

Email Security System Administrator's Guide



 **GOSECURE**

© 2001–2020 GoSecure. All rights reserved. The GoSecure logo is a trademark of GoSecure Inc. All other trademarks and registered trademarks are hereby acknowledged.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

The GoSecure Email Security product and its documentation are copyrighted materials. Law prohibits making unauthorized copies. No part of this software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into another language without prior permission of GoSecure.

Contents

Chapter 1 Overview	1
Overview of Services	1
Email Filtering (EMF)	1
Archive	2
Continuity	2
Encryption	3
Data Loss Protection (DLP)	3
Personal Health Information	3
Personal Financial Information	4
ThreatTest	4
Vx Service	5
Document Conventions	5
Supported Browsers	5
Reporting Spam	5
Contacting Us	6
Additional Resources	6
Chapter 2 The Email Security Appliance	7
Planning for the Appliance	7
About MX Records	7
Configuration Examples	7
Appliance Outside Corporate Firewall	7
Appliance Behind Corporate Firewall	8
Mandatory	8
Optional	9
Accessing the Email Security Appliance	9
Online Help	10
Appliance Status	10
Appliance Settings	11
Account	11
Licensing	11
Network	12
Appliance Server Configuration	12
IP Address Configuration	13
Services	14
DNS Server Configuration	14
External DNS Configuration	15
SMTP	15
Sender Allow List	16
Sender Block List	16
Bounce Suspension List	16
Greylisting	16
Country Codes	18
System	18
Appliance Server Configuration	18
System Logging Configuration	19
Time Zone Configuration	19
Appliance Branding	19

Adding a Brand	20
Joining a Brand	21
Administering the New Brand	21
Removing Brands from the Primary Server	21
Appliance Encryption	22
Viewing the Local Certificate	22
Generating and Downloading a Certificate Signing Request	23
Uploading a Local Certificate	24
Generating a Self-Signed Certificate	24
Uploading an External Certificate and Key	25
Viewing Trusted Certificates	25
Adding Trusted Certificates	26
Removing a Trusted Certificate	26
Configuring Appliance Encryption Policies	26
Appliance Troubleshooting	27
Logs	27
Diagnostics	28
Statistics	29
Restarting the Appliance	29
Chapter 3 The Administrator Dashboard	31
Using the Administrator Dashboard	31
Customizing the Dashboard Tiles	32
Using OmniSearch	32
Changing Your Password	33
Chapter 4 Accounts	34
Best Practices	34
Configuring with Other Spam Filter Clients	34
Whitelists and Blacklists	34
Quick Start	34
Adding an Account	35
Managing Account Information	35
Managing Administrators	36
Account Administrators	36
System Administrators	37
Chapter 5 Groups	38
Adding a Group	38
Managing Group Information	38
Chapter 6 Domains	40
Adding a Domain	40
Default Domain Settings	40
Domain Settings	41
Domain Group Options	41
Domain Digest Options	41
Personal Dashboard Options	43
Filtering Options	45
Filtering Categories	46
Attachments	47
Spoof Options	48

Protecting Against Internal Domain Spoofing	48
Sender Policy Framework Options	49
DKIM Options	49
DMARC Options	50
Display Name Spoofing Option	50
Filter by Sender	50
Filter Exceptions	52
Delivery Status Notification	52
Message Annotation	52
Mailbox Discovery	53
Authentication	54
Unrecognized Recipient Handling	56
Directory Harvest Attack Protection	56
Alias Handling	57
Mail Gateways	57
Boundary Encryption	58
Test Connection	58
Routing and Session Management	58
Email Continuity	59
Anti Virus Engines	61
Moving Domains Between Accounts	61
Deleting a Domain	61
Viewing Domain Status	62
Bulk Email Filtering	62
Email Continuity	63
Configuration	63
Reporting	63
Chapter 7 Outbound IP Addresses	64
Adding an Outbound IP Address	64
Outbound Authenticated Relay Settings	64
Outbound IP Settings	65
Member Domains	65
Outbound Filtering	66
Outbound Filtering Options	66
Outbound Filtering Categories	68
Filter By Sender	69
Filter Exceptions	70
Delivery Status Notification	70
Rate Limits	72
Message Annotation	73
Encryption	74
Configuring the Encryption Service	76
Delivery Options	76
Email Message View Options	77
Attach Encrypted Options	77
Notification Message Options	78
Routing and Session Management	78
Domain-Specific Delivery Exceptions	79
Authentication	81

Special Routing	81
Encryption Service	82
Custom Routing	82
Anti Virus Engines	83
Nicknaming an Outbound IP	83
Viewing Outbound IP Status	83
Moving Outbound IPs Between Accounts	84
Chapter 8 Mailboxes	85
Adding a Mailbox	85
Configuring Individual Mailboxes	86
General Settings	86
Change Login Password	86
Digest Options	87
Personal Dashboard Options	88
Filtering Options	89
SpooF Options	90
Filter by Sender	91
Authentication	92
Outbound Mail Options	92
Mailbox Aliases	93
Creating Mailbox Aliases	93
Autodiscovering Aliases	94
Reversing Autodiscovered Alias Relationships	94
Accessing the Personal Dashboard	95
Unprotecting a Mailbox	95
Deactivating a Mailbox	95
Deleting Mailboxes	96
Chapter 9 Verifiers	97
Adding a Verifier	98
LDAP Verifier	99
VRFY Verifier	101
RCPT TO Verifier	102
CommuniGate CLI Verifier	102
POP - Authentication Only Verifier	103
Database Verifier	103
Static Verifier	104
Composite Verifier	104
Custom Verifier	105
Microsoft/Office365 Verifier	105
G-Suite Verifier	106
Testing the Verifier Connection	106
Modifying Verifiers	107
Deleting a Verifier	107
When Verification Servers Fail	107
Chapter 10 Content Filters	108
Creating a Content Filter	108
Modifying a Content Filter	110
Adding a Content Filter to a Domain or Outbound IP	111
POSIX Regular Expression Syntax	111

Chapter 11 Notifications	114
Adding a Notification	115
Units of Measurement	118
Editing a Notification	118
Chapter 12 Bulk Operations	120
Bulk Domain Settings	120
Bulk Outbound Settings	120
Bulk Mailbox Settings	121
Chapter 13 Reporting	122
Running a Report	122
Sorting Report Data	122
Releasing Messages	123
Downloading Report Data	123
Subscribing to a Report	124
Reports	124
Charts	125
Post-Run Options	126
Advanced Report	126
Delivered Message Report	127
Deferred Queue Report	128
Deferred Queue Summary	128
Instant Spam Digest	128
Message Category Summary	128
Message Handling Summary	129
Quarantine Report	129
DLP Activity Report	129
Top Senders Report	130
Encrypted Attachment Report	130
Audit Trail	130
Mailbox Report	131
ThreatTest Report	131
ThreatTest Summary Charts	131
Chapter 14 Brand Preferences	133
Personal Dashboard Preferences	133
General Settings	133
Policies Tab	134
Inbound and Outbound Preview Message Page	134
Administrator Dashboard Preferences	134
Branding Preferences	135
Dashboard Logos	135
Dashboard Content	136
Spam Digest Settings	137
Authentication	138
Account Preferences	139
Account Branding	139
Spam Digest Settings	140
Appendix A GoSecure Message Headers	141
X-MAG-Category Descriptions	141

This document is a general guide for planning, configuring, and operating the GoSecure Email Security appliance and hosted systems. It describes the features and applications of the system, and assists administrators in effectively deploying the product in their environment.

Overview of Services

The GoSecure Email Security product delivers next-generation services that protect your business with comprehensive end-to-end solutions. The email security services defend against internal and external threats, assure continuous mail stream flow, protect against data loss, and help fulfill regulatory compliance requirements, while assuring fast, accurate delivery of business-critical email.

GoSecure takes the complexity out of operating its products and removes the administrative burden from email security. The platform is simple and easy to use. The Email Security product provides two primary services:

- **Hosted:** With the hosted solution, you do not install any client software, modify servers, or train staff. You enjoy lower bandwidth costs, lower mail server utilization, and lower archival capacity demands.
- **Appliance:** The Email Security product offers a full family of appliances that leverages the resources of the GoSecure Security Operations Center to provide redundancy and managed service.

Email Filtering (EMF)

The Email Security product provides email defense against internal and external threats such as spam, viruses, spyware, phishing schemes, identity theft, and other dangerous or offensive content. Services include inbound/outbound spam and antivirus filtering, policy categorization, and automated seamless directory integration. GoSecure technical experts provide proactive monitoring and management designed to stop threats before they get near your internal servers.

- **Both Inbound and Outbound Protection:** Protecting outbound email is critical to preventing dangerous botnet attacks that can turn infected computers into zombie networks. Our award-winning filtering offers protection from spam, viruses, and criminal malware on both inbound and outbound mail streams. The Email Security product's kernel technology is a proprietary message defense system that eliminates spam, viruses, spyware, phishing schemes, and offensive content. It also stops Directory Harvest Attacks (DHA) and Distributed Denial of Service (DDoS) attacks.
- **No-Touch Email Security:** GoSecure hosts the applications and infrastructure required to protect your organization in a fully managed solution requiring zero administration.
- **Disaster recovery protection:** GoSecure Email Security spools all email for up to 320 hours, in case of unexpected events, so you never lose your business-critical email.
- **Proactive monitoring:** GoSecure engineers continually monitor email processes to assure they are performing at peak efficiency.

- **Zero Minute Defense:** As soon as an emerging threat is identified, GoSecure engineers deploy a specific rule to block it.
- **TLS Encryption:** This feature establishes private email networks linking you with your business-critical partners via the use of certificates. Every email sent or received by these networks is fully and securely encrypted while the encryption remains completely transparent to both sender and recipient.
- **Technical Support -** GoSecure's Security Operations Center (SOC) is staffed around the clock with email experts and security specialists for 24/7/365 support. They provide proactive monitoring of any email threats to assure continuous service for all of your domains and users.
- The service offers the option of a Spam Digest for mailbox holders. The Spam Digest is an emailed version of a quarantine report that enables users to review blocked spam messages and release them to their email inbox.

The Email Security product's behavior-based perimeter defense system uses real-time awareness of spam campaigns to implement a merit-based response while providing defenses at each step of the SMTP connection and session layer. GoSecure does not rely on IP Real-time Blackhole Lists (RBLs) to defend against spammers, and uses a variety of patent-pending techniques to deal with spam and attacks originating from botnets. The product employs a combination of techniques to protect email domains and to filter spam email that does not conform to the common techniques used within the industry. Key differentiators of the Email Security product are:

- A managed appliance solution or a hosted solution, to meet your organization's specific needs
- Industry-leading block rate without any IT staff maintenance
- Dynamic resource allocation and service redundancy

Archive

The Email Security product offers secure email archiving that is scalable to fit the requirements of any size organization. This archiving retains your email in an unalterable state to help you meet requirements for regulatory compliance, litigation issues, and storage management needs or to fulfill business best practices guidelines. The Archiving Services are in-the-cloud, so scalability is assured. And GoSecure's secure data collection technology provides comprehensive interoperability with all email systems.

Continuity

The Continuity service enables continuous web-based email access, management, and use during planned or unplanned mail server outages. Continuity is enabled via a simple admin checkbox, giving your users access to their mail so that they can manage messaging and avoid any disruption in the flow of critical, legitimate business communications. In case of an outage, end users access the Web 2.0 email client allowing them to manage their email and perform the following tasks:

- Know that any sent messages in limbo as a result of an outage will not be lost because they are Bcc'd and will be delivered when the mail server is back online. Rules on the mail server can be implemented to take those messages and divert them to the users' Sent Mail folders to complete the activity synchronization.
- Read, compose, reply to, forward and delete messages.
- Upload and download attachments.
- Perform full text searches of all the messages in their mailboxes.

For more information on configuring Email Continuity, see [Email Continuity](#). For details on setting up a domain with Email Continuity, see [Routing and Session Management](#).

Encryption

Encryption services assure the secure delivery of your email in accordance with your organization's Security Policy, and provide confirmation of message delivery. Comprehensive reporting offers message tracking and an audit trail to support regulatory and other requirements.

For more information on configuring Encryption, see [Special Routing and Encryption](#). For details on how messages are routed, see [Outbound Filtering Options](#).

Data Loss Protection (DLP)

DLP, also referred to as Email Data Compliance, is a content analysis and policy engine that uses proprietary technology to protect private information transmitted via outgoing email. This data protection technology analyzes information being sent out of your network to detect private content in data in motion and prevent sensitive and confidential data from leaving your network. The Email Security's DLP gives you the powerful tools you need to comply with government regulations, such as HIPAA and GLBA, and prevents the outbound communication of all types of sensitive or objectionable material, including:

- Patient healthcare information
- Financial information
- Social Security numbers
- Credit Card numbers
- Profanity

Personal Health Information

Personal health information includes both health terms and personal identifying information. Both must be present in an email to produce a match.

Health terms include words and phrases such as:

- fractures
- cat scan
- convulsions
- aggressive fibromatosis
- ocular refraction

Health personal identifiers include words or phrases such as:

- Social Security Number or SSN followed by a valid Social Security number
- Date of Birth, DOB, Birth Date, etc., followed by a date in any of several formats
- Patient followed by an ID (alphanumeric first character followed by five or more digits)
- Account, Member, Record, etc., followed by a number

Examples

Match	Date of Birth 10/02/74 and the word fractures both detected in the file. The word convulsions and the phrase Patient D832915 both detected in the file.
No match	Date of Birth 10/2/74 with no health terms detected in the file. The word convulsions with no personal identifiers detected in the file.

Personal Financial Information

Personal financial information includes both financial terms and personal identifying information. Both must be present in an email to produce a match.

Financial terms include words and phrases such as:

- Account balance
- ATM
- Direct Deposit
- Mortgage Loan
- Routing Number

Financial personal identifiers include words or phrases such as:

- Social Security Number or SSN followed by a valid number
- Account, Loan, Customer, Certificate, etc., followed by a name or number

Examples

Match	Date of Birth 10/02/74 and the word routing number both detected in the file. SSN 480-80-0058 and the phrase account balance both detected in the file. The word ATM and the phrase Customer A35521 both detected in the file.
No Match	The phrase account balance with no personal identifiers detected in the file. The phrase Customer John Doe with no financial terms detected in the file.

For more information on configuring DLP, see [Outbound Filtering Categories](#).

ThreatTest

ThreatTest is a service that enables advanced real-time detection and prevention of Phishing, Ransomware, and other malicious email-based threats. Suspect messages are sent for analysis to GoSecure's Hybrid Threat Detection Center, which combines iGuard URL analysis, email threat detection, and advanced anti-Phishing technology. ThreatTest analyzes and removes malicious messages, alerting end users on message status with reports and notifications.

Vx Service

The Vx service provides network-based overload and failover protection for the onsite Email Security appliance(s). If the Vx service is processing 20% or more of the appliance(s) capacity for greater than 15 days in a calendar month, this is considered excessive use of the service, and the customer must purchase additional onsite appliance capacity to accommodate the traffic load.

For appliances, during a complete outage of the local appliance (due to factors such as a network or power outage), email continues to flow uninterrupted if your mail exchanger is still online and the Vx service is licensed. The appliance management console is unavailable during the outage. For an extended period outage, contact GoSecure Technical Support to arrange for access to the administrative console.

The quarantine information stored on the local hard disk of the appliance is inaccessible during the outage. New quarantine is stored in the Vx network and is accessible both during the outage and after the outage.

Document Conventions

Bold text denotes any of the following:

- Names of screen elements such as buttons and menu options
- Names of screen fields such as text boxes, drop-down lists, and radio buttons
- Names of other visible screen components
- Other important concepts

Navigation

Navigation begins with the menus at the top of the screen.

Braces { } indicate a choice from a list. Depending on the screen, you may have to use **OmniSearch** to generate the list inside the braces.

In the example below, select the **Manage** menu, choose **Mailboxes**, then select a mailbox from the list.

Manage >> Mailboxes >> {Mailbox}

Supported Browsers

The Email Security product supports the following Web browsers:

- Microsoft Internet Explorer version 11 and Microsoft Edge
- Mozilla Firefox version 67
- Safari version 12
- Google Chrome version 74

Reporting Spam

Report any spam messages that have passed through the GoSecure system to spam@edgewave.com. Include the spam message as an attachment to your email.

Contacting Us

If you have any questions, you can contact GoSecure Technical Support:

- Phone: 1-800-782-3762
- Web form: http://www.edgewave.com/forms/support/email_security.asp

For GoSecure sales or general inquiries, call 1-855-881-2004.

Additional Resources

The [product website](#) provides the latest available documentation for the Email Security product.

This section describes how to plan for the installation of the Email Security appliance at your location, gives configuration examples, describes the appliance dashboard configuration and administration screens, and shows how to configure the appliance branding feature.

Planning for the Appliance

For the Email Security appliance installed at the customer location, block all incoming TCP and UDP connections to the mail server that the appliance is defending, other than the IP address range and ports specified in the email that you will receive from the GoSecure installation support staff.

About MX Records

The MX record is a type of resource record in the Domain Name System (DNS) specifying how Internet email should be routed. Properly configured MX records point to the Email Security product servers that receive incoming email, and list their priority relative to each other. When configured correctly for use with the Email Security product, your MX record should resemble the following:

```
yourdomain.net. 3600 IN MX 10 yourdomain.net.mx1.mybrand.rcimx.net.
yourdomain.net. 3600 IN MX 20 yourdomain.net.mx2.mybrand.rcimx.net.
yourdomain.net. 3600 IN MX 30 yourdomain.net.mx3.mybrand.rcimx.net.
yourdomain.net. 3600 IN MX 40 yourdomain.net.mx4.mybrand.rcimx.net.
```

Configuration Examples

Appliance Outside Corporate Firewall

The following illustration shows a typical configuration with the Email Security appliance outside the corporate firewall.

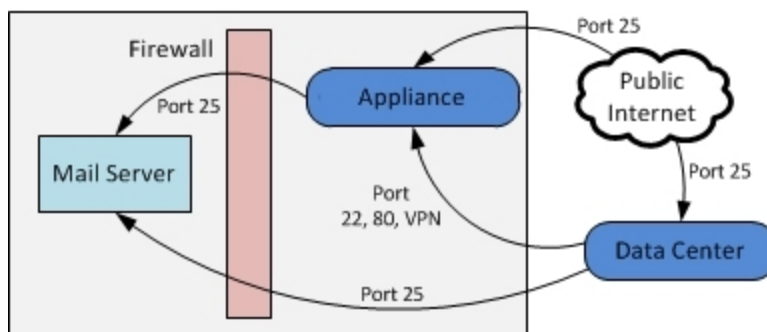


Figure 1. Typical configuration with appliance outside corporate firewall

Appliance Behind Corporate Firewall

The following illustration shows a typical configuration with the Email Security appliance inside the corporate firewall.



Note: GoSecure recommends that you do not configure the appliance for use with a Network Address Translation (NAT) device.

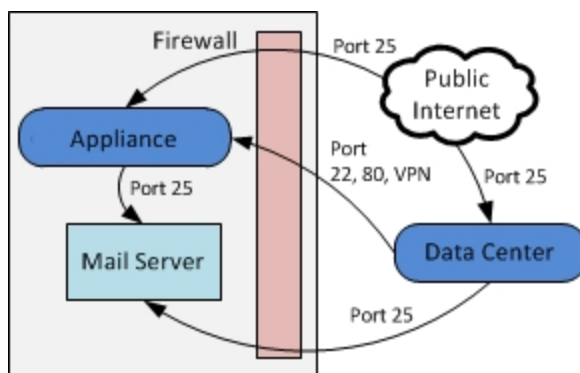


Figure 2. Typical configuration with appliance inside corporate firewall

The following tables show the firewall access required and optional TCP and UDP ports for the Email Security appliance inside the firewall.

Mandatory

Port	Protocol	Direction	Description
N/A	ICMP echo request/reply		
22	TCP/SSH	Inbound	Remote diagnostics and technical support
25	TCP/SMTP	Both	SMTP server
53	TCP/UDP/DNS	Both	Domain Name Server (DNS)
80	TCP/HTTP	Both	Dashboard and other services
123	UDP/NTP	Outbound	Network Time Protocol (NTP)
443	TCP/UDP/HTTPS	Both	Secure Web access
1194	UDP/Application	Both	Internal GoSecure Use

Optional

Port	Protocol	Direction	Description
366	TCP/ODMR	Inbound	On Demand Mail Relay
389	TCP/LDAP	Inbound	Lightweight Directory Access Protocol (LDAP)
587	TCP/SMTP	Inbound	Alternate SMTP server
636	TCP/LDAPS	Inbound	Secure LDAP



Note: All outbound TCP and UDP ports must be allowed.

After traffic is cut over to the appliance, GoSecure recommends that a firewall rule or Access Control List (ACL) be configured such that the incoming TCP/IP port 25 traffic only be accepted from the appliance IP address and the GoSecure data center IP address ranges. All other IP addresses should be blocked to prevent back-door spam campaigns.



Note: Although there are extra NICs in the appliance the use of multiple interfaces on the same subnet is not supported.

Accessing the Email Security Appliance

The Email Security appliance dashboard is used for maintaining system wide settings for your server. You can add a new brand, or join an existing brand, and manage your settings.

To access the appliance dashboard:

1. Enter one of the following addresses into your browser:

`http://<IP Address>/mag`

or

`http://<hostname>/mag`

where <hostname> is the name defined in DNS.

2. The appliance dashboard login page opens. Type your username and password and click **Login**.

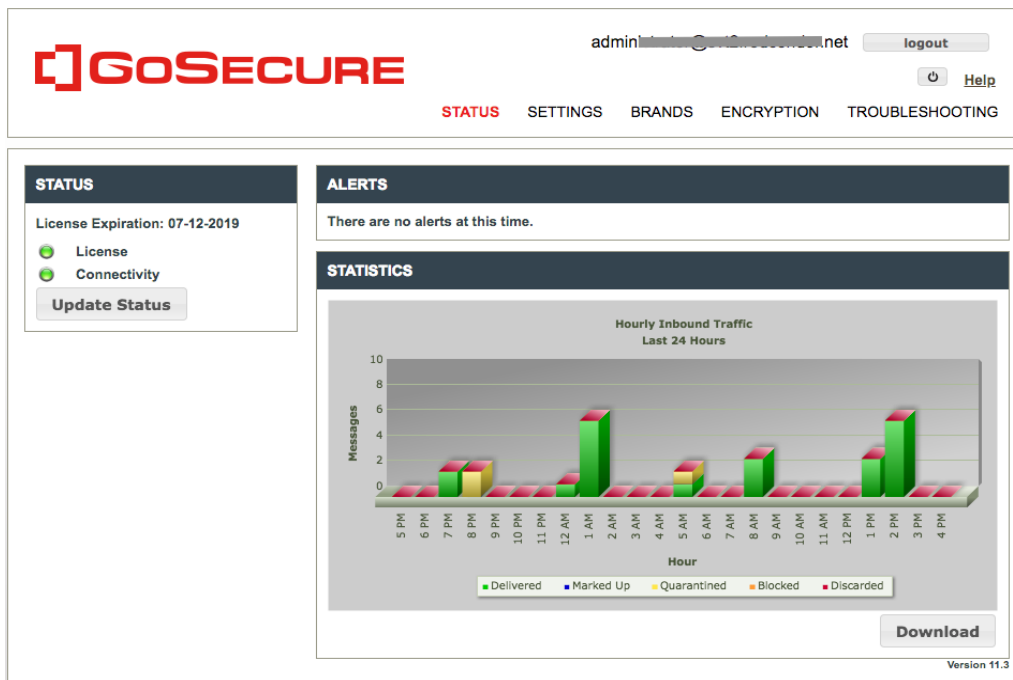


Figure 3. Appliance Dashboard

Online Help

The Email Security appliance dashboard contains a link to an online version of this guide. Click **Help** near the top right of any dashboard screen to display this guide in a browser window. For your convenience, it opens to the appliance section.

Appliance Status

The Status tab is the home page of the Email Security appliance. It displays the current status of your appliance license and connectivity, both network-wide and appliance local alerts, and a chart of the previous 24 hours of message traffic color-coded by classification.

- Click **Update Status** to view the current connectivity and license status, and update the Alerts list.
- Click the **System Alert** link to display information about an alert.

License and connectivity buttons are color-coded to display appliance status.

Button	Color	Meaning
License	Green	The license is valid for at least the next 30 days.
	Yellow	The license will expire within 30 days.
	Red	The license is expired.
Connectivity	Green	All connectivity tests passed.

	Yellow	A non-fatal error occurred during testing. The error displays in the Alerts section.
	Red	One or more connectivity tests failed. The error displays in the Alerts section.

The license expiration date is shown in the Status section.

You can hover the mouse over the connectivity button to see a description of the status.

Click **Download** below the status graphic to save a .csv file of the 24-hour traffic statistics to your local or network drive.

Appliance Settings

Use the Appliance Settings tabs to configure and manage the account, licensing, network, SMTP, and system logging preferences of your appliance.

Account

To update the account configuration settings of your appliance:

Settings >> Account

1. Update your contact information or change your password.
2. Click **Update**.

Figure 4. Account Settings

Licensing

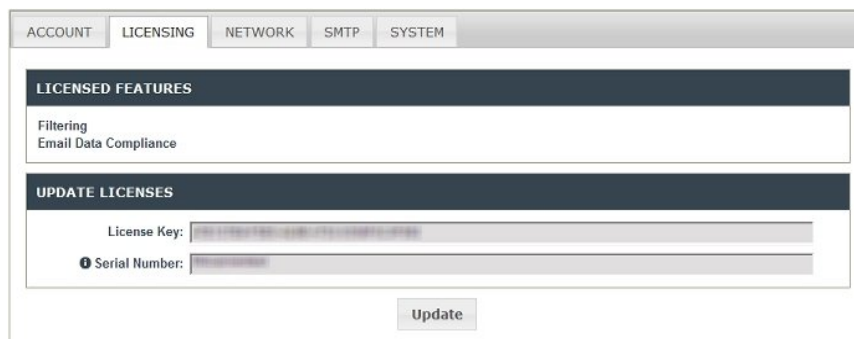
The Licensed Features section lists the additional features that have current licenses.

To update the licensing settings of your appliance:

Settings >> Licensing

1. Enter your license key and appliance serial number to update your license after it has been renewed.

2. Click **Update**.



The screenshot shows a web interface with a navigation bar at the top containing tabs for ACCOUNT, LICENSING, NETWORK, SMTP, and SYSTEM. The LICENSING tab is active. Below the navigation bar, there are two main sections. The first section, titled 'LICENSED FEATURES', lists 'Filtering' and 'Email Data Compliance'. The second section, titled 'UPDATE LICENSES', contains two input fields: 'License Key:' and 'Serial Number:'. Both fields have placeholder text. Below these fields is an 'Update' button.

Figure 5. Licensing

Network

Use the network settings to:

- Configure all of the NICs on the server
- Assign multiple IPs to a network interface
- Set up load balancing
- Configure DNS servers
- Configure the services on each IP

To update the network settings of your appliance:

Settings >> Network

Appliance Server Configuration

1. Enter the host name. This name is used in the following areas:
 - Client HELO string
 - Notification sender
 - Certificate Signing Request
 - SMTP greeting default
2. Set the default gateway IP address.
3. Click **Update**.



Note: The session terminates if you modify the IP address or netmask of the physical resource to which you are connected, or if you modify the gateway. You will need to log in to the dashboard with the new IP address until the DNS is updated.

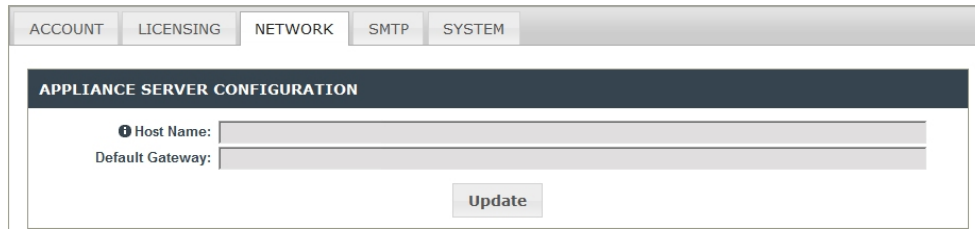


Figure 6. Network settings: Appliance server configuration

IP Address Configuration

Use the IP Address Configuration section to set up additional network interfaces, IPs, and load balancing for your appliance.

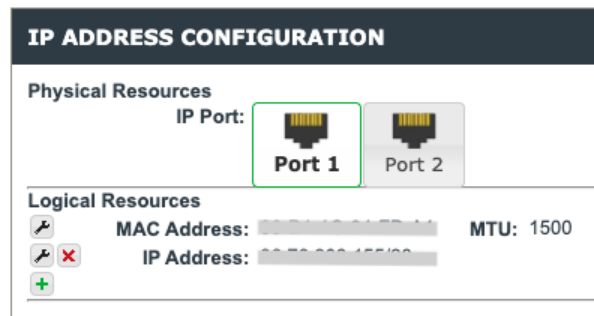


Figure 7. Network settings: IP address configuration

To add an IP address:

1. Click on the physical resource.



Note: Port 1 is for initial setup only, it is not accessible for configuration here.

2. Click the + icon.
3. Enter the IP address and netmask using CIDR format.
4. Click OK.

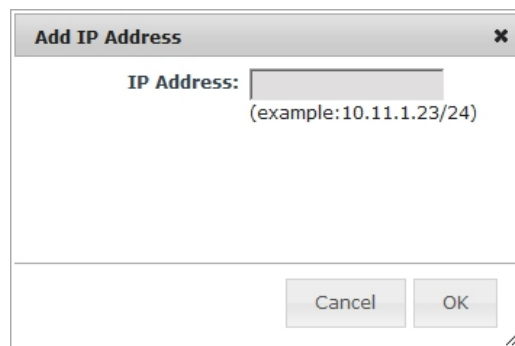


Figure 8. Network settings: Add IP address

Services

Use the Services section to specify the type of traffic to be filtered on an IP. One IP address can have multiple services assigned to it as long as they run on different ports.

SERVICES				
Enabled	Service	IP	Port	SMTP Greeting
<input checked="" type="checkbox"/>	SMTP Out		25	PhishNet SVT Relay Host
<input checked="" type="checkbox"/>	SMTP In/Out		25	smtp10.redcondor.net ESMTP EdgeWave mag3000
+ <input type="checkbox"/>				

Figure 9. Network settings: Services

To add a service:

1. Click the + icon.
2. Select the service.
3. Select the IP address.
4. Enter the port and SMTP greeting.
5. Click OK.

Add Service ✕

Enabled:

Service: SMTP In/Out ▼

IP Address: 208.80.201.14 ▼

Port: 25

SMTP Greeting:

Figure 10. Network settings: Add service

DNS Server Configuration

This section sets up the appliance to point DNS lookups to a designated server.

DNS SERVER CONFIGURATION

To specify the DNS server to be used by the appliance enter the zone and the address of the DNS server that serves it.

+ Add a Zone:

	Zone	Servers
<input checked="" type="checkbox"/>	.	208.67.222.222

Figure 11. Network settings: DNS server configuration

To add DNS servers:

1. Enter the zone name.

- You can enter "." (no quotes) as the zone, to override all other entries, forcing all DNS lookups to point to the designated server.
 - If you use a zone of the format xxx.yyy, the DNS lookups for this zone will point to the designated server.
2. Click the + icon.
 3. Enter the IP addresses of the DNS servers.
 4. Click OK.

External DNS Configuration

Use this section to set up the system to manage DNS MX records for inbound or outbound email, and the A record for the dashboards.

1. Enter the external IP address in the appropriate box.
2. Select the corresponding checkbox.



Note: For staging of the setup, you can enter the address first and mark the checkbox to enable each option later.

Figure 12. Network settings: External DNS configuration

SMTP

Use the SMTP settings to allow or block specific senders at the SMTP session level, manage greylisting, and control message bouncing.

Settings >> SMTP

1. Set up each list as applicable.
2. Click **Update**.

Figure 13. Connection and session level settings

Sender Allow List

To add a sender to the Sender Allow list, enter their IP address, CIDR address, or country code. Incoming connections from senders in the Allow list are accepted and then filtered for spam and viruses. CIDR and Country Code only override Greylisting. Each entry must appear on its own line.

Sender Block List

To add a sender to the Sender Block list, enter their IP address, CIDR address, or country code. Connections from senders on the blocked list are rejected.

Bounce Suspension List

Use the Bounce Suspension list to define destination domains that will not receive a DSN message when mail is rejected.

Use the following optional parameters after the domain name to define address resolution:

- :MX to use the address defined by the MX record in DNS
- :AAAA to use the IPV6 address for the domain
- :A to use the DNS A record for the domain

For example, anydomain.com:AAAA.

Greylisting

Greylisting is used to temporarily reject undesirable senders via simple SMTP protocol checks. Select a predefined level based on risk as shown in Step 2 below, or choose **Custom** to specify which tests to run.

1. To enable greylisting, select the **Enabled** checkbox in the Greylisting section.
2. Select the level:
 - Custom

- Low (default)
- Medium
- High

3. If Custom is chosen, choose the settings from the following list:

Type	Explanation
HELO Checks	
DNS (helo.fdns)	The forward and reverse DNS entries for the announced domain in the HELO/EHLO match.
RDNS (helo.rdns)	The announced domain in the HELO/EHLO command must have valid reverse DNS entries.
Syntax (helo.name)	The announced domain in the HELO/EHLO command must contain a dot.
TLD (helo.tld)	The announced domain in the HELO/EHLO command must contain a known TLD.
IP (helo.ip)	The announced domain in the HELO/EHLO command must match the connecting IP.
Mail From Checks	
DNS (mail.fdns)	The sender in a MAIL FROM: command must exist in DNS.
TLD (mail.tld)	The sender in a MAIL FROM: command must contain a known TLD.
Syntax (mail.name)	The sender in a MAIL FROM: command must contain a dot.
Header Checks (Inbound)	
Empty Header	A valid inbound message must contain information in the header.
Illegal Field	A valid inbound message cannot contain an illegal field.
Incorrect Termination	Mail header cannot contain an incorrect termination.
Header Checks (Outbound)	
Empty Headers	A valid outbound message must contain information in the header.
Illegal Field	A valid outbound message cannot contain an illegal field.
Incorrect Termination	Mail header cannot contain an incorrect termination

Country Codes

You can choose to accept mail from specific country codes using the Country Codes checkbox and list.

1. To filter by country, select the **Enabled** checkbox in the Country Codes section.

When this box is checked, the Email Security product will filter out all country codes except for those listed in the text box below the checkbox. You can edit the contents of the checkbox to add or remove country codes. For example, you can list US, CA, and MX to accept mail from the United States, Canada, and Mexico.



Note: Country codes must conform to the ISO 3166 Alpha-2 standard.

System

The System tab allows you to enable system logging, select the time zone of the appliance, set the appliance name, and control access to the administrator and appliance dashboards.



Note: Be sure to set the appliance time zone before creating a brand. During brand creation the brand time zone is set to the appliance time zone.

Settings >> System

Appliance Server Configuration

1. Update the appliance name. The appliance name identifies the appliance in reporting, logging and monitoring.

Figure 14. Appliance server configuration

2. In the Dashboard access control IP list, enter IP addresses that are allowed to access the administrator and appliance dashboards. If this list is empty, access to these dashboards is limited only by login, and can come from any IP address.



Note: For automatic mailbox discovery to function correctly the IP addresses of all servers in your cluster must be included in the access control list.

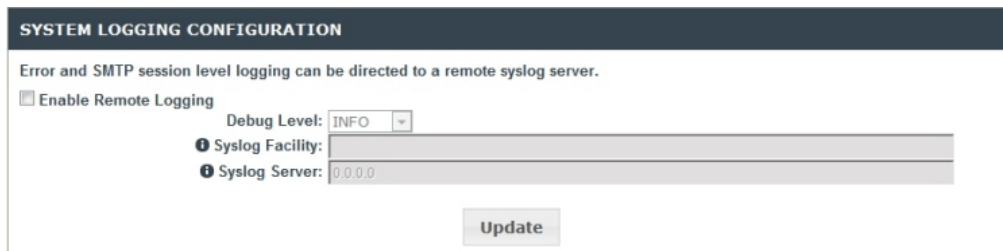
3. Click **Update**.
4. Click **Reboot Required** at the top of the page.



Note: You must reboot the appliance after clicking **Update**.

System Logging Configuration

1. In the **System Logging Configuration** section, enable remote logging and set the destination server.
2. Click **Update**.

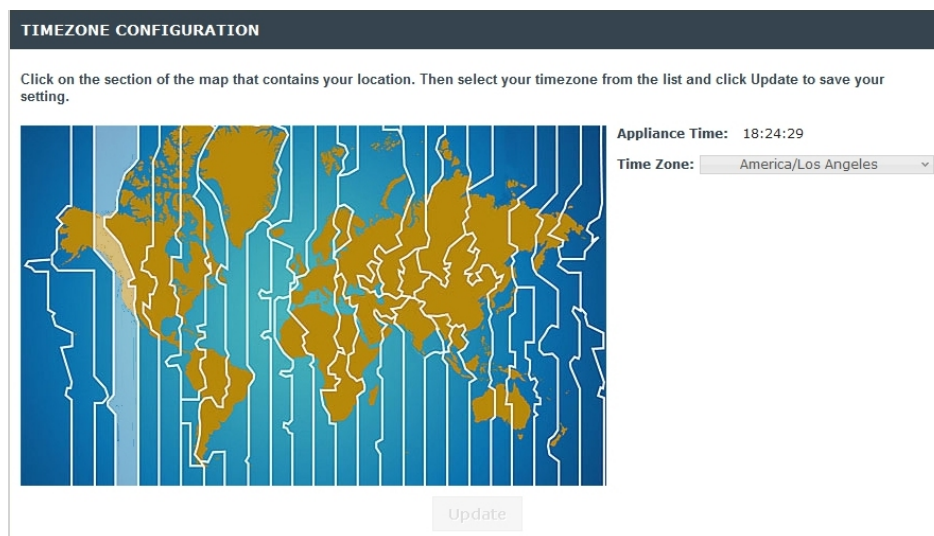


The screenshot shows the 'SYSTEM LOGGING CONFIGURATION' interface. At the top, it states: 'Error and SMTP session level logging can be directed to a remote syslog server.' Below this, there is a checkbox for 'Enable Remote Logging' which is checked. To the right of the checkbox is a 'Debug Level' dropdown menu set to 'INFO'. Below these are two input fields: 'Syslog Facility' and 'Syslog Server', both containing the value '0.0.0.0'. An 'Update' button is located at the bottom center of the configuration area.

Figure 15. System logging configuration

Time Zone Configuration

1. In the Time Zone Configuration section, click on the section of the map that contains your location.
2. Select your time zone from the drop-down list.
3. Click **Update** to save your settings.



The screenshot shows the 'TIMEZONE CONFIGURATION' interface. At the top, it states: 'Click on the section of the map that contains your location. Then select your timezone from the list and click Update to save your setting.' Below this is a world map with vertical lines representing time zones. To the right of the map, there is an 'Appliance Time' field showing '18:24:29' and a 'Time Zone' dropdown menu set to 'America/Los Angeles'. An 'Update' button is located at the bottom center of the configuration area.

Figure 16. System Time Zone Configuration

Appliance Branding

Branding allows you to set up the Email Security appliance to show your company's dashboard and logo. You can set up multiple brands, with each brand containing a group of accounts.



Note: Make sure the correct appliance time zone has been configured before adding a brand.

Brand settings apply to all dashboards, accounts, domains, and mailboxes within the brand. The brand name is used as the base name of the website for the dashboard. Once a brand name is defined, it cannot be changed.

After one or more brands have been added, the appliance can be set up to relay mail and/or to be the dashboard for a brand.

Adding a Brand

When you add a brand, the Email Security appliance runs the dashboard service and relays mail for the brand. The dashboard service supports all aspects of the user interface including the three dashboards, digest delivery and notifications.

To add a new brand:

Brands >> Operations >> Add Brand

DASHBOARD SERVICE BRANDS MAIL RELAY BRANDS OPERATIONS

A brand has its own dashboard URL and logo and contains a group of accounts.

Add Brand Filter Mail For Brand Backup Dashboard Server

A brand contains one or more accounts.

BRAND IDENTIFICATION

Name:

URL:

SYSTEM ADMINISTRATOR SETTINGS

Email:

Password:

Confirm:

SPAM DIGEST SETTINGS

Customize the end user email notification that contains the list of quarantined messages. [Help](#)

Digest Sender address:

Technical Support address:

Important Note:
If you are using Edgewave's Vx service, new Brands are not automatically added to Vx. Please contact Customer Service at wavesupport@edgewave.com or 1-877-355-0553.

Save

Figure 17. Adding a Brand

1. Enter the Brand Identification settings:

- **Name:** Name of your brand.



Note: The Name must be a single word. It can contain alphanumeric characters or '-' and it is not case-sensitive.

- **URL:** Internet address of the brand's Personal and Administrator Dashboards.

2. Enter the System Administrator settings:

- **Email:** Email address of the System Administrator.
- **Password/Confirm:** System Administrator password.

3. Enter the Spam Digest settings:

- **Digest Sender address:** Replies to the Spam Digest are sent to this address.

- **Technical Support address:** The contact address for technical assistance listed in the Spam Digest and other notifications.

4. Click **Save**.

Joining a Brand

When you join an existing brand, your Email Security appliance is set up to relay mail for all mailboxes in the brand. It retrieves its branding information from a properly in-service Email Security appliance that is running the dashboard service.

To join the server to a brand for mail filtering:

Brands >> Operations >> Filter Mail for Brand

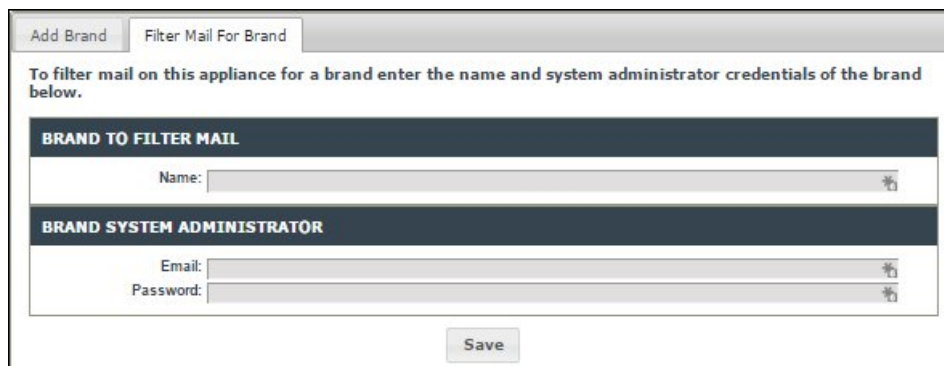


Figure 18. Filtering Mail for a Brand

1. Enter the brand name for which you want to filter mail on this appliance.
2. Enter the system administrator email address and password for the brand.
3. Click **Save**.

Administering the New Brand

To access your brand:

Brands >> Dashboard Service Brands

1. Click the name of your new brand.

The Email Security Administrator Dashboard login screen opens.

2. Log in to administer the brand, including managing your accounts, domains and mailboxes.

Removing Brands from the Primary Server

If you no longer want a specific Email Security appliance to run the dashboard service for a brand, or to relay mail for a brand, you can remove the brand from that appliance .

If you have designated a backup server for the brand, you must manually remove the brand from the backup server as well. This does not happen automatically.

Brands >> Dashboard Service Brands

This section lists the brands for which this appliance runs the dashboard service.

- To remove a brand from the list, select the checkbox and click **Remove Brands**.

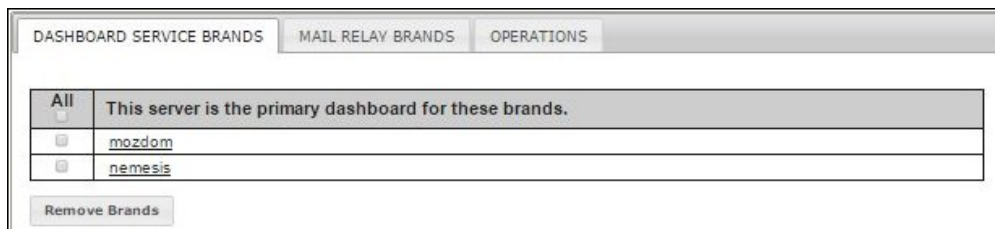


Figure 19. Dashboard Service Brands

Brands >> Mail Relay Brands

This section lists the brands for which this appliance relays mail.

- To remove a brand from the list, select the checkbox and click **Remove Brands**.



Figure 20. Mail Relay Brands

Appliance Encryption

The Email Security appliance supports encryption for both the SMTP and HTTP protocols. You can configure inbound SMTP encryption, secure access to all dashboards, and manage certificates.

The appliance ships with a self-signed certificate. You can view this certificate and all other certificates on the appliance. In addition, you can generate a Certificate Signing Request (CSR) and upload the certificate generated by it to the appliance from a local network drive, generate a new self-signed certificate, or upload a trusted certificate.

Viewing the Local Certificate

The Local Certificate tab displays the common name, issuer, issued to, and expiration date of the local certificate on the appliance. The expiration date of an invalid certificate displays in red type. On this page you can generate a CSR or self signed certificate, or upload a certificate.

Before uploading a certificate signed by a Certificate Authority (CA), you must generate a CSR on the appliance. The CSR is an encrypted text file containing company and domain specific information known as a Distinguished Name (DN). The CSR is then sent to the CA, which uses it to generate a signed certificate.

Certificate	
Issued To	
Common Name (CN)	
Organization (O)	
Organizational Unit (OU)	
Serial Number	01:27:73:33:7E:60
Issued By	
Common Name (CN)	
Organization (O)	
Organizational Unit (OU)	
Validity	
Issued On	Thu Mar 18 21:35:06 GMT 2010
Expires On	Wed Mar 18 21:35:06 GMT 2020
Fingerprints	
SHA1 Fingerprint	03:B9:29:5E:20:19:5C:40:59:19:ED:AF:65:E2:AA:63:9C:6D:D9:CC
MD5 Fingerprint	24:FE:62:32:23:A9:0D:3D:CC:A3:C9:17:22:60:D7:16

Figure 21. Local certificate

To view the local certificate:

Encryption >> Local Certificate

- Click the **local certificate** link. A pop-up window opens with the certificate.

Generating and Downloading a Certificate Signing Request

The CSR requires the following information:

- **Country Name:** Two-digit country code. See the [ISO website](#) for a list of two-digit country codes.
- **State/Province:** Full name of state or province.
- **Locality/City:** Full name of city or town.
- **Organization:** The department of your company ordering the certificate.
- **Common Name:** Fully qualified domain name for which you are ordering the certificate. Requests for wildcard certificates must start with an asterisk and period (*). For example, *.example.com.
- **Subject Alternative Name:** A list of host names to be protected by a single SSL certificate.

To generate and download a CSR:

Encryption >> Local Certificate

1. Select **Generate a Certificate Signing Request**.
2. Click **Generate CSR & Download**. A pop-up window opens.
3. Fill in the form. All fields are required except **Subject Alternative Name**.
4. Click **Create & Download**. A File Download dialog box opens.
5. Navigate to a location on your local or network drive, and save the file. By default, the file is named certreq.csr. Rename the file as needed.

Figure 22. Generate a CSR

Uploading a Local Certificate

You can upload a local certificate generated from a CSR created on the appliance.

To upload a local certificate:

Encryption >> Local Certificate

1. Select **Upload a Locally Generated Certificate**.
2. Click **Upload Certificate**. Navigate to the location on your local or network drive, select the certificate, and click **Open**.

The certificate uploads and displays on the Local Certificate tab.

3. If your certificate authority provided a certificate that does not directly chain to a root certificate then you must also upload an intermediate certificate. Click **Upload Certificate Chain**. Navigate to the location on your local or network drive, select the file, and click **Open**.
4. Click **Save**.
5. Restart the appliance software after uploading your certificate.



Note: You must log back into the server after the restart. See [Restarting the Appliance](#) for more information.

Generating a Self-Signed Certificate

You can generate a self-signed certificate valid for ten years. The contact information for the certificate is automatically populated from the information entered in [Appliance Settings](#). The common name, which is the fully qualified domain name for which you are generating the certificate, is pre-populated. You can manually edit this field as needed.

To generate a self-signed certificate:

Encryption >> Local Certificate

1. Select **Generate a self signed certificate**.
2. Click **Generate Self Signed Certificate**.



Figure 23. Generate a self-signed certificate

3. Complete the form and click **Generate**. The certificate is generated, and can be viewed on the Local Certificate tab.
4. Restart the appliance software after generating your certificate.



Note: You must log back into the server after the restart. See [Restarting the Appliance](#) for more information.

Uploading an External Certificate and Key

You can upload an external certificate and key that were not generated from a CSR created on the appliance.

To upload an external certificate and key:

Encryption >> Local Certificate

1. Select **Upload External Certificate & key**.
2. Click **Upload Certificate**. Navigate to the location on your local or network drive, select the certificate, and click **Open**.
3. If the CA chain was not included in the certificate upload, click **Upload Certificate Chain**. Navigate to the location on your local or network drive, select the CA chain file, and click **Open**.
4. Click **Upload Private Key**. Navigate to the location on your local or network drive, select the private key file, and click **Open**.
5. Restart the appliance software after completing all of these steps.



Note: You must log back into the server after the restart. See [Restarting the Appliance](#) for more information.

Viewing Trusted Certificates

You can view a list of trusted certificates. Any certificate that chains to one of these certificates is trusted as well. An expired certificate displays in red type.

Encryption >> Trusted Certificates

- Click a trusted certificate. A pop-up window opens with the properties of the trusted certificate.

Adding Trusted Certificates

If you communicate with a partner whose certificate does not chain to a CA, you must upload their root certificate in order to send mail to this partner. Add additional root certificates to trust as needed.

Encryption >> Trusted Certificates

1. Click **Add Certificate**.
2. Navigate to the location on your local or network drive, select the certificate, and click **Open**. The certificate uploads and is added to the list of Trusted Certificates.

Removing a Trusted Certificate

You can remove trusted certificates that you have manually added to the Email Security appliance.

Encryption >> Trusted Certificates

1. Select the checkbox next to the trusted certificate to remove.
2. Click **Remove**.

Configuring Appliance Encryption Policies

You can configure inbound SMTP encryption options for mail from the Internet to the Email Security appliance. Additionally, you can enable SSL connections to all Email Security product dashboards.

To configure appliance encryption policies:

Encryption >> Policies

1. If you want to enable a secure connection to all dashboards, select the checkbox.
2. Select the inbound encryption policy in the drop-down list under **Inbound SMTP**. Options are:
 - **Never Encrypt:** Transport Layer Security (TLS) is never offered during the session.
 - **Offer to Encrypt:** If an encrypted session cannot be established, the message is received in the clear.
 - **Always Encrypt:** If an encrypted session cannot be established the connection is closed. Requiring that all incoming mail be encrypted can block a substantial portion of your incoming mail.
3. Deselect the TLS protocols to disable in the **SSL/TLS Configuration for HTTPS and SMTP** section. By default, all TLS protocols are enabled.
4. If you want to disable weak ciphers to increase security, deselect the checkbox for each cipher you want to disable.
5. Click **Update**.



Note: Restart the appliance software after making changes to the HTTPS or cipher selections. You must log back into the server after the restart. See [Restarting the Appliance](#) for more information.

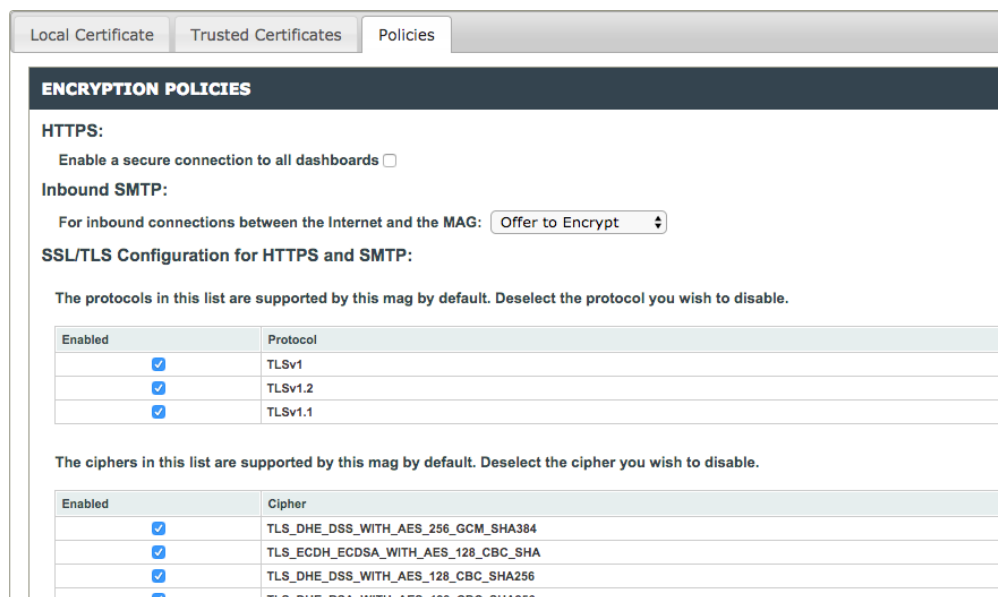


Figure 24. Encryption Policies

Appliance Troubleshooting

The Email Security appliance provides various troubleshooting options, including logs, diagnostics, and statistics.

Logs

The Email Security appliance provides SMTP Session logs for the past seven days for download to resolve message tracking issues. Set the start and end times, in one minute increments for up to one calendar day per log. Times are displayed in GMT. For your convenience, the current time (retrieved from your browser setting) displays in local and GMT on the left side of the screen. Additionally, to assist in finding a specific entry, there is a filter that accepts regular expressions. For more information see [Content Filters](#).

To download a session log:

Troubleshooting >> Logs

1. From the displayed calendar, select the date of the log.
2. Enter the start and end times of the portion of the log to download.
3. Optional: Enter a regular expression in the filter box.
4. Click **Download** to open the file or navigate to a location on your local or network drive, and save the file. By default, the file is named with the current date in YYYYMMDD format. Rename the file as needed.

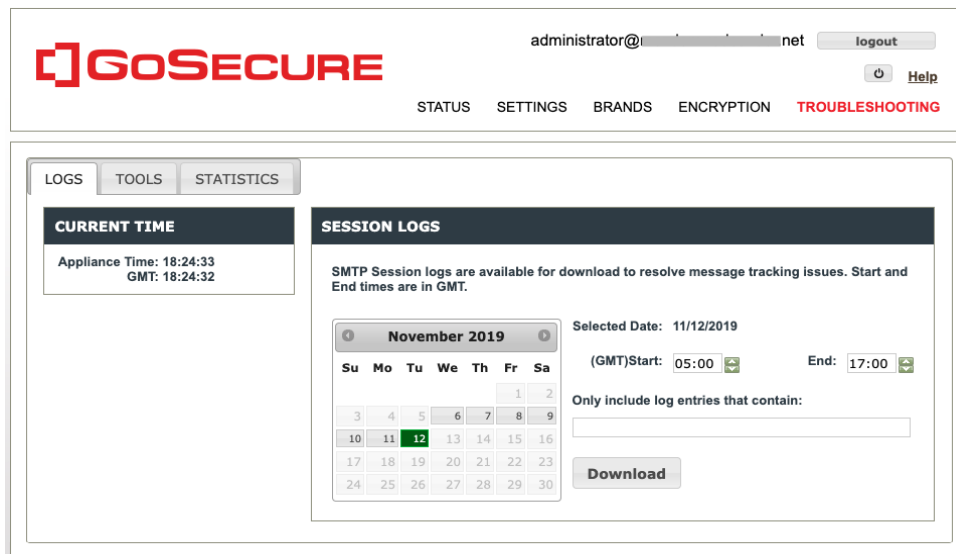


Figure 25. Appliance Troubleshooting: Logs

Diagnostics

The Diagnostics tab provides the ability to execute the following commands and have the results displayed on the page:

- Ping
- DNS Lookup - A and MX (use the appliance's DNS resolver)
- Telnet 25 - You can enter the IP address or the hostname. The connection response is then reported back. This can be useful when connections are failing, as the error response can be seen.

To run diagnostics:

Troubleshooting >> Diagnostics

1. Select the type of diagnostic you want to perform (Ping, DNS Lookup, or Telnet 25).
2. Type the hostname/address.
3. Click **Run**. The results of the diagnostic test are shown in the bottom portion of the Diagnostics window.

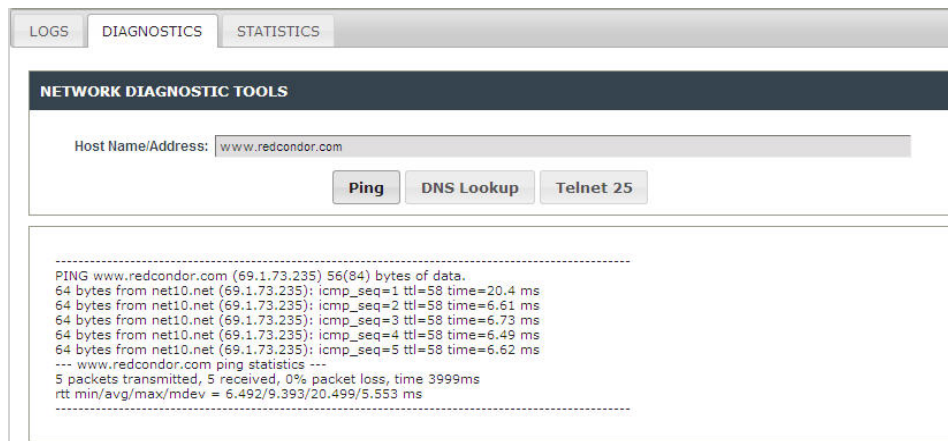


Figure 26. Appliance Troubleshooting: Diagnostics

Statistics

The Statistics tab provides statistics on the Email Security appliance, including:

- a count of inbound sessions
- inbound messages accepted for filtering per hour
- the number of inbound messages per hour that have been filtered
- the number of inbound messages in the queue ready for filtering
- the number of messages that have been accepted for delivery per hour
- the number of delivery attempts per hour
- the number of messages in the deferred queue

Troubleshooting >> Statistics

Category	06:16PM	06:17PM	06:18PM
Inbound session count	80	86	70
Inbound messages accepted for filtering per hour	5578	5937	5038
Inbound messages filtered per hour	5398	5757	5218
Inbound messages ready for filtering	0	0	0
Messages accepted for delivery per hour	0	0	0
Message delivery attempts per hour	0	0	0
Deferred queue	0	0	0

Figure 27. Appliance Troubleshooting: Statistics

Restarting the Appliance

The following configuration changes require a restart of the appliance software:

- Generating a self-signed certificate
- Uploading a certificate
- Changing the encryption policy for HTTPS

When a restart of the software is required, a message displays next to the power button beneath the Logout button on the top right of the screen.



Figure 28. Restart required

If you want to restart the appliance software, reboot, or shut down the appliance:

1. Click  . This opens the Reboot menu.

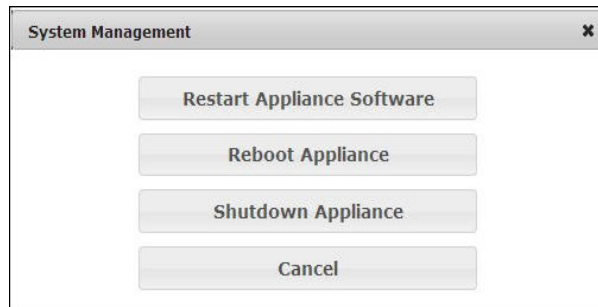




Figure 29. Appliance Reboot menu

2. Click an option:
 - **Restart the Appliance Software:** Closes and restarts the appliance software
 - **Reboot Appliance:** Turns off the appliance and turns it on again, reloading the software
 - **Shutdown Appliance:** Turns the appliance off
3. Click **Confirm**.

The Administrator Dashboard is where you access all of the data for managing your Email Security product. You can see the system status, set up domains and outbound IPs, manage verifiers and content filters, manage mailboxes, and access reports.

Using the Administrator Dashboard

The Administrator Dashboard gives you several ways to manage and view your data.

- **Menus** across the top of the screen provide access to additional functions such as adding new domains, managing mailboxes, viewing reports, and locating messages.
- **More >>** If a menu has more items than fit on the list, this option appears at the bottom of the list. Click it to get the full list, with links to additional options.
- **OmniSearch**, located in the top center of the screen, is a quick way to find the data you want to view or manage. For details, see [Using OmniSearch](#).
- **Tiles** in the work area of the screen show status or lists (such as the domain list), including counts if applicable. You can choose the content shown in each of these tiles. See [Customizing the Dashboard Tiles](#)
- **Home** is a customized screen that includes the tiles you choose. To get back home from anywhere in the system, click the Home icon  in the top center of the screen, next to OmniSearch.
- **Help** is always just a click away. Click the Help icon  in the upper right corner of any screen to get help that is specific to that screen.



Note: The current software version number appears at the bottom of the screen.

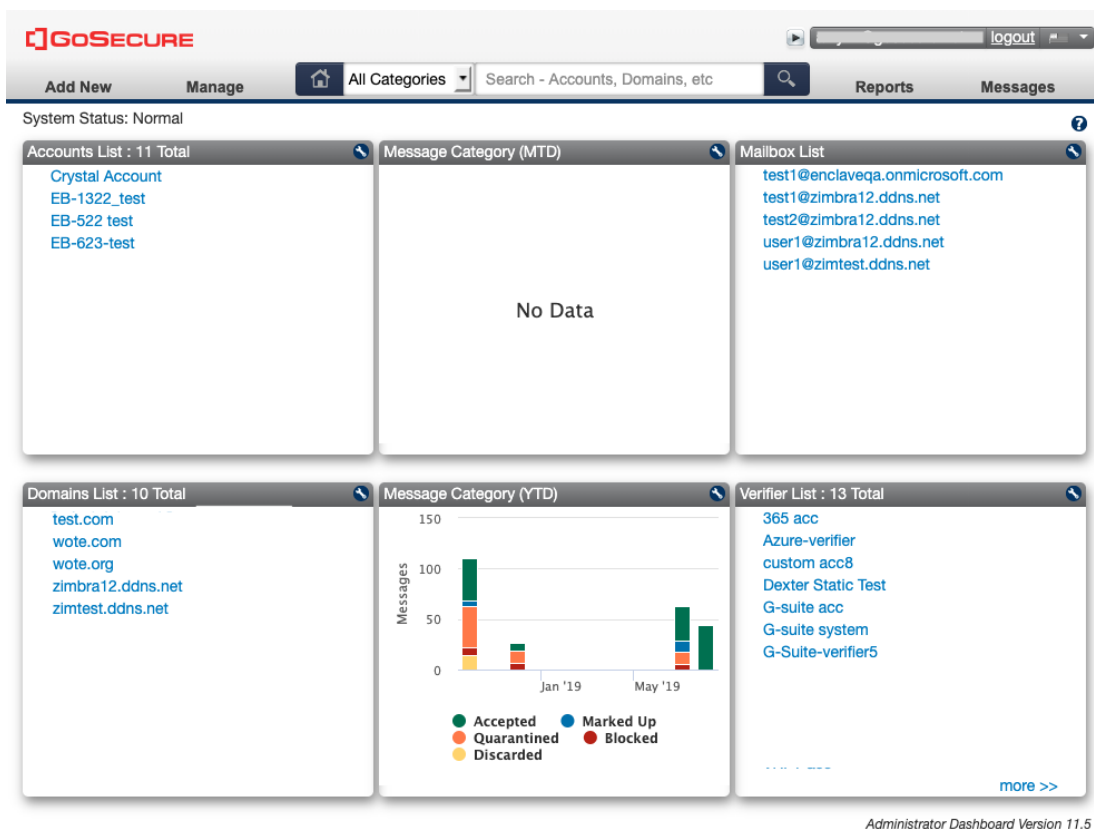



Figure 30. Administrator Dashboard

Customizing the Dashboard Tiles

The home page of the Administrator Dashboard has space for six tiles. These tiles can show system data or lists. For some types of lists (such as the domains list), the total count is included in the title. You select the information contained in each tile.

To change the information shown in a tile:

1. Click the edit icon  in the upper right corner of the tile.
2. In the Change Tile window, select the type of content you want to show.
3. Make additional selections as applicable, depending on the type of content selected.
4. Click **Save**.

Using OmniSearch

From anywhere in Email Security you can jump to a specific domain, outbound IP, verifier, report, or anywhere in the system. OmniSearch allows you to narrow your search by category, and you can use a keyword to find the specific data you want to see.

OmniSearch is located in the top center of every screen in Email Security.



Figure 31. OmniSearch

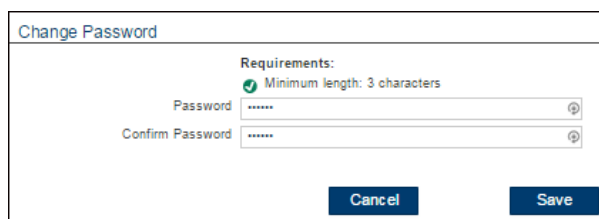
To use OmniSearch:

1. Select a category (optional, helps narrow the search).
2. Enter a keyword.

As you type a list shows the available options. The list narrows as you continue to type. You can press **Enter** to go to the first item in the list.

Changing Your Password

1. Click the down arrow ▼ beside your login name at the top of the screen.
2. Click **Change Password**.



The screenshot shows a 'Change Password' dialog box. At the top, it says 'Change Password'. Below that, there are two text input fields: 'Password' and 'Confirm Password', both containing asterisks. Above the 'Password' field, there is a 'Requirements:' section with a green checkmark and the text 'Minimum length: 3 characters'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Save'.

3. Enter your new password in the **Password** and **Confirm Password** text boxes.
 - Your new password must contain between 8 and 30 ANSI characters.
 - Your Administrator Dashboard and Personal Dashboard passwords are separate. They can be the same, but for security reasons, you should use a different password for each dashboard.
4. Click **Save** to save the new password.

Accounts can have as many domains assigned to them as needed. All domains in an account have the same administrators. You can create multiple accounts to organize and segregate domains, and to apply roles to specific users or administrators.

Some changes to an account or an administrator will result in a notification email being sent to administrators.

Best Practices

Follow these best practices for optimal results using the Email Security product.

Configuring with Other Spam Filter Clients

GoSecure recommends that its spam filter product not be used in conjunction with any other spam filter clients within the user environment. The Microsoft Outlook default Junk Email setting of Low should be changed to Automatic.

The Automatic setting only puts emails in the Junk folder from sender email addresses that are specifically blocked by the user. Once users have been added to the GoSecure solution, such point solutions of blocking email addresses within the Outlook client are not required.

Whitelists and Blacklists

The Email Security product makes whitelist and blacklist options available to domain administrators and end users. However, whitelist and blacklist entries are not required to ensure that users do not receive spam. If there is a conflict between the whitelist entry for the user and a blacklist entry for the entire domain, the user-level setting takes precedence.

GoSecure does not recommend using whitelists and blacklists to manage email accounts because spammers have adopted techniques to send email from addresses within the recipient's domain (including the recipient's own address). Whitelists, in this case, would override the Email Security spam filter rule and result in the spam being delivered to the recipient even though GoSecure has identified it as spam. Similar unintended consequences can result from the use of blacklists.

Quick Start

The Getting Started Wizard steps you through setting up email filtering for an account.

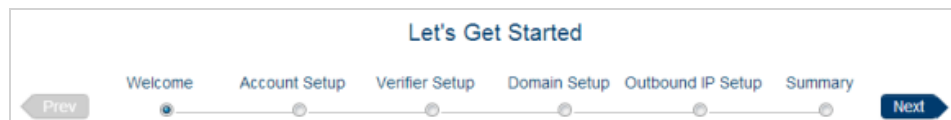


Figure 32. Getting Started Wizard

Add New >> Getting Started

1. Add an account.
2. Add a verifier (optional).
3. Add a domain (optional).
4. Add an outbound IP range (optional).
5. **Save** your data.

Adding an Account

Add New >> Account

1. Enter the account information.
 - The Email address is used for status and release notifications.
 - The Timezone is used to adjust the time stamp in reports and the spam digest to your local time zone.
2. Click **Add**.

Managing Account Information

The Account screen shows your account information, including licensed features.

Domains, Outbound IPs, Verifiers, and Content Filters in the Account are listed across the top of the screen. You can click on any item in a list to go to the detail screen.

Manage >> Accounts >> {Account}

To edit account information:

- Edit the information as needed and click **Update**.



Note: Email Data Compliance, Encryption Service, and ThreatTest Submissions are enabled or disabled based on the account license. Email continuity, if licensed, can be turned on/off for all domains here. If the ThreatTest Service is licensed, the ThreatTest plug-in for Microsoft Outlook can be downloaded here.

To set an account as the default:

- Select the checkbox. If the account is already the default, this checkbox is not available.

To delete an account:

1. Click **Delete**.
2. Click **OK** to confirm.



Note: You can not delete the default account. Once you delete an account, you cannot undelete it. You must manually recreate the account to reactivate it.

Managing Administrators

There are several different types of administrators in the Email Security product. Each type of administrator has different permissions. These permissions apply for the user, for all domains in an account. They also determine which menu options and other screen elements each administrator can access.

Email Security provides four types of administrators:

- **System Administrator** (appliances only): Full rights to the system. The system administrator manages all accounts in the system.
- **Account Administrator**: Full rights to all domains within an account. The account administrator manages a single account. Use this when you have two or more distinct domains that require separate administrators. An account can have multiple administrators.
- **Account Operator**: Controls all domain-level settings (blacklist, whitelist, block vs. quarantine options), and can add or delete mailboxes. The account operator can also run historical reports of email delivery and blocking for any email user. Accounts can have multiple operators. The account operator cannot modify user roles.
- **Dashboard Operator**: Access to the user's Personal Dashboard for individual configurations. This user cannot change domain or user settings but can view any mailbox setting, and can also run historical reports of email delivery and blocking for any mailbox in the domain. All registered mailbox owners are dashboard operators.

System and account administrators do not have to have mailboxes in accounts they administer or in a domain managed by the Email Security product. They must have a valid email account (in any domain) to receive informational and administrative messages.

The administrator hierarchy is as follows:

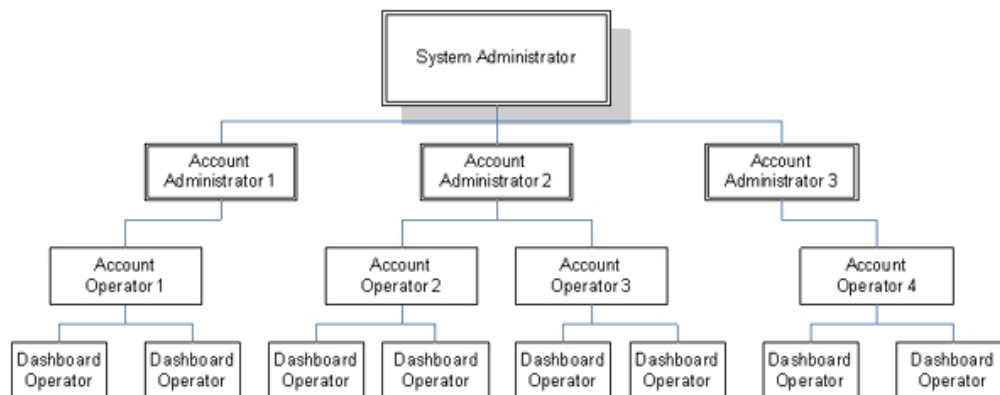


Figure 33. Administrator Types

Account Administrators

When you add a user to the system, they have the same level of access to all domains in the account.

Manage >> Administrators >> Account Administrators

To add a user:

1. Enter the user's email address in the Add User field. You can use an internal email address, an Office365 address, or a Google address.
2. Select the user's access level.


3. Click the Add icon .

To delete a user:

- Click the Delete icon  next to the user's name.

To change a user's access level:


- Select the access level and click **Update**.

Admins who have not yet activated their login appear in the list with the Inactive icon  next to their name. If the admin would like the activation message resent, you can click **Send activation email** to resend it.

System Administrators

Manage >> Administrators >> System Administrators

To add a system administrator:

1. Enter the user's email address in the Add User field. You can use an internal address, an Office365 address, or a Google address.
2. Click the Add icon .

To delete a system administrator:

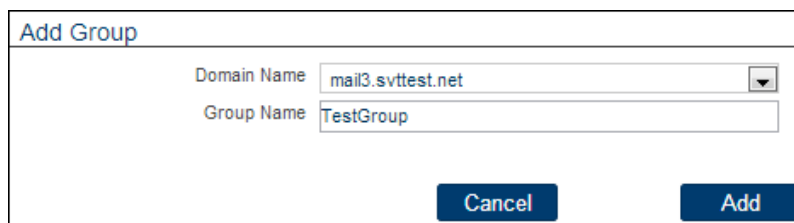
- Click the Delete icon  next to the user's name.

Groups allow you to specify settings for mailboxes within a domain or outbound IP. Group settings override those for the domain or outbound IP, and individual mailbox settings override group settings.

Adding a Group

Add New >> Group

1. Select the domain.
2. Enter the group name.



3. If the selected domain uses an LDAP verifier for mailbox discovery, there is a checkbox for LDAP. If you want all members of an LDAP group to become members of this group, select the checkbox and then select the LDAP group.



Note: To show here, the LDAP verifier must have group support enabled. See [LDAP Verifier](#) for details.

4. Click **Add**.
5. Click **OK** to confirm.

For information on adding members to the group, see [Managing Group Information](#).

Managing Group Information

When a new group is added, the next step is to add members to the group. Then you can configure group settings that override the domain or outbound IP settings for users in the group.

Manage >> Groups >> {Group}

To add users to the group:

1. Use the arrow buttons to move users from the **Available** (non-LDAP) list to the **Selected** list.
2. Click **Update Section**.

To edit group settings:

1. Click **Inbound Settings** or **Outbound Settings** to edit the corresponding information.
2. Make changes as needed.
3. Click **Update**.

To delete a group:

1. Click **Delete**.
2. Click **OK** to confirm.

An account can have one or more domains. The domain contains settings for inbound filtering, mail routing, address validation and user access.

Adding a Domain

Add New >> Domain

1. Select the account.
2. Enter the domain name.

3. Select the method of mail gateway definition. Options are:

Automatic	Populates from the DNS record
Choose	If another domain exists for the account, you have the option to use it as the mail gateway
Manual	Enter the host name of the mail gateway

4. Select the type of mailbox discovery. See [Mailbox Discovery](#) for a description of the discovery options.
5. Click **Add**.



Note: It takes a few minutes for the Email Security product to process the new domain.

Default Domain Settings

When you add a domain, the default domain settings are used. These should be set up the way you want to configure the majority of your domains. You can then change any of the settings that are different for a specific domain, while leaving the others as they are already set.

Manage >> Domains >> Default Inbound Domain

- Update the settings as needed and click **Update**.

Domain Settings

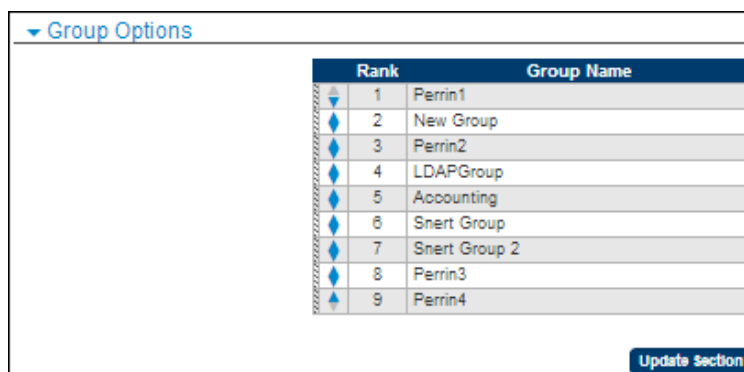
You can configure domain-level settings that apply to all mailboxes in the domain. Then you can customize settings for each mailbox as needed. Individual users can later modify their own mailbox settings. Individual user settings override the domain settings, except when the filter is set to Block.

Manage >> Domains >> {Domain}

- Configure the settings as needed and click **Update**.

Domain Group Options

The Group Options list determines the order in which group settings are applied within the domain. You only see this section if you have set up groups for the domain.



Group Options		
	Rank	Group Name
▼	1	Perrin1
◆	2	New Group
◆	3	Perrin2
◆	4	LDAPGroup
◆	5	Accounting
◆	6	Snert Group
◆	7	Snert Group 2
◆	8	Perrin3
▲	9	Perrin4

Update Section

Figure 34. Group Options

If a mailbox belongs to more than one group, this list determines which settings are applied. Higher ranking means higher priority.



Note: If a setting in the higher-ranked group is set to **default** the setting from the lower-ranked group will be used.

To rearrange the order:

1. Click and drag a group to a new location, or use the up and down arrows.
2. Click **Update Section**.

Domain Digest Options

The Digest Options allow you to specify when and how the spam digest is sent to each user, as well as the type of content it includes.

▼ Digest Options

Frequency

Cutoff Time

Ordering Ascending

Include Outbound Quarantine

Report Format

Report Content

Automatic login token duration Use Default Settings

Automatic login token is valid for days

Figure 35. Digest Options

Option	Description
Frequency	How often the spam digest is sent. By default, the spam digest is sent out daily.
Cutoff Time	For daily digests, you can specify the time of day (up to 2 per day by clicking <input type="button" value="⊕"/>) to generate the report. Early morning is approximately 1:30am. Note that the report will be sent 1-2 hours after the specified cutoff time.
Ordering	The sort order of messages in the spam digest. To sort in ascending order, select the checkbox. If the checkbox is not selected, messages are sorted in descending order.
Include Outbound Quarantine	Includes outbound messages in the spam digest. This option is available if the Direction column was selected in Branding, Spam Digest Settings.
Report Format	The format of the spam digest.
Report Content	The level of detail and type of messages that users receive in their spam digest.
Automatic login token duration	Length of time to set the token for automatic login. If you uncheck the Default Settings box, a text box displays where you can set the number of days the token will be valid.

The report content types are based on zones, as follows:

Content Type	Description
Summary	Includes only the total number of each message type
Green Zone	Junk (bulk email)

Yellow Zone	Foreign, Attachments
Red Zone	Spam, Virus, Adult Spam, Phishing, Bot

Personal Dashboard Options

The Personal Dashboard is where users can manage their email filtering rules, and view and release quarantined messages. There are two versions: low-bandwidth and high-bandwidth. The user can switch between them depending on the type of connection currently in use. You can configure access to the Personal Dashboard for your users, as shown below.

Personal Dashboard Options	
Description	Enable
Allow access to the Personal Dashboard and digest delivery	Default ▼
Allow Delete of Messages	Default ▼
Allow Release of DLP Messages	Default ▼
View/Edit Attachments	Default ▼
View/Edit Foreign	Default ▼
View Outbound Quarantine	Default ▼
View/Edit Policies	Default ▼
View Inbound Quarantine	Default ▼
Allow Release of Inbound Messages	Default ▼
Allow Release of Outbound Messages	Default ▼
View/Edit Friends/Enemies Lists	Default ▼
View/Edit Settings	Default ▼
View message body	Default ▼
Allow setting of SPF exceptions	Default ▼
Allow Recipient Whitelisting	Default ▼

[Update Section](#)

Figure 36. Personal Dashboard Options

Option	Description
Allow access to the Personal Dashboard and digest delivery	<p>Administrators can allow users in this domain to access their Personal Dashboard and digest delivery. Enable is checked by default; if unchecked, the remaining Personal Dashboard options are not available.</p> <p>Note: Changes made to mailboxes in the Personal Dashboard override this domain setting. The administrator must view each mailbox to determine the appropriate setting.</p>

Allow Delete of Messages	Users can delete messages from the Personal Dashboard. If disabled, the Delete icon/button does not appear on the Personal Dashboard.
Allow Release of DLP Messages	Enables releasing of DLP messages. If disabled, the Release icon/button does not appear on the Personal Dashboard for DLP messages.
View/Edit Attachments	Users can view attachments when they view messages.
View/Edit Foreign	Users can view messages tagged as Foreign.
View Outbound Quarantine	Users can view outgoing messages that were quarantined.
View/Edit Policies	Users can view mailbox policies.
View Inbound Quarantine	Users can view incoming messages that were quarantined.
Allow Release of Inbound Messages	Enables releasing of incoming messages. If disabled, the Release icon/button does not appear on the Personal Dashboard.
Allow Release of Outbound Messages	Enables releasing of outgoing messages. If disabled, the Release icon/button does not appear on the Personal Dashboard.
View/Edit Friends/Enemies Lists	Users can view and change their friends and enemies lists. If disabled, the system lists apply.
View/Edit Settings	Users can view and change their Personal Dashboard settings. If disabled, the default settings apply.
Clicking on a "View" link in the Spam Digest will initiate automatic login	<p>When allowed, the user can click a link on their Spam Digest to automatically launch a browser window directly with the Personal Dashboard displayed. If disallowed, the browser launches and brings the user to a login screen.</p> <p>Note: This link is valid for 7 days for weekly digests and 3 days for daily digests.</p>
View message body	Users can view the body of the message in Personal Dashboard. If disabled, a message displays when the user clicks the "contact the administrator" message.
Allow Setting of SPF Exceptions	Users can exempt domains from SPF handling.
View Domain Friends	Users can view list of friends for the domain.
View Domain Enemies	Users can view list of enemies for the domain.

Allow setting of SPF exceptions	Users can set enabled Sender Policy Framework (SPF) options. See Sender Policy Framework Options .
Allow Recipient Whitelisting	Users can whitelist domains.

Filtering Options


Depending on how aggressively you want to filter your email, you can configure to handle messages in each of filtering category.


To specify message handling:

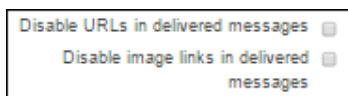
Manage >> Domains >> {Domain}

- Select how to handle blocked messages with the **Blocked Messages** dropdown box. For end users, blocked messages are not included in the quarantine or digest. There are two options for this setting:
 - System Quarantine** – (Only available to administrators) Stores quarantined messages for 35 days.
 - Permanently discard** – Immediately deletes the message.
- For each category, select how to handle messages. For category definitions, see [Filtering Categories](#).

Action	Description
Allow	Passes messages directly to the mailbox without a tag.
Markup	Forwards messages to the mailbox. When you select this option, a text box displays for text entry, which appends to the beginning of the Subject line of the message. A Subject Tag can be up to 20 characters. Note: GoSecure recommends enclosing the text with brackets (for example, [ADV]) to denote an email classified as Junk.
Strip	Applies to attachments only. Strips the attachment (permanently deletes) and delivers the message with an annotation specifying the number of attachments stripped. Stripped attachments cannot be recovered.
Quarantine	Sends messages to quarantine for review.
Block	Immediately deletes messages. Note: Individual mailbox users cannot override this setting.

- To accept messages from a Security Awareness vendor (who usually tests email security on your behalf), click the **Accept Security Awareness test messages** checkbox.
- Select the settings for the available **Compliance** filters.
- To add language filtering, click the Add icon  and then select the desired language from the dropdown box. You can then choose the Action to take when a message in that language is received.
- Select handling for attachments. See [Attachments](#) for more information.

- To select handing of content filters, click the Add icon  and then select the desired filter from the dropdown box. You can then choose the Action to take when the filter is invoked on a message.
- If you want Web links or image links to be disabled in delivered messages, select the corresponding checkbox.



- Click **Update Section**.

Filtering Categories

The Email Security product flags messages that have suspicious content, and sorts them into one of categories listed below.



Notes:

- The default settings can be manually changed for a domain or individual mailbox.
- Credit Card, Social Security, and Email Data Compliance categories are available only on the Email Security appliance. These categories are not available on the Email Security hosted service.

List of Categories

- Virus:** The Email Security product uses traditional signature-based filtering for virus detection. Each email message is analyzed by two separate third-party virus definitions: ClamAV and Kaspersky. By default, the system blocks all emails that have viruses detected in them.
- Phishing:** Phishing fraudulently tries to lure the user into giving up personal information such as credit card numbers, passwords, social security numbers, and account information. Phishing messages often claim to come from banks, department stores, and online merchants such as eBay. By default, the system places this type of email in quarantine.
- Adult Spam:** The Adult Spam category is reserved for spam messages exhibiting sexually explicit characteristics (words, images, hyperlinks, etc.). By default, the system blocks adult content so that it is not available within user quarantine.
- Spam:** Spam is unsolicited or unwanted bulk electronic messaging. By default, the system places this type of email in quarantine.
- Bot:** Messages of this type come from a Bot. A Bot is a compromised or infected PC that has sent spam. By default, the system places this type of email in quarantine.
- Non-Delivery Report/Bounce:** This category includes bounce messages and auto replies (such as out of office messages). It is designed to help reduce backscatter. By default, the system allows these messages.
- PDF contains Javascript:** Portable document format (PDF) files can optionally contain and execute Javascript code. If a PDF file that contains Javascript is attached to an incoming message, by default the system allows these messages.
- MS Office file contains macro:** Files created with Microsoft Office applications can optionally contain and execute a macro, which is a series of commands and instructions. If a Microsoft Office file that contains a macro is attached to an incoming message, by default the system allows these messages.
- Not AV Scanned** For messages that cannot be scanned with the Email Security antivirus scanner or filtered, you can specify how the messages will be handled.

- **Junk:** The Junk category is reserved for bulk mailings where the primary intent is essentially a promotion or advertisement and no deceptive tactics are used. Junk rules only apply to inbound traffic. By default, the system allows junk mail but adds a subject tag of ADV: before the mail subject line. The subject tag is configurable on a domain or individual mailbox level. Junk email is also configurable to be quarantined on a per domain or per mailbox level.
- **Non-compliant MIME:** Handling of emails that do not conform to RFC standards.
- **Accept Security Awareness test messages:** Bypass filtering of messages sent from a Security Awareness vendor. The default is to filter such messages.
- **Credit Card:** Scans the message and text attachments for credit card numbers.
- **Social Security:** Scans the message and text attachments for Social Security numbers.
- **Add Foreign Language:** You can apply foreign language filtering on a per-language basis. By default, the system blocks mail with non-English language character sets (Russian, Cyrillic, Chinese, Korean, and Japanese), but you can also filter email for languages that use the English character set like Spanish or French. If you normally receive email in blocked languages, configure your settings so that these messages pass through the filters.
- **Attachments:** For each type of attachment, you can specify how the message will be handled.
- **Content Filters:** Keyword filtering of messages containing specific words, phrases, and regular expressions in the subject line, message body and plain text attachments. Other types of attachments are not filtered. Messages containing blank headers can also be filtered. Content filtering is primarily used as a security measure to prevent data leaks in outgoing mail. Administrators create one or more content filters in an account, then activate filters on individual domains and outgoing IPs as needed.

Attachments

Some attachments contain potentially harmful programs, such as viruses, spyware, and keyboard capture, that can cause loss of data and/or personal information. GoSecure recommends that you never open an attachment from a sender you do not know, or from whom you were not expecting a file.

You can filter messages with attachments, by attachment type. Additionally, you can add a new attachment type to filter.



Note: Zipped attachments (zip and rar format) are also screened. If an attached zip/rar file contains a file type listed here, the specified action is applied to the entire zip/rar automatically. If there are multiple types of files in the zip/rar, the most aggressive filtering is applied to the zip/rar.

Individual users can configure their attachment settings on the Policies page of the High Bandwidth Personal Dashboard, and the Attachments page of the Low Bandwidth Personal Dashboard.

To add an attachment type:


1. Enter the attachment extension in the text entry box.



Note: The action applied is based on the detected file type, independent of the file name. For example, if an .exe file is named file.txt, the action you choose for an .exe file will still be applied.



Note: Any file with the .exe file extension has the action for an .exe file applied, independent of the file type. For example, if a text file is named file.exe, the action you choose for an .exe file will still be applied.

2. Click the Add icon .
3. Select the action to apply.



Note: If you choose **Strip**, the attachment will be permanently deleted and the message will be delivered with an annotation specifying how many attachments were stripped. Stripped attachments cannot be recovered.

4. Optional: Delete or change the prepended subject line of marked up attachments.
5. Click **Update Section**.

Spoof Options

This section explains the options to protect against spoofing.

For most options, you can choose from one of several actions.

Action	Description
Allow	Passes messages directly to the mailbox without a tag.
Markup	Forwards messages to the mailbox. When you select this option, a text box displays for entering text. This text is added to the beginning of the subject line of the message. A Subject Tag can be up to 20 characters. Note: GoSecure recommends enclosing the text with brackets (for example, [ADV]) to denote an email classified as Junk.
Quarantine	Sends messages to quarantine for review.
Block	Immediately deletes messages. Note: Individual mailbox users cannot override this setting.

Protecting Against Internal Domain Spoofing

These options allow you to configure protection against internal domain spoofing.

Option	Description
Global Protection Check	Specifies handling for all incoming messages with an envelope or MIME sender address that contains this domain (spoofing).
Sender Exceptions	Lists exceptions to accommodate email that your domain sends through a service such as Salesforce. These exceptions can be email addresses, an individual IP address, or an IP range in CIDR format. To exempt internal mail from spoof protection add 0.0.0.0/32 to the exception list. Note: This setting does not display when Global Protection Check is set to Allow.

Smart Protection Check	Specifies handling for incoming messages that appear to be from this domain, if no mailbox exists. Note: Mailbox Discovery must be set to Manual to use this option.
Domain Fuzz Check	Specifies handling for messages coming from domains that are very similar to this one (for example, googel.com instead of google.com).
Domain Fuzz Exceptions	Lists exceptions for domains of allowed message senders. These exceptions can be domain names only. Note: This setting does not display when Domain Fuzz Check is set to Allow.

Sender Policy Framework Options

You can set the following options for Sender Policy Framework (SPF). When you enable the **Allow setting of SPF exceptions** option in the Personal Dashboard Options section, these options are available. Also, when **SPF Envelope Check** is set to **Allow**, the other options do not display.

Option	Description
SPF Envelope Check	Specifies how to handle messages when the sender is not explicitly authorized by SPF.
SPF MIME Check	Enables SPF for the sender displayed in the email client.
SPF SoftFail	Action to take when the sender may not be authorized by SPF.
SPF PermError	Action to take on a permanent SPF error; for example, a badly formatted SPF record.
No SPF Record	Action to take when there is no SPF record.
SPF Exceptions	Sets exceptions for the domain. Enter a domain name in the Forwarding Domain or IP range text box as an individual IP address or an IP range in CIDR format.

DKIM Options

Use these options to manage Domain Keys Identified Mail (DKIM) for the domain.

Option	Description
Add DKIM Signature	Adds DKIM signature to all outbound messages.
Selector	Provides support for multiple DKIM keys for the same domain.
Domain Key	Displays the current domain key.
Generate New Domain Keys	Creates new domain keys.

DMARC Options

Use this option to manage Domain-based Message Authentication, Reporting and Comformance (DMARC). You only see the Exceptions and Policy options when you enable DMARC verification.

Option	Description
Enable DMARC	Enables the DMARC verification of inbound messages.
DMARC Exceptions	Specifies any exceptions for the domain. You can enter a domain range, an individual IