

SonicWall® Email Security

9.2

Managed Service Provider Deployment
Guide



Contents

Email Security as a Service	4
Custom Branding in Email Security	5
Quick Settings	5
Text Preferences	6
Image Preferences	6
Junk Summary Preferences	8
Packages	8
Using Multi-Tenancy with Email Security	12
Pre-Configuration Caveats	12
Adding an Organizational Unit (OU)	14
Setting up Active Directory on the OU	15
Configuring Email	15
Configuring the Inbound Path	15
Configuring Outbound Email	16
Setting up an MSP Environment	17
Distributing Mail Flow to Multiple Remote Analyzers	18
Setting Up Split Configuration	18
Setting up the RA for Inbound Mail Flow	19
Routing Inbound Mail to Mail Servers	20
Understanding Proxy and MTA Mode	20
Setting up the RA for Outbound Mail Flow	21
Routing Outbound Mail to the WAN	21
Global vs. OU Administration	22
Spam Management Access for Tenants	22
Setting Up User Accounts	22
Configuring Organization LDAP Settings	22
Adding an Email Address for Alerts	22
Understanding Connection Management Settings	23
Configuring the Log Feature	23
Global Logging	23
Logging for Organizations	24
Configuring End User Login Access for Junk Box Summary	25
Configuring End User Login per OU	25
Reports and Monitoring	27
Using the Reports	27
Customizing the Display	27
Configuring Chart Formats	28
Filtering Chart Data	29
Managing Table Formats	29
Customizing Data Table Formats	29

Sorting	29
Search Filters	30
User Statistics	30
SonicWall Support	32
About This Document	33

Email Security as a Service

Managed Service Providers can set up SonicWall® Email Security as a managed service for customers, effectively deploying Email Security as a Service (ESaaS). The SonicWall Email Security virtual appliance or regular appliance can be used in the deployment. Any deployment of ESaaS is compatible with the built-in Multi-Tenancy features and can be custom branded for the desired appearance.

This deployment guide provides information and procedures for Managed Service Providers to deploy the Email Security product as a service.

This guide includes the following topics:

- [Custom Branding in Email Security](#)
- [Using Multi-Tenancy with Email Security](#)
- [Setting up an MSP Environment](#)
- [Reports and Monitoring](#)

Custom Branding in Email Security

This section provides information about branding in the Email Security product. Branding provides the ability to customize aspects of the user interface. Administrators can upload replacement assets for the key branding elements, including company name, logo, and other branding assets. The **MANAGE | System Setup > Customization > Branding** page includes the following tabs:

- [Quick Settings](#)
- [Packages](#)

Quick Settings

The **Quick Settings** options allows you to specify global settings for particular elements on the user interface.

NOTE: Any settings configured in **Quick Settings** overrides those specified by deployed packages.

Quick Settings

Packages

Preferences

Use this section to specify global settings for particular GUI elements. Any settings specified here will take precedence over those specified by deployed packages.

Text Preferences

Contact Us URL: [Test Connectivity](#)

(Examples: somebody@somewhere.com or http://contact.info.net/)

Image Preferences

Web Icon file: (favicon.ico)	Choose File No file chosen	
Logon logotype file: (logon.logotype.png)	Choose File No file chosen	
Logon backdrop art file: (logon.backdrop.png) [this file has been modified.]	Choose File No file chosen	
Page logotype file: (page.logotype.png)	Choose File No file chosen	
Page header art file: (page.header.png)	Choose File No file chosen	
Pop-up logotype file: (popup.logotype.png)	Choose File No file chosen	
Pop-up header art file: (popup.header.png)	Choose File No file chosen	

Junk Summary Preferences

Junk Summary logotype file: (junksummary.logotype.png)	Choose File No file chosen	
Junk Summary header art file: (junksummary.header.png)	Choose File No file chosen	

Save

Reset

The following sections are available on the Quick Settings tab:

- [Text Preferences](#)
- [Image Preferences](#)
- [Junk Summary Preferences](#)

Text Preferences

The **Text Preferences** section allows you to modify the email address or URL tied to the Contact Us link that appears in the footer of each page.

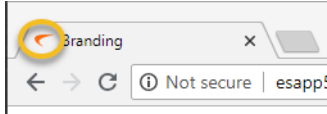


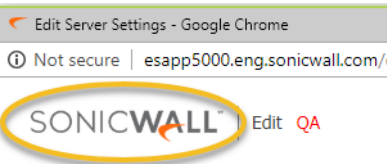
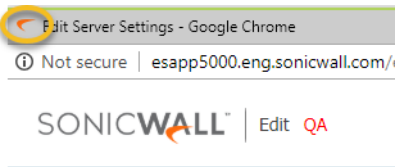
To configure Contact Us URL:

- 1 Navigate to **MANAGE | System Setup > Customization > Branding**.
- 2 Ensure the **Quick Settings** option is selected.
- 3 Input an email address or a custom URL in the field labeled **Contact Us URL**. It supports http://, https://, and mailto: formats.
- 4 Click **Save**.
- 5 Click **Test Connectivity** to verify the link was configured correctly.

Image Preferences

The **Image Preference** files can all be customized by choosing a file locally or downloading a new file. An error message displays if you uploaded an incorrect file type. Each file has to meet the specifications listed in the following table.

File	Description	Specifications
Web Icon file 	This field replaces the 4-bit SonicWall logo that appears in the address bar of every web page across all browser platforms.	The filename must be favicon.ico . Dimensions must be 32x32 pixels.
Logon logotype file 	This field replaces the short version of the SonicWall logotype that appears at the top of each web page's banner art.	The filename must be logon.logotype.png . Dimensions must be 144x67 pixels.

File	Description	Specifications
Logon backdrop art file	This field replaces the logotype bitmap that appears with every challenge screen, similar to the Logon logotype file .	The filename must be logon.backdrop.png . Dimensions must be 425x40 pixels.
Page logotype file 	This field replaces the short version of the SonicWall logotype that appears at the top the login banner.	The filename must be page.logotype.png . Dimensions must be 144x67 pixels.
Page header art files	This field replaces the SonicWall banner art bitmap at the top of each web page.	The filename must be page.header.png . Dimensions must be 15x93 pixels.
Pop-up logotype file 	This field replaces the smaller version of the SonicWall logotype that appears at the top of each pop-up dialog's page banner art.	The filename must be popup.logotype.png . Dimensions must be 144x67 pixels.
Pop-up header art file 	This field replaces the smaller version of the SonicWall banner art that appears at the top of each pop-up dialog page.	The filename must be popup.header.png . Dimensions must be 15x93 pixels.

