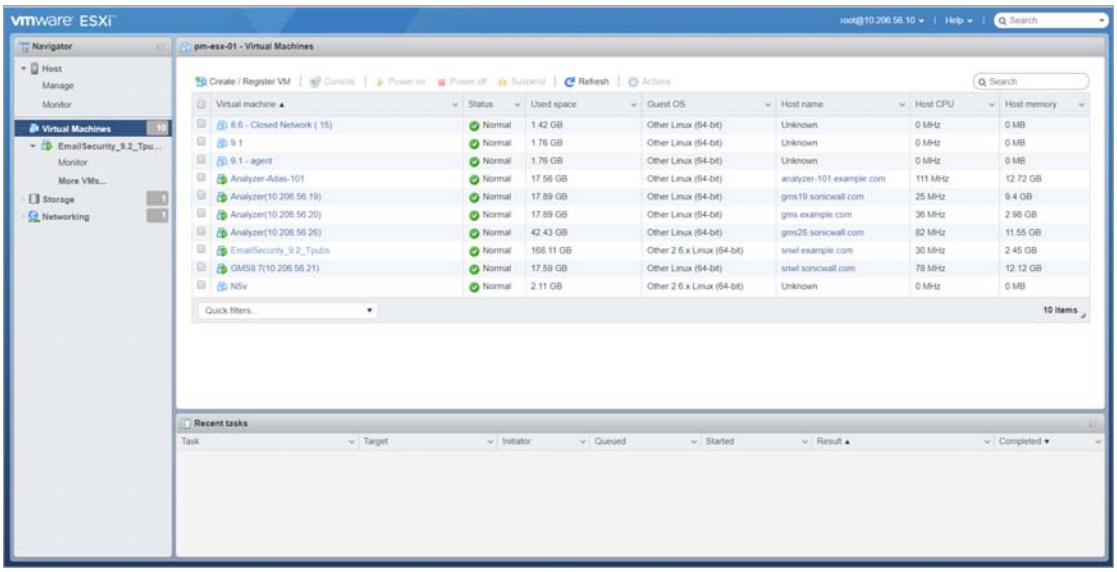
- Network Mappings: Select **VM Network**
- Disk Provisioning: Select **Thick**
- Power on Automatically: Click the check-box to enable **Power on Automatically**

14 Click **Next**. The **Ready to complete** page displays.

15 In the **Ready to Complete** screen, review and verify the displayed information. To begin the deployment with these settings, click **Finish**. Otherwise, click **Back** to navigate back through the screens to make a change.



16 The name of the new SonicWall Email Security Virtual Appliance appears in the **VMware ESXi Virtual Machines** page.



- To power on the virtual appliance and perform required host configuration, see Performing Basic Tasks on page 11.
- To register the SonicWall Email Security appliance, see Activating Email Security License Subscriptions on page 16.

3

Performing Basic Tasks

The following sections describe how to view and edit settings on the virtual appliance:

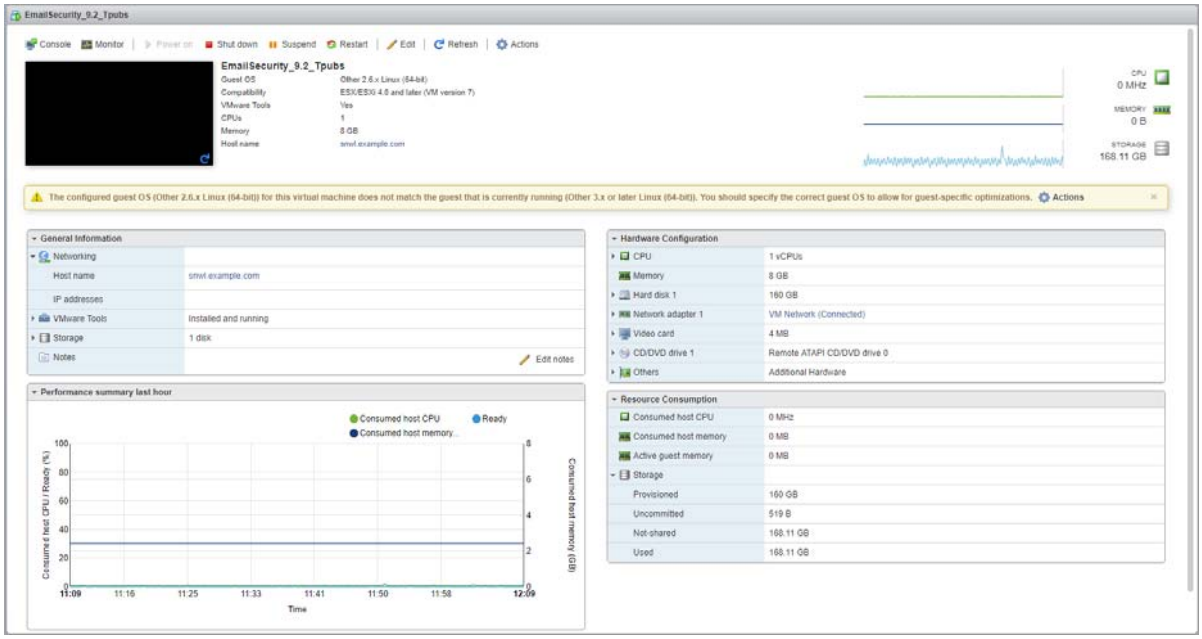
Viewing Settings Summary

When the SonicWall Email Security Virtual Appliance is selected, the **Summary** tab of the vSphere interface displays pertinent information such as memory, powered on/off state, hard disk storage usage, network subnet settings, and other settings.

NOTE: This page might incorrectly indicate that VMware Tools are not installed.

A short list of commands is also provided on this page, including **Power On, Suspend,** and **Edit**.

When using vSphere with vCenter Server, the **Migrate** and **Clone** commands are also available.



Editing Virtual Machine Settings

You can use the vSphere client to edit settings for the SonicWall Email Security Virtual Appliance, including memory, CPUs, descriptive name, datastore, and resource allocation.

To edit virtual machine settings:

1 In the vSphere client, right-click the SonicWall Email Security Virtual Appliance in the left navigation pane and select **Edit Settings** from the right-click menu.

2 In the **Virtual Machine Properties** page, the Hardware tab displays the settings for memory, CPU, hard disk, and other hardware. Click on the arrow in the table to access the editable settings in the **Hardware Configuration** panel.

Hardware Configuration	
CPU	1 vCPUs
Memory	8 GB
Hard disk 1	
Backing	[datastore1] EmailSecurity_9.2_Tpubs/EmailSecurity_9.2_Tpubs.vmdk
Capacity	160 GB
Thin provisioned	No
Controller	SCSI controller 0:0
Mode	Dependent
Network adapter 1	VM Network (Connected)
Video card	4 MB
CD/DVD drive 1	Remote ATAPI CD/DVD drive 0
Others	Additional Hardware

3 Click the **Actions** icon to view and edit the SonicWall Email Security Virtual Appliance name, guest operating system, and other settings.

4 Click the **Resource Consumption** panel to view and edit the resource allocation settings.

Powering the Virtual Appliance On or Off

There are multiple ways to power the SonicWall Email Security Virtual Appliance on or off.

To power the virtual appliance on (or off):

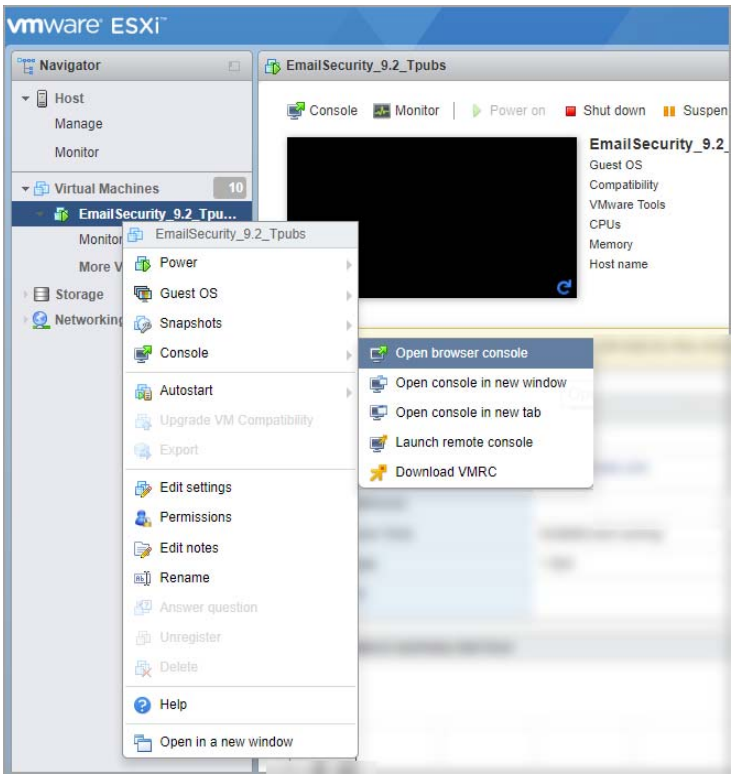
1 Do one of the following:

- Right-click the SonicWall Email Security Virtual Appliance in the left pane and click **Power > Power On** (or **Power > Power Off**) in the right-click menu.
- Select the SonicWall Email Security Virtual Appliance in the left pane and then click **Power on the virtual machine** (or **Shut down the virtual machine**) on the appliance tool bar at the top of the screen.

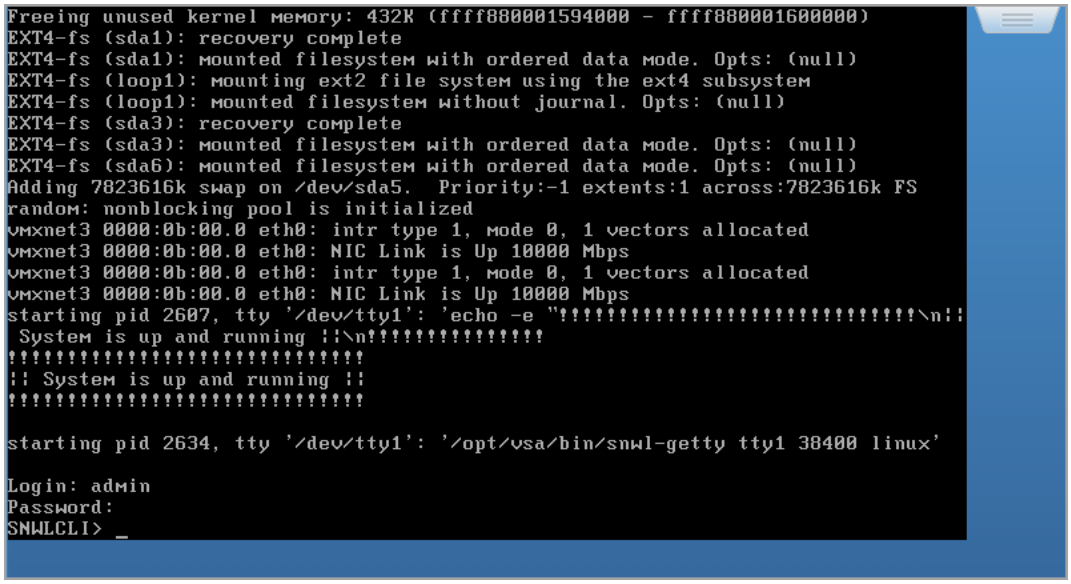
Configuring Host Settings on the Console

After powering on the SonicWall Email Security Virtual Appliance, perform the following steps to open the console and configure the IP address and default route settings:

1 In vSphere, right-click the SonicWall Email Security Virtual Appliance in the left pane and select **Open Console in new tab** in the right-click menu.



2 When the console window opens, click inside the window, type **admin** at the Login: prompt and press **Enter,** and then type **password** at the Password: prompt and press **Enter**. The SNWLCLI> prompt is displayed.



NOTE: The mouse pointer disappears when you click in the console window. To release it, press Ctrl+Alt.

3 Configure the local IP address for the virtual appliance with the command:

interface eth0 <IP Address> <Subnet Mask>

4 Configure the DNS with the command:

dns --nameserver <DNS IP>

5 Configure the default route for the virtual appliance with the command:

route --add default --destination <gateway IP>

You can test connectivity by pinging another server or your main gateway, for example:

ping <gateway IP>

Press **Ctrl+c** to stop pinging.

6 Type **exit** to exit the CLI. Close the console window by clicking the **X**.

4

Initial Setup and Configuration

After configuring the IP address and default route settings on the SonicWall Email Security Virtual Appliance console, the next steps are to configure host name, network, and time settings in the appliance management interface.

Topics:

Logging Into SonicWall Email Security

Perform the following steps to complete log into the Email Security Appliance:

1 Launch a browser and enter the URL of the virtual appliance.

If you assigned a web server port number other than 80, you will need to add the port number to the Web address to manually access the Email Security software user interface, using this format: <http://localhost:port/login.html>.

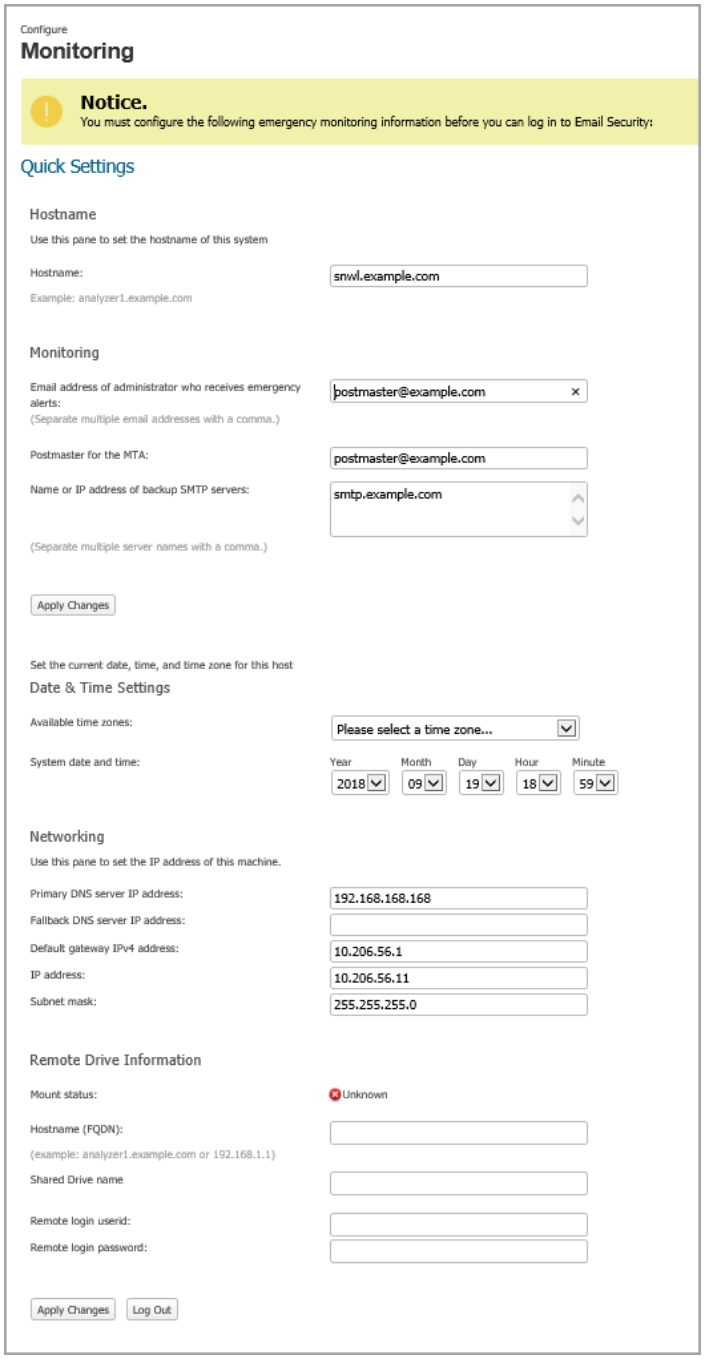
For example, if you assigned port 8080, the address would be: <http://localhost:8080/login.html>.

2 The login page displays. Enter **admin** in the **User Name** field and **password** in the **Password** field.

3 Click **Log In**.

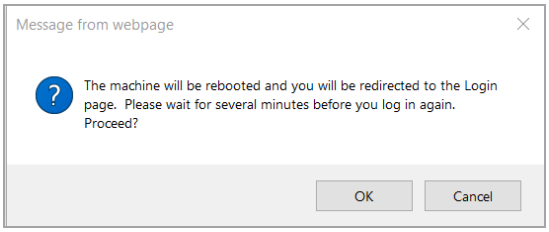
4 If this is the first time you have logged into a SonicWall Email Security appliance, you must enter the following system configuration information before you can continue:

- **Monitoring**—The email address of the mail server administrator who receives emergency alerts, the email of the MTA postmaster who will receive emergency alerts, and the name or IP address of the SMTP servers.
- **Hostname**—A descriptive hostname for this SonicWall Email Security appliance.
- **Networking**— The static IP address for this computer, including the Primary and Fallback DNS server IP addresses.
- **Date and Time**—The system date and time, current time zone, and an option for automatically adjusting for Daylight Savings Time.



When you have finished configuring these system settings, click **Apply Changes** to continue.

5 A dialog box warns you that the virtual appliance will reboot. Click **OK**.



NOTE: If you modified the DNS settings, the services on the appliance will restart when the changes are applied, causing a momentary connectivity loss to the Web server. Your browser will be redirected to the appliance management interface login page. If you modified the Time settings, the virtual appliance will reboot. Use your browser to reconnect to the appliance management interface.

Registering Email Security and Activating Licenses

The SonicWall Email Security Virtual Appliance must be registered before use. SonicWall Email Security provides dynamic licensing, which allows you to activate your licenses by simply logging into your mysonicwall.com account and entering the serial number and authentication code that came with your purchase of Email Security Software. Most of the licensing process takes place on mysonicwall.com and not the administration interface.

A MySonicWall account is required for product registration. If you do not have an account, see Creating a MySonicWall Account on page 19. If you already have an account, continue to Registering Your Email Security Virtual Appliance on page 17.

This section contains the following subsections:

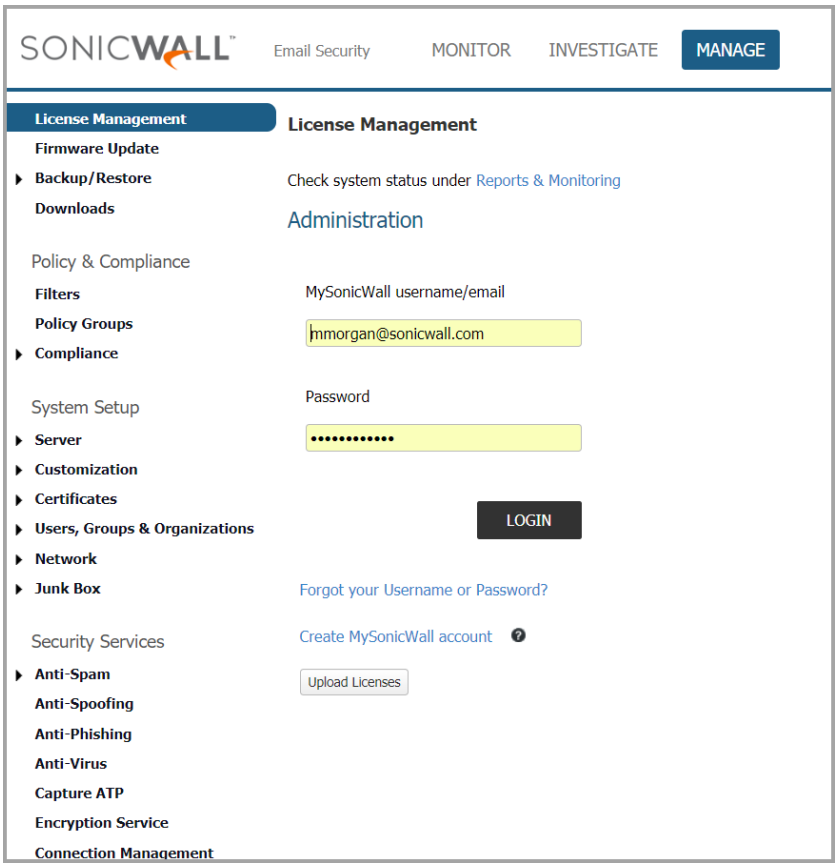
Registering Your Email Security Virtual Appliance

You must register your SonicWall Email Security Virtual Appliance before first use. Registration is performed using the appliance management interface. When registration is completed, SonicWall Email Security will be licensed on your virtual appliance.

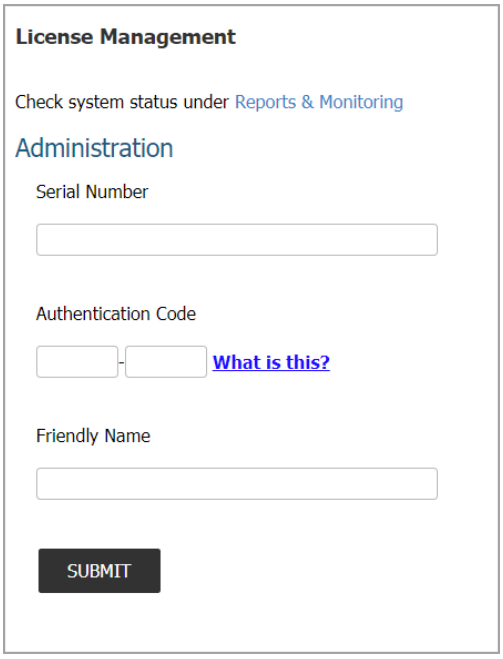
To register your SonicWall Email Security Virtual Appliance, perform the following steps:

1 Log in to your SonicWall Email Security Virtual Appliance. The **MANAGE | License Management** page displays.

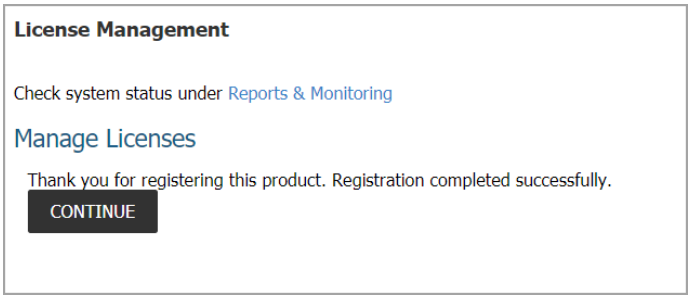
2 Enter your MySonicWall.com account **Username** and **Password** in the appropriate fields then click **LOGIN**.



3 The Administration section displays. Enter the **Serial Number**, **Authentication Code**, and **Friendly Name** for your SonicWall appliance.



4 Click **Submit**. A confirmation page appears stating the registration is completed successfully.



5 Click **Continue** to view the Manage Licenses screen or continue configuring other settings within the appliance.

Creating a MySonicWall Account

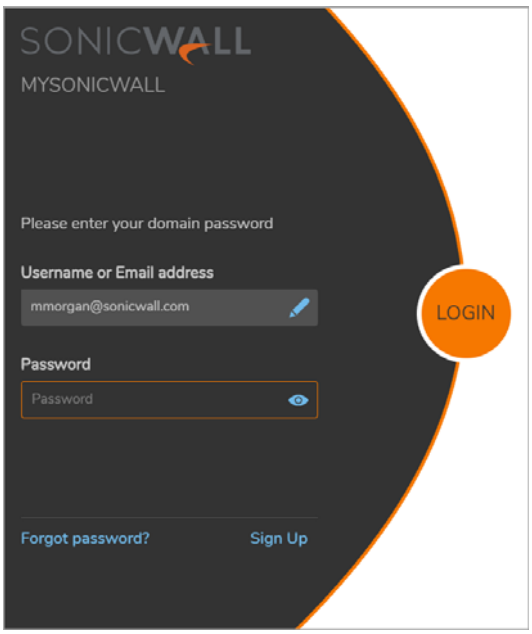
A MySonicWall account is required for product registration.

NOTE: Mysonicwall.com registration information is not sold or shared with any other company.

To create a MySonicWall account:

1 In your browser, navigate to http://www.mysonicwall.com.

2 On the login page, click the **Sign Up** link.



3 Complete the Registration form, then click **Register**.

4 Follow the prompts to finish creating your account. SonicWall will email a subscription code to the email address you entered in the personal information.

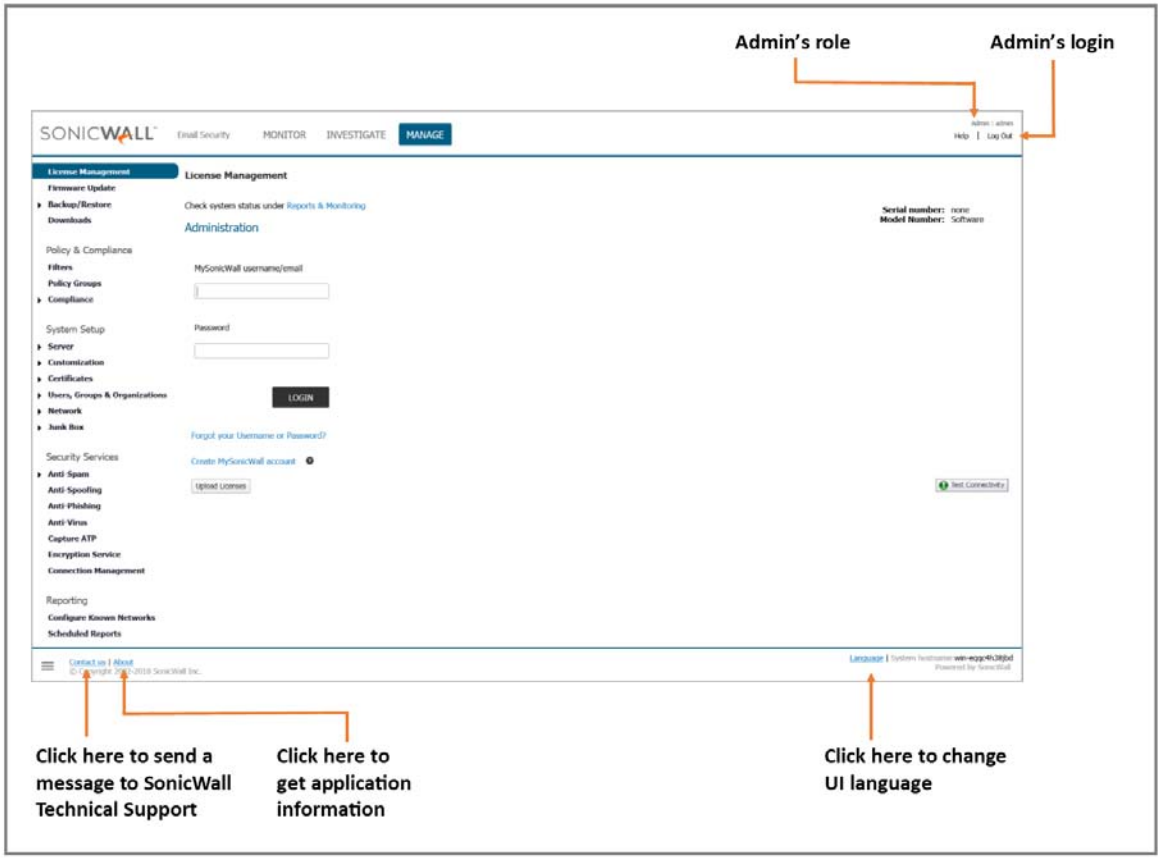
5 Verify that the information is correct and click **Submit**.

6 In the screen confirming that your account was created, click **Continue**.

NOTE: MySonicWall registration information is not sold or shared with any other company.

Overview of the Email Security Interface

This section describes the SonicWall Email Security management interface.



For a detailed SonicWall Email Security management interface overview, refer to the *SonicWall Email Security Administration Guide*.

Changing the Default Administrator Password

Change the default password for security reasons.

To change the default password:

1. In the Email Security user interface, navigate to the **MANAGE |System Setup | Server > Administration** page.
2. In the Email Security Master Account section, enter the old password in the **Old Password** field.
3. Enter a new management password into the **New Password** field.
4. Enter the new password again in the **Confirm Password** field.
5. Click **Apply Changes**.

5

Verification and Further Configuration

This section contains the following subsections:

Updating the Email Security Virtual Appliance

The **System > Advanced** page of the appliance interface is used to update the SonicWall Email Security Virtual Appliance to a newer build or version.

To update the SonicWall Email Security Virtual Appliance, perform the following steps:

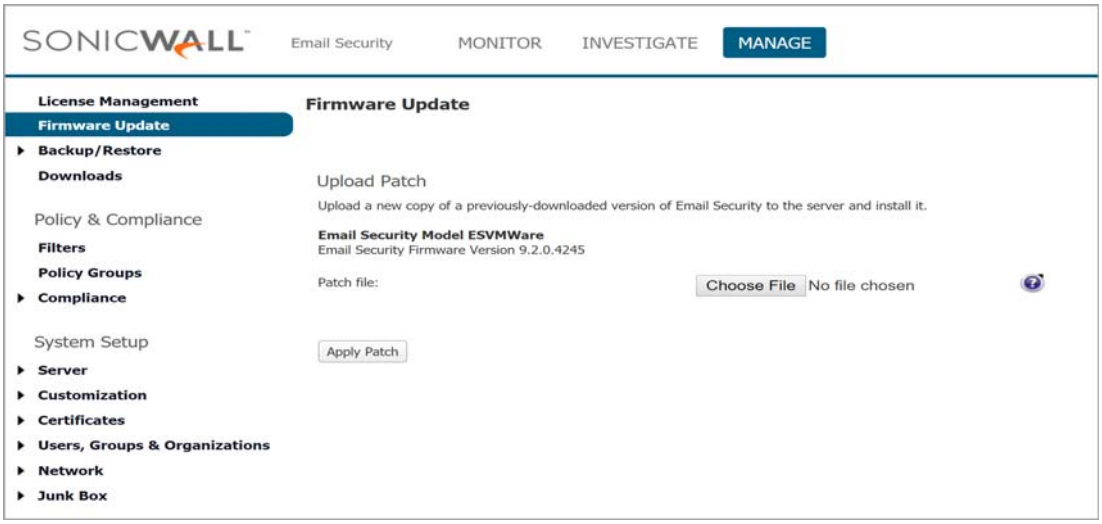
1 Download the updater file from MySonicWall. The file name is in the format:

es-X.X.X.XXXX-linux-updater-Haswell-der-signed.sh

NOTE: Do not rename the updater file.

2 Log on to the appliance interface of the SonicWall Email Security Virtual Appliance and navigate to the **MANAGE | Firmware Update** page.

3 Click **Choose File** and select the ***es-X.X.X.XXXX-linux-updater-Haswell-der-signed.sh*** file on your local system.



4 Click **Apply Patch** to update your virtual appliance with the new software.

Backup and Restore

Note that all configuration data resides on the Central Console (CC). Because there is really no stored or persistent data on the Remote Agent (RA), taking a snapshot of an RA and restoring it at a later time will not cause issues with other RAs. Any time a new RA is brought online and associated with a CC, the settings are replicated out to the RA.

Routing Mail to Your SonicWall Email Security

For your SonicWall Email Security software to start filtering and monitoring mail, you must re-route mail traffic through your SonicWall Email Security software. Mail traffic must pass from the Internet to the software, and then the software sends the good mail on to your mail server.

You have two choices to route mail traffic to your SonicWall Email Securitysoftware before your mail server:

- Change the MX record in your DNS server to resolve to the IP address of your SonicWall Email Security software. You may have to work with your ISP to change this record.
- Create a rule in your firewall or router to route all port 25 (SMTP mail) traffic to your SonicWall Email Security software. Refer to your firewall or router documentation for instructions on creating rules to route traffic.

Verifying Mail from the Internet Through Your SonicWall Email Security

To verify mail from the Internet:

1 Go to an external mail account, for example Yahoo mail or GMail.

2 Create a new email message:

To:	An email address where you receive email that is on the mail server for which you have configured the SonicWall Email Security software.
Subject:	SonicWall Email Security Verification Message
Body:	SonicWall Email Security Verification Message

3 Send the message.

4 In the SonicWall Email Security software administrative interface, click the **Auditing** button on the top.

5 Check the **Inbound** auditing reports to make sure the email appears as Delivered.

6 Check the mail account you sent the message to. If you received the message, you have correctly configured your SonicWall Email Security software.

Configuring Outbound Mail Filtering

Your SonicWall Email Security software can filter outbound mail from your mail server to the Internet. To configure outbound mail filtering, you configure both your mail server and your SonicWall Email Security software for the outbound mail path.

Configure the outbound mail destination of your mail server to point to the IP address or host name of your SonicWall Email Security software. This is typically done by configuring a Smart Host on your mail server.

On your SonicWall Email Security software, in the **Server Configuration > Network Architecture page**, configure a separate, outbound path to handle the outbound email flow at the software (if not already configured).

Configure the path to use the MTA (MX routing or SmartHost) under **Destination of Path**.

Configure something unique between the inbound and outbound path to distinguish inbound from outbound mail flow. A very simple way to do this is to have them listen on different ports or enter the IP address of the Exchange Server as the **Source IP Contacting Path** on the outbound path.

Example

Given:

```
10.100.0.10: Exchange Server (exch1.example.com)
10.100.0.100: SonicWALL Email Security software (esa.example.com)
```

You might have two paths like this:

```
          Source IP    Listen On  Destination
Inbound   Any          Any:25     (proxy) exch1.example.com:25
Outbound  10.100.0.10  Any:25     MX
```

In this scenario, any message that arrives at the SonicWall Email Security software from 10.100.0.10 will be treated as an outbound message, handed off to the MTA component in the system, which will deliver the message via MX-lookup on the domain in the **TO** field. Messages that arrive at the SonicWall Email Security software from any other IP address will be treated as an Inbound message, and delivered directly to the Exchange server. The SonicWall Email Security software always gives preference to specific matches (for example an exact IP address match takes precedence over “Any”).

Another example using port numbers to distinguish which path a message should take:

```
          Source IP  Listen On  Destination
Inbound   Any        Any:25     (proxy) exch1.example.com:25
Outbound  Any        Any:2525   MX
```

Another alternative would be to assign your SonicWall Email Security software multiple IP addresses, and have it listen on one for inbound and one for outbound.

In all of the above cases, the admin will configure Exchange to deliver outbound email to the IP address and port number where the SonicWall Email Security software is listening for outbound mail.

To test your SonicWall Email Security software, click the Auditing button at the top of the SonicWall Email Security software user interface and search for your sent email to verify it has been sent and received.

6

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

For answers to all your support questions, visit the SonicWall Support Web site at: http://www.sonicwall.com/us/Support.html where you'll find featured support topics, tutorials, and more. If you need further assistance, SonicWall offers telephone, email, and Web-based support to customers with valid Warranty Support or a purchased support contract. Please review our Warranty Support Policy for product coverage.

Related Documentation

The SonicWall Email Security 9.2 documentation set includes the following user guides:

- SonicWall Email Security 9.2 *Administration Guide*
- SonicWall Email Security 9.2 *User's Guide*
- SonicWall Email Security 9.2 *Software Getting Started Guide*
- SonicWall Email Security 9.2 *Release Notes*
- SonicWall Anti-Spam Desktop 6.2 *User's Guide*
- SonicWall Anti-Spam Desktop *Quick Start Guide*

For basic and advanced deployment examples, refer to SonicWall Email Security user guides.

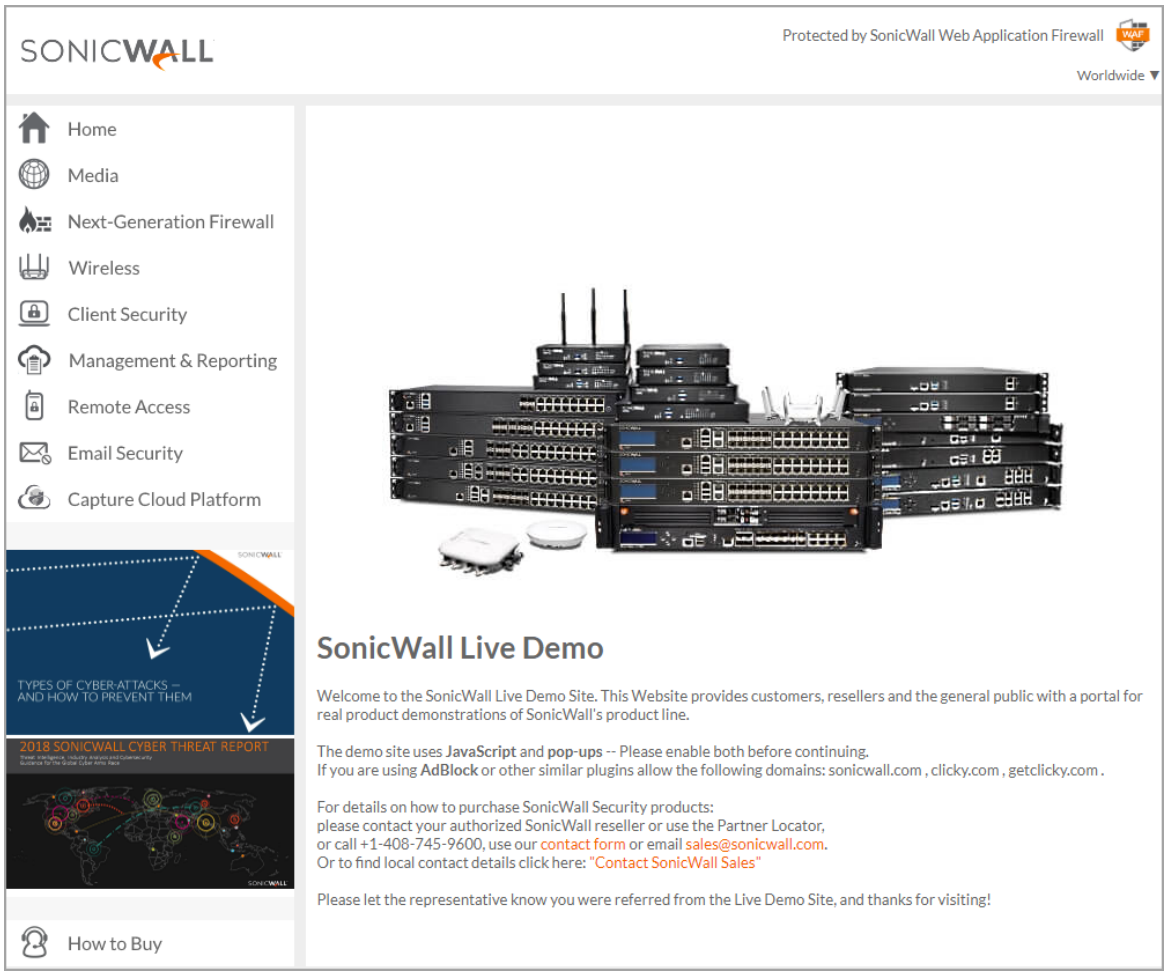
SonicWall Live Product Demos

Get the most out of your SonicWall Email Security with the complete line of SonicWall products. The SonicWall Live Demo Site provides free test drives of SonicWall security products and services through interactive live product installations:

- Media
- Next-Generation Firewall
- Wireless
- Client Security
- Management and Reporting
- Remote Access
- Email Security
- Capture Security Platform

For further information, visit:

http://livedemo.sonicwall.com/



About This Document

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

Email Security Getting Started Guide
Updated - October 2018
Software Version - 9.2
232-004530-00_Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035