To choose a local file:

- 1 Navigate to **MANAGE | System Setup > Customization > Branding**.
- 2 Ensure the **Quick Settings** option is selected.
- 3 Click on **Choose File** for the file you want to replace.
- 4 Navigate to the file, select it and click **Open**.

NOTE: You get an error if you select a file that is the wrong file type. Click **Reset**, at the bottom of the page, to remove the file choice.

A green note is added under the file type, stating that this file has been modified, and the file name is listed.

To download a file:

- 1 Navigate to **MANAGE | System Setup > Customization > Branding**.
- 2 Ensure the **Quick Settings** option is selected.
- 3 Click on the **Download** button to download the current version of the file selected.
- 4 Confirm that you want to download the file.

The file can now be modified and then selected for an image preference.

To remove a modified file:

When a file has been modified, the delete button is added so you have the option to remove the file.

Logon backdrop art file:
(logon.backdrop.png)
[this file has been modified.]

Choose File No file chosen



- 1 Navigate to **MANAGE | System Setup > Customization > Branding**.
- 2 Ensure the **Quick Settings** option is selected.
- 3 Click on the **Delete** button to remove the current version of the file selected.

Junk Summary Preferences

The Junk Summary Preferences can all be modified by clicking the **Choose File** button or clicking the **Download** icon to download the default image file. An error message displays if you try to upload an incorrect file type.

The following Junkbox Summary Preferences can be modified:

- **Junkbox Summary logotype file** - This field replaces the black-on-white logotype that always appears at the top of each Junkbox summary email. When uploading a new file, make sure the filename is **junksummary.logotype.png** with a dimension of 144x67 pixels.



Junk Emails Blocked: 2

- **Junkbox Summary header art file** - This field replaces the Junkbox summary banner art bitmap at the top of each page. When uploading a new file, make sure the filename is **junksummary.header.png** with a dimension of 15x93 pixels.

Packages

On the Packages tab, administrators can manage, upload, and apply branding packages to their user interface. The Manage Packages table displays the available packages the administrator can apply to the interface,

including the default brand package, which cannot be deleted. Administrators can edit or delete all other brand packages that have been uploaded.

Quick Settings

Packages

Manage Packages

These are the currently available packages. Click the "Upload" button to upload another package. Click [here](#) to download the SonicWall package.

	Package	Brand	Full name	Size (KB)	Date	Contact Us	Notes	Configure
	SonicW...	SonicW...	SonicWALL	1926.1	11/10/2016 14:16...	http://www.sonic...	This is the SonicWALL package; it can't be deleted. All other packages when added and applied will ov...	

Apply

Upload

Upload Package

The easiest way to build a customized package is to download the default SonicWall package and then use it as a template. The new package has to have the same directory structure as that of the default package. The names of the files must be also be identical to the default package. Save the new package in .zip format before uploading it.

The following files can be customized for your configuration:

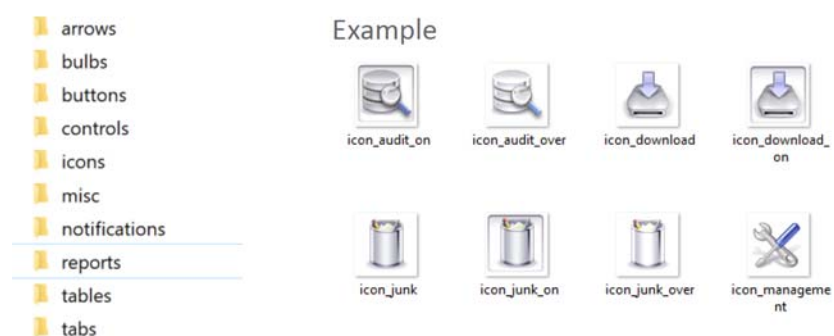
Cascading style sheets

You can edit the cascading style sheets (.css files) so you can provide customize the layout, fonts and colors.

	SWLbanner	Cascading Style Sheet Doc
	SWLbranding	Cascading Style Sheet Doc
	SWLbubble	Cascading Style Sheet Doc
	SWLbutton	Cascading Style Sheet Doc
	SWLdialog	Cascading Style Sheet Doc
	SWLfooter	Cascading Style Sheet Doc
	SWLform	Cascading Style Sheet Doc
	SWLgrid	Cascading Style Sheet Doc
	SWLhelpinfo	Cascading Style Sheet Doc
	SWLicon	Cascading Style Sheet Doc
	SWLjunkbox.summary	Cascading Style Sheet Doc
	SWLlayout	Cascading Style Sheet Doc
	SWLleftnav	Cascading Style Sheet Doc
	SWLlicense	Cascading Style Sheet Doc
	SWLlogin.overrides	Cascading Style Sheet Doc
	SWLmain	Cascading Style Sheet Doc
	SWLmodal	Cascading Style Sheet Doc
	SWLmodule	Cascading Style Sheet Doc
	SWLoverrides	Cascading Style Sheet Doc
	SWLpaginate	Cascading Style Sheet Doc
	SWLpaintbox	Cascading Style Sheet Doc
	SWLpopup	Cascading Style Sheet Doc
	SWLprintable.custom.reports	Cascading Style Sheet Doc
	SWLreset	Cascading Style Sheet Doc
	SWLsort	Cascading Style Sheet Doc
	SWLtab	Cascading Style Sheet Doc
	SWLtable	Cascading Style Sheet Doc
	SWLutility	Cascading Style Sheet Doc

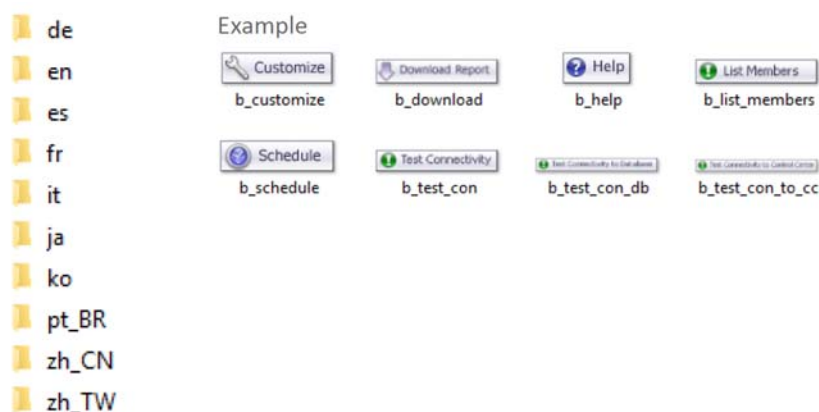
Miscellaneous elements

You can edit other images such as arrows, buttons, icons, and controls.



Language

You can edit the language action buttons.



To download the default package:

- 1 Navigate to **MANAGE | System Setup > Customization > Branding**.
- 2 Select the **Packages** option.
- 3 Click the **Download** icon for the default package.

To upload a new package:

- 1 Navigate to **MANAGE | System Setup > Customization > Branding**.
- 2 Select the **Packages** option.
- 3 Click **Upload**.

Upload Package

Uploads are restricted to .zip files and must contain the exact structure of the directories to modify or replace. Click [here](#) to download the SonicWall package.

File to upload
(* .zip) No file chosen

Brand Label:

Full name

Contact Us
(Examples: somebody@somewhere.com or http://contact.info.net/)

Notes

- 4 Click **Choose File** and navigate to the .zip file you want to upload.
- 5 Type the **Brand Label** in the field provided.
- 6 Type the **Full name** of the package in the field provided.
- 7 In the **Contact Us** field, add either an email address or a URL where you can be contacted.
- 8 Add any other details about the package in the **Notes** field.
- 9 Click **Save**.

Using Multi-Tenancy with Email Security

Multi-tenancy features allow for a single instance of software to run on an appliance and serve multiple groups of users, or tenants. The following sections provide information for deploying the Multi-Tenancy functionality for Email Security.

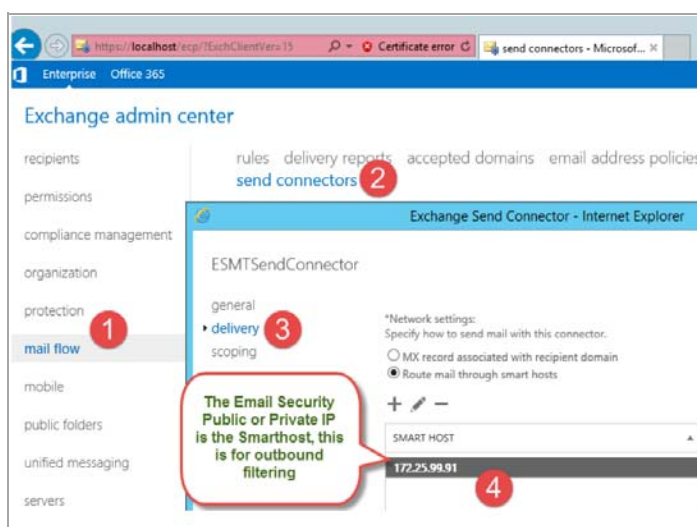
Topics:

- [Pre-Configuration Caveats](#)
- [Adding an Organizational Unit \(OU\)](#)
- [Setting up Active Directory on the OU](#)
- [Configuring Email](#)
- [Configuring Outbound Email](#)

Pre-Configuration Caveats

Review and understand the impact of the following caveats when setting up multi-tenancy with your Email Security solution:

- Each tenant needs to have both inbound and outbound email filtered by the Email Security solution.
- Each tenant needs to modify the MX record to point to the public IP where the SonicWall Email Security appliance can be reached. This typically is not the same IP address where the Exchange server is located.
- The local Exchange server has the Email Security IP address as a smart host in the **Send Connector** section. The image below shows how to navigate to the **ESMT Send Connector** page.



- To integrate Active Directory (AD) with the Email Security solution, set up a VPN tunnel between the sites, or configure an inbound firewall rule for TCP port 389 or port 636. The image below shows how to set the rule on a SonicWall network security appliance between two zones:

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From :

To :

Source Port:

Service:

Source:

Destination:

Users Included: ... these users will be allowed if not excluded,

Users Excluded: ... these users will be denied.

Schedule:

Comment:

☒ Enable Logging ☐ Enable Geo-IP Filter

☒ Allow Fragmented Packets ☐ Enable Botnet Filter

☐ Enable flow reporting

☐ Enable packet monitor

☐ Enable Management

NOTE: When the source IP is a public IP, an inbound NAT policy must be created on the SonicWall network security appliance. Refer to the KB article, [SonicOS Enhanced How To Configure NAT Policies](#), for more information.

- When deploying your Email Security solution, the basic Host Configuration information may be changed from the default IP address (192.168.168.169).
 - Navigate to the **MANAGE** view.
 - Select **System Setup > Server > Host Configuration**.
 - Scroll down to **Network Settings**.

Network Settings

Use these settings to configure the host system on which Email Security is running.

- ☒ Use the static settings below

Networking

Use this pane to set the IP address of this machine.

Primary DNS server IP address:	
Fallback DNS server IP address:	
Default gateway IPv4 address:	
Default gateway IPv6 address: (Required when IPv6 interface is configured)	

This textbox will be enabled, if one or more IPV6 addresses are added to the interface.

Ethernet 0

- ☒ Enable use of Ethernet0 port

IP address:	
Subnet mask:	

d Enter the following:

- Primary DNS server IP address
- Default gateway IP address
- IP address of the interface connects to the network
- Network submask

Adding an Organizational Unit (OU)

To add a tenant or Organizational Unit:

- 1 Navigate to the **MANAGE view** and select **System Setup > Users, Groups & Organizations > Organizations**.
- 2 Click the **Add Organization** button.
- 3 Enter the **Primary Domain**.
- 4 Enter a name for the **Organization Admin Login ID**. Based on the data provided, Email Security automatically pulls the **Admin Login ID** from that domain.
- 5 Enter a password for the **Organization Admin Password**.
- 6 Enter additional **Domains** associated with the tenant. Multiple domains can be separated with a comma, space or carriage return.

NOTE: Adding multiple domains under one organization allows you to manage multi-tenancy.

- 7 Click **Add**. A warning message displays regarding domains per-user data migration.
- 8 Click **OK** to finish adding the OU.

Setting up Active Directory on the OU

Before setting up Active Directory on an individual OU, you need login as the OU administrator. Configuration changes made then only apply to that OU and not the entire Email Security implementation.

To set up Active Directory (AD) on the OU:

- 1 Navigate to the **MANAGE view** and select **System Setup | Users, Groups & Organizations > Organizations** page.
- 2 Click the **Sign In** icon of the OU you wish to configure (in the **Actions** column). You can tell you are logged in as the OU administrator by seeing the username and OU listed in the upper right corner of the Email Security window.
- 3 Navigate to the **MANAGE view** and select **System Setup > Server > LDAP Configuration**.
- 4 Click **Add Server**.
- 5 Enter a **Friendly Name** or keep the default provided.
- 6 Enter the LDAP IP address in the **Primary Server name or IP address** field.
- 7 Enter the LDAP **Port Number** or keep the default provided.
- 8 Select **Active Directory** as the **LDAP server type**.
- 9 For **Authentication Method**, select **Login**.
- 10 Enter a **Login Name** to log into the domain. This can be a regular domain user.
- 11 Enter the **Password** for this user.
- 12 Click the **Test LDAP Login** button to verify this user is able to successfully log in to the LDAP server.
- 13 Click **Save Changes** to finish setting up AD.

Configuring Email

The global administrator configures the email parameters for the Email Security solution. If you are logged in as the OU administrator, the options for configuring the mail paths are not available.

Configuring the Inbound Path

To configure the Inbound Email path:

- 1 Navigate to the **MANAGE view** and select **System Setup | Network Architecture > Server Configuration**.
- 2 With **All in One** selected, click the **Add Path** button under the heading **Inbound Email Flow** to add a new path. To edit an existing path, select an inbound path and click the **Edit Path** button.
- 3 In the **Source IP Contacting Path** section:
 - a Select **Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains**.
 - b Enter the domains for the tenants. Separate the domains with a carriage return.

 **NOTE:** SonicWall recommends listing all the domains that will be filtered through the Email Security solution.

- 4 In the **Destination of Path** section:
 - a Select **This is an MTA. Route email using MX record routing with these exceptions: ...**
 - b List the associated IP addresses and hostnames in the field provided. When making the entries, separate the domain from the IP address with a space and separate IP address with a comma. Then separate entries with a carriage return. For example:

```
eng.example.com 10.1.1.2,10.1.1.3,10.1.1.4  
salex.example.com 10.1.1.1
```
- 5 Click **Apply**.

Configuring Outbound Email

To configure the Outbound Email path:

- 1 Navigate to the **MANAGE view** and select **System Setup | Network Architecture > Server Configuration**.
- 2 With **All in One** selected, click the **Add Path** button under the heading **Outbound Email Flow** to add a new path. To edit an existing path, select an outbound path and click the **Edit Path** button.
- 3 In the **Source IP Contacting Path** section:
 - a Select **Only these IP addresses/FQDNs can connect and relay through this path:**
 - b Enter the IP addresses in the field provided. Separate addresses with a comma.
- 4 In the **Destination of Path** section, select **This is an MTA. Route email using MX record routing. Queue email if necessary**.
- 5 Click **Apply** to finish configuring the outbound email path.

Setting up an MSP Environment

In a Managed Service Provider (MSP) environment, a Split Configuration is deployed to help scale for email volume, distribution of load, and to provide redundancy. Split-Configuration allows multiple Remote Analyzers (RA) to be deployed at various locations with a single point of management through the Control Center (CC).

The Control Center is an appliance that acts as a single point through which all end users view and manage their Junk Box. It is also the single point through which the system administrator can make and distribute the necessary changes to the Email Security infrastructure.

Email Security supports both Microsoft Exchange mail servers and Office 365.

Many things should be considered when setting up a Split Configuration as an MSP environment. Review the following topics to determine which are applicable and need to be set up for your environment:

- [Distributing Mail Flow to Multiple Remote Analyzers](#)
- [Setting Up Split Configuration](#)
- [Setting up the RA for Inbound Mail Flow](#)
- [Routing Inbound Mail to Mail Servers](#)
- [Understanding Proxy and MTA Mode](#)
- [Setting up the RA for Outbound Mail Flow](#)
- [Routing Outbound Mail to the WAN](#)
- [Global vs. OU Administration](#)
- [Spam Management Access for Tenants](#)
- [Setting Up User Accounts](#)
- [Configuring Organization LDAP Settings](#)
- [Adding an Email Address for Alerts](#)
- [Understanding Connection Management Settings](#)
- [Configuring the Log Feature](#)
- [Configuring End User Login Access for Junk Box Summary](#)
- [Configuring End User Login per OU](#)

Distributing Mail Flow to Multiple Remote Analyzers

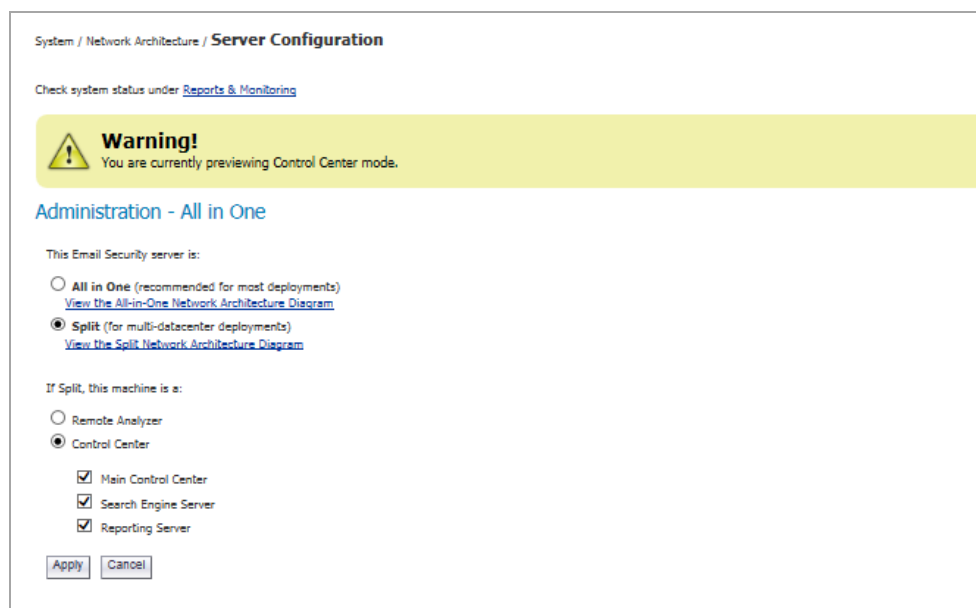
To distribute Mail Flow evenly across multiple Remote Analyzers, the two best practices are:

- Set up multiple ES devices in the DMZ utilizing a network security appliance to balance the inbound SMTP traffic load.
- Set up the Email Security appliance as the first-touch/last-touch server in the DMZ, using multiple MX records with the same priority or defining multiple A records in your DNS zone with the same name and different IP addresses.

 **NOTE:** Email Security appliances can be set on the LAN as well as the DMZ.

Setting Up Split Configuration

By default, the Email Security appliance is defined as an All-in-One device when first set up. To set up the **Split** configuration option recommended for an MSP environment, navigate to the **MANAGE** view and select **System Setup | Network > Server Configuration**. Define the appliance as a **Remote Analyzer** or the **Control Center**. Refer to the *Email Security Administration Guide* for more details.



Once you apply the new setting, the appliance restarts, and you need to log back in to the system. After logging back in, you can specify which hosts are the RA in your Split Configuration by clicking the **Add Server** button for Inbound or Outbound Remote Analyzer Paths.

Server Configuration - Control Center

Control Centers (where the Remote Analyzers send junk emails)

Add Server Edit Server Delete Server Test Connectivity

Control Centers
☐ greenland.srademo.com:2599

Inbound Remote Analyzer Paths

Add Server

Remote Analyzer	1. Source IP / 2. Path Listens On	3. Destination of Path	TLS
No remote analyzer servers are entered.			

Outbound Remote Analyzer Paths

Add Server

Remote Analyzer	1. Source IP / 2. Path Listens On	3. Destination of Path	TLS
No remote analyzer servers are entered.			

Setting up the RA for Inbound Mail Flow

To set up a Remote Analyzer for Inbound Mail Flow:

- 1 Navigate to the **System Setup | Network > Server Configuration** page on the **MANAGE** view.

NOTE: Before proceeding, you must have your Email Security server configured for Split Configuration with a server added as an Inbound Remote Analyzer Path as described in [Setting Up Split Configuration](#).

- 2 Select the Remote Analyzer you want to configure for Inbound Mail Flow and click the **Add Path** button under **Inbound Email Flow**.

In the **Source IP Contacting Path** section, select **Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains** and add the domains to be filtered for Inbound mail. Separate domains with a carriage return.

1. Source IP Contacting Path

Specify the IP addresses of other systems that are allowed to connect to and relay through this path.

☐ Any source IP address is allowed to connect to this path. (Warning: may make an open relay.)

☒ Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains:

demo.com
sonictest.com
sonicboom.com
sonicdemo.com

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

☐ Only these IP addresses / FQDNs can connect and relay through this path:

(Separate addresses with a comma.)

- 3 Scroll to the bottom of the window and click **Apply** to save the settings.

Routing Inbound Mail to Mail Servers

To route inbound mail to specific mail servers:

- 1 Navigate to the **System Setup | Network > Server Configuration** page on the **MANAGE** view.

NOTE: Before proceeding, you must have your Email Security server configured for Split Configuration with a server added as an Inbound Remote Analyzer Path as described in [Setting Up Split Configuration](#).

- 2 Select the Remote Analyzer you want to configure for Inbound Mail Flow and click the **Add Path** button under **Inbound Email Flow**.
- 3 In the **Destination of Path** section, select **This is an MTA. Route email using MX record routing with these exceptions** and add the email addresses or domains.

☐ This is an MTA. Route email using MX record routing.
Queue email if necessary.

[What is this?](#)

☒ This is an MTA. Route email using MX record routing with these exceptions:
Email sent to email addresses or domains in the table on the right is routed directly to the associated IP addresses or hostnames in Round-Robin mode. Email is queued if necessary.

[What is this?](#)

Separate the domain from the IP addresses with a space. Separate IP addresses with a comma. Separate entries with a <CR>. Examples:
engr.example.com 10.1.1.2,10.1.1.3,10.1.1.4
sales.example.com 10.1.1.1

This option allows routing of the message from Email Security to the recipient's mail server by way of MX records. It also allows for exceptions to be explicitly listed if the recipient domain's MX record have unforeseen issues.

- 4 Enter the domains and associated IP addresses in the text field provided. Separate the domain from the IP addresses with a space and separate IP addresses with a comma. Separate entries with a carriage return. For example:

```
engr.example.com 10.1.1.2,10.1.1.3,10.1.1.4  
sales.example.com 10.1.1.1
```

- 5 Scroll to the bottom of the window and click **Apply** to save the settings.

Understanding Proxy and MTA Mode

Email Security can run either as an SMTP Proxy or a Mail Transfer Agent (MTA). SMTP Proxy operates by connecting to a destination SMTP server before accepting messages from a sending SMTP server. The MTA service operates by writing messages to disk and allows for routing the message. The following table shows which features are supported on which option.

Proxy and MTA Features

Feature	Supported on MTA	Supported on Proxy
Spool email	Yes	No
Faster, more efficient connections	No	Yes
Multiple downstream servers	Yes	No

Setting up the RA for Outbound Mail Flow

This procedure is similar to creating the inbound paths for each RA.

To set up a Remote Analyzer for Outbound Mail Flow:

- 1 Navigate to the **System Setup | Network > Server Configuration** page on the **MANAGE** view.

NOTE: Before proceeding, you must have your Email Security server configured for Split Configuration with a server added as an Outbound Remote Analyzer Path as described in [Setting Up Split Configuration](#).

- 2 Select the Remote Analyzer you want to configure for Outbound Mail Flow and click the **Add Path** button under **Outbound Email Flow**.
- 3 In the **Source IP Contacting Path** section, select **Only these IP addresses / FQDNs can connect and relay through this path**.

- 4 Add the domains to the text field provided. Separate the addresses with a comma.
- 5 Scroll to the bottom of the window and click **Apply** to save the settings.

Routing Outbound Mail to the WAN

To route outbound mail to specific mail servers:

- 1 Navigate to the **System Setup | Network > Server Configuration** page on the **MANAGE** view.

NOTE: Before proceeding, you must have your Email Security server configured for Split Configuration with a server added as an Outbound Remote Analyzer Path as described in [Setting Up Split Configuration](#).

- 2 Select the Remote Analyzer you want to configure for Inbound Mail Flow and click the **Add Path** button under **Outbound Email Flow**.
- 3 In the Destination of Path section, select **This is an MTA. Route email using MX record routing. Queue email if necessary**.

When a path is configured with this choice, any messages received are routed by standard MX (Mail Exchange) records. This is the most common choice for outbound paths because in most configurations the email must be routed across the internet using MX records. With this choice, messages can be queued on disk and retry transmissions later if the destination SMTP server is not immediately available.

- 4 Scroll to the bottom of the window and click **Apply** to save the settings.

Global vs. OU Administration

Email Security has levels of administration built into the product. The highest level is the global administrator, and this level has the most privileges. Changes made by the global administrator can be applied to all domains specified in the global Email Security setup.

The OU (organizational unit) administrator can manage the setup that has been defined for a particular tenant. Once logged into an OU, the OU administrator cannot see other tenants' configurations. The functions that an OU administrator can perform are a subset of the functions that a global administrator manages.

Spam Management Access for Tenants

The tenant can log into the OU administration account specific to their Organization. They can configure organizational settings, including Spam Management settings. By navigating to the **Security Services | Anti-Spam > Spam Management** page, the OU administrator can select options for managing **Definite Spam** and **Likely Spam**. The default setting for Definite Spam and Likely Spam is to quarantine the message in the user's Junk Box.

Setting Up User Accounts

You can leverage LDAP for Email Security to automatically query and update user accounts from your LDAP server by navigating to the **MANAGE** view and then selecting **System Setup | Server > LDAP Configuration**.

If the client does not have an LDAP server, you can manually add each user to Email Security with complete login capability for Junkbox access and management. Navigate to the **System Setup | Users, Groups & Organizations > Users** page on the **MANAGE** view. Click the **Add** button and provide the new user information in the **Add User** window.

Configuring Organization LDAP Settings

To configure LDAP settings for organizations:

- 1 Navigate to the **System Setup | Users, Groups & Organizations > Organizations** page.
- 2 Click the **Sign in as Organization Admin** icon for the organization you want to configure.
- 3 Navigate to the **System Setup | Server > LDAP Configuration** page.
- 4 Click the **Add Server** button to add a new server or click the **Edit** icon to update a server definition.

Adding an Email Address for Alerts

You can customize and send alerts for global- and OU-related monitoring. For global alerts, you can define who receives emergency alerts, who receives outbound quarantine notifications and who the postmaster for the MTA is. For OU monitoring, you can set up emails for emergency alerts.

To set up global alerts:

- 1 Navigate to the **System Setup | Server > Monitoring** on the **MANAGE** view.

- 2 In the Monitoring section, enter the **Email address of administrator who receives emergency alerts**.
- 3 Set the preferred language for alerts.
- 4 Enter the **Email address of the administrator who received outbound quarantine notifications**.
- 5 Enter the **Postmaster for the MTA**.
- 6 Click **Apply Changes** to save the settings.

To set up OU alerts:

- 1 Navigate to the **System Setup | Users, Groups & Organizations > Organizations** on the **MANAGE** view.
- 2 Select the organization and log into that OU.
- 3 Navigate to the **MANAGE** view and select **System Setup | Server | Monitoring**.
- 4 Enter the **Email address of administrator who receives emergency alerts**.
- 5 Set the preferred language for alerts.
- 6 Set the remaining parameters if needed.
- 7 Click **Apply Changes** to save the settings.
- 8 Log out of the OU.

Understanding Connection Management Settings

The Connection Management settings are only supported at the global level; they cannot be set at the OU level. The Connection Management features that can be defined includes:

- Intrusion prevention settings like Directory Harvest Attack (DHA) protection and Denial of Service (DoS) attack protection
- Quality of Service settings such as throttling, connection limits, message limits and delayed connection management
- The ability to manually edit the IP address lists

To navigate to the Connection Management page, select **Security Services | Connection Management** on the **MANAGE** view.

Configuring the Log Feature

You can enable the Log feature and track the messages that Email Security has received. You can use these messages to investigate issues or audit status. Logging is available at both the global level of the configuration and at the organization level (tenant), although there are some differences.

Global Logging

To enable global logging:

- 1 Navigate to **Logs | Message Logs** on the **INVESTIGATE** page.

- 2 Select the **Inbound** or **Outbound** button, depending on which traffic you are configuring.
- 3 Click the **Settings** button.

Auditing for inbound email: ☒ on | ☐ off

Auditing for outbound email: ☒ on | ☐ off

Enable Judgment Details logging: ☒ on | ☐ off

Auditing for connections: ☒ on | ☐ off

Keep Email auditing files for: 30 Days ▼

Keep connection auditing files for: 30 Days ▼

Apply

- 4 Select on or off for the following features:
 - **Auditing for inbound email**
 - **Auditing for outbound email**
 - **Enable Judgment Details logging**
 - **Auditing for connections**
- 5 Select how long to **Keep Email auditing files for:** from the drop down menu.
- 6 Select how long to **Keep connection auditing files for:** from the drop down menu.
- 7 Click **Apply**.

The Message Logs page displays all of the messages sitting in the JunkStore. You have access to the message details of each message for both inbound and outbound messages. The table can be customized. Refer to the *Email Security Administration Guide* for details.

Logging for Organizations

To enable organization logging:

- 1 Navigate to the **System Setup | Users, Groups & Organizations > Organizations** on the **MANAGE** view.
- 2 Select the organization and log into that OU.
- 3 Navigate to the **INVESTIGATE** view and select **Logs | Message Logs**.
- 4 Select the **Inbound** or **Outbound** button, depending on which traffic you are configuring.
- 5 Click the **Settings** button.

Auditing for inbound email: ☐ on | ☒ off

Auditing for outbound email: ☐ on | ☒ off

Enable Judgment Details logging: ☐ on | ☒ off

Keep Email auditing files for: 30 Days ▼

Apply

- 6 Select on or off for the following features:
 - **Auditing for inbound email**
 - **Auditing for outbound email**
 - **Enable Judgment Details logging**
- 7 Select how long to **Keep Email auditing files for**: from the drop down menu.
- 8 Click **Apply**.

The Message Logs page displays all of the messages sitting in the JunkStore. You have access to the message details of each message for both inbound and outbound messages. The table can be customized. Refer to the *Email Security Administration Guide* for details.

Configuring End User Login Access for Junk Box Summary

You can configure the Junk Box so that a user has full access to their individual Junk Box. This is a two-step process where you first enable the access as the global administrator. Then you set up the appropriate LDAP mappings as the OU administrator.

To configure end user login access for Junk Box summary:

- 1 Navigate to **System Setup | Junk Box > Summary Notifications** on the **MANAGE** view.
 - 2 Scroll down to **Miscellaneous Settings**.
 - 3 Under the feature **Enable “single click” view of messages**:, select **Full access (clicking any link in a Junk Box Summary grants full access to this particular user’s settings)**.
 - 4 Scroll to the bottom of the list and select **Apply Changes**.
 - 5 Navigate to the **Users, Groups & Organizations > Organizations** page.
 - 6 Select the organization and log into that OU.
 - 7 Navigate to the **MANAGE** view and select **System Setup | Server > LDAP Configuration**.
-  **IMPORTANT:** LDAP must be configured before continuing.
- 8 On the LDAP Mappings section, enter the domains.
 - 9 Click **Save Changes**. This domain appears on the drop-down menu for the Login screen.
 - 10 Log out of the OU.

Configuring End User Login per OU

In some cases, you may prefer to preserve customer privacy. The LDAP Configuration page can be changed to specify an attribute that refers to the email address for the end user. As this may vary for various LDAP servers, the most commonly used attribute could be the UPN for the end user as used in Microsoft platforms.

To access the LDAP configuration page, select **System Setup | Server > LDAP Configuration** on the **MANAGE** view. Select the server and then expand the **LDAP Query Panel**.

LDAP Query Panel

These fields will be automatically filled in with default values after the basic server configuration steps are completed - if the "Auto-fill LDAP Query fields" checkbox is checked.

Query Information for LDAP Users:

Directory node to begin search: ?

Filter: ?

User login name attribute: ?

Email alias attribute: ?

Use SMTP addresses only ☐

Query Information for LDAP Groups:

Directory node to begin search: ?

Filter: ?

Group name attribute: ?

Group members attribute: ?

User membership attribute: ?

Change the **User Login Name Attribute** to **userPrincipalName** to allow the end user to log in using their email address.

Reports and Monitoring

SonicWall Email Security allows you to view system status and data through the **MONITORING** view. **MONITORING** is comprised of four key segments when logged in as an organization administrator: Dashboard, Event Summaries, Policy & Compliance, and Appliance Health. An additional segment, Current Status, is available when logged in as a global administrator.

By default, SonicWall Email Security retains 366 days of reporting information in the database. You can change this setting in **System > Advanced** and scroll to **Other Settings**. Set the number of days you want to retain report data in the appropriate field. Data is deleted when older than the number you set. Lowering this number means less disk space is used, but you do not retain report data older than the number of days specified. If your organization's email volume is very high, you may want to consider lowering this number.

This section provides information on the **MONITORING** view, including how to navigate, customize, and configure the reports.

- [Using the Reports](#)
- [Managing Table Formats](#)
- [User Statistics](#)

Using the Reports

The reports shown on the **MONITOR** view can be managed and customized in a similar way across all the options:

- [Customizing the Display](#)
- [Configuring Chart Formats](#)
- [Filtering Chart Data](#)

Customizing the Display

Several buttons are provided so you can customize what reports are shown for each of the options.

Button	Function
Add Charts	Allows you to add charts to be displayed. Click on the down arrow to select the report category, and then click on the report name you want to add.
Save View	Saves the view after you configured or made adjustments to your settings.
Reset to Default View	Resets the report view to the default settings.

Button	Function
Customize	Opens Custom Reports page so you can define the parameters for any report displayed. 1 Select the report to customize 2 Specify the date range for the report. 3 Select the units for how you want to list results: by the hour, day, week or month. 4 Enter the domains in the text field for Report shows email sent to these domains. Separate multiple domains with a comma, if left blank the report shows email sent to all domains. 5 Select delivery method. Choose Display to show data on the dashboard. Choose Email to to send the report to someone and provide the email address for the report recipient. 6 If you selected Email to, provide the following information in the text fields: • Name from which report is sent • Email address from which report is sent • Subject 7 Select Generate This Report.
Refresh Reports	Refreshes the data in the charts.

NOTE: The **Appliance Health | Live Monitor** and either of the **Current Status** options are not customizable so these buttons don't appear in those tables.

Configuring Chart Formats

Each of the charts can be moved up and down or left and right in the display. Simply drag-and-drop the chart wherever you want it. You can also customize the data displayed in the charts by using the options provided. Select the tabs across the top of a chart to set the format and contents as described below:

To set the data style:	Select the data format you want: • Some data can be presented in Stacked Chart, Line Chart, or Table form. • Some data can only be presented in Bar Chart or Table form.
To set the time style:	Select one of the following: • Hourly • Daily • Monthly
To zoom:	Use the mouse to draw a box around the segment you want to zoom in on and the display adjusts to show only that portion of the data.
To undo zoom:	Click the Undo Zoom button to reset the view in that chart to the default setting. You might have to click the right-arrow to scroll over and make the Undo Zoom button visible.
To download data:	Click the download arrow allow you to download the chart in PDF , JPEG , or CSV formats.

To minimize or open the chart:	Use the double arrow head to minimize the chart when arrows are pointing up and opens the chart when the arrows are pointing down.
To close a chart and remove it from the view:	Click the close (X) button.

Filtering Chart Data

Since some charts display several types of data in a single view, you can customize what data shows in the charts. Click on an item listed in the legend. That item becomes grayed out and the data is removed from the display. To restore that item to the chart or table, click on the grayed out item and the data is returned.

Managing Table Formats

If you choose to show a table instead of a chart, use the following options to customize how the data is displayed, sorted or filtered:

- [Customizing Data Table Formats](#)
- [Sorting](#)
- [Search Filters](#)

Customizing Data Table Formats

Most of the tables in the **MONITOR** view be customized by selecting which columns of data to show and what columns to omit.

To define the columns of data to display:

- 1 Go to any heading in a table and click on the down arrow to see the drop box.
- 2 Navigate to **Columns** to see what columns of data are available for that table.
- 3 Check the box by those columns you want to appear and uncheck the boxes you want to hide. The table reconfigures itself in response to each action.

Sorting

The columns in the data table can be sorted in sorted in ascending or descending order.

To sort a column:

- 1 Click in a the column you want to sort. A small arrowhead appears in the column. The arrowhead points up to indicate ascending order and down to indicate descending order.
- 2 Click in the column again to change the direction of the arrowhead. The data refreshes immediately to reflect the choice you made.

In the drop down menus for the column headings, you can also chose **Sort Ascending** or **Sort Descending**.

Search Filters

Search filters have been integrated into the reporting tool so you can show just part of the data. Filters can be applied to multiple columns, but not all columns have the option to be filtered. The filtering is performed directly on the data that's displayed.

To filter data in a column:

- 1 Select the down arrow next to the column title.
- 2 Highlight the **Filter** option.
- 3 Depending on the options provided, do one of the following:
 - Type in a string of text to filter on.
 - Choose one or more filters from a list of pre-populated options.

The results of any filtering are immediately shown in the data table.

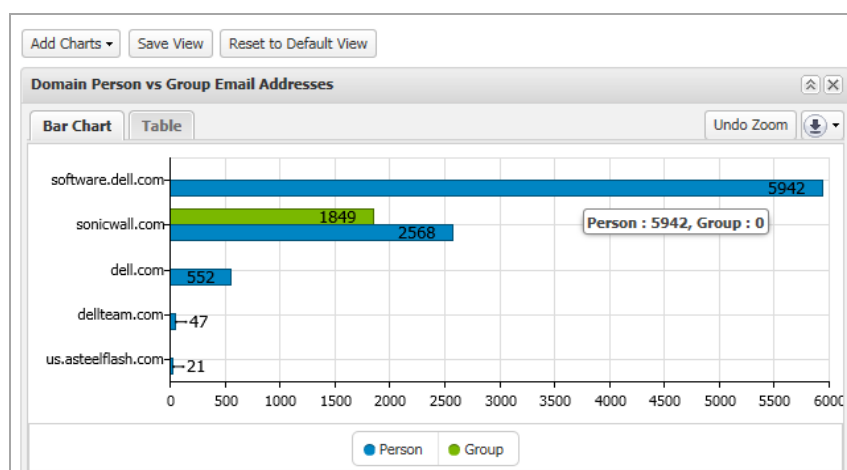
User Statistics

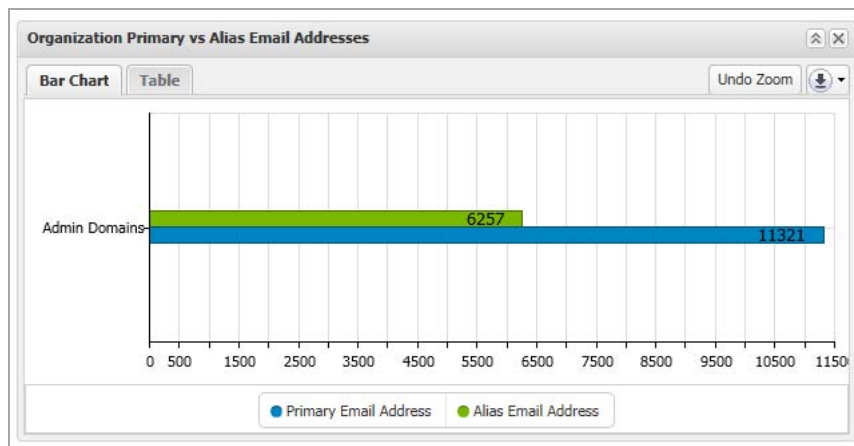
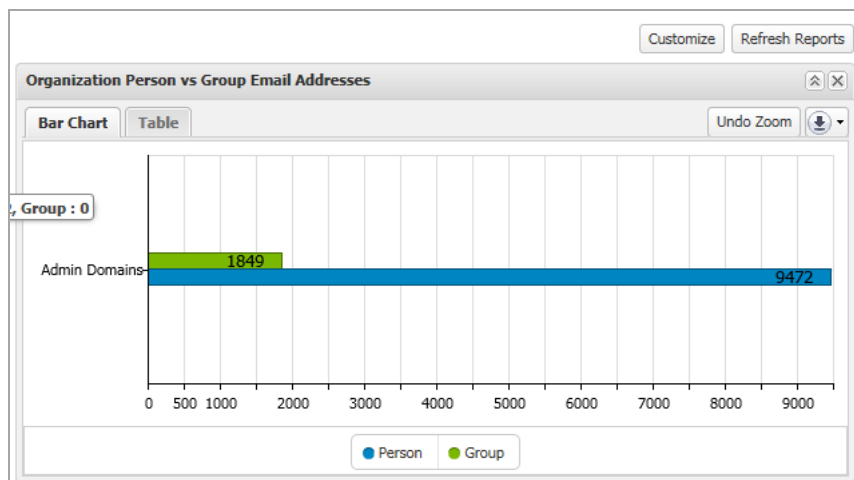
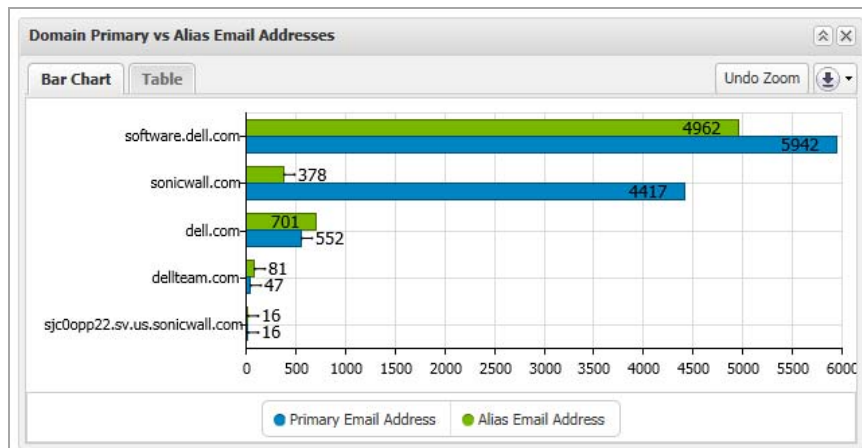
In a Managed Service Provider environment, the collection named **LDAP Users (Appliance Health | LDAP Users)** provides an overview of the amount of mail flow attributed to each currently hosted domain.

NOTE: When you first log into Email Security, the default view is the **Dashboard** on the **MONITOR** view.

The LDAP Users reports are presented as a function of the number of users per domain or organization. With it, you can determine if users are license compliant. These reports illustrate the volume of mail flow per each domain. The following reports are shown:

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





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>.

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 MSP Deployment Guide
Updated - September 2018
Software Version - 9.2
232-003466-01 Rev A

Copyright © 2018 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

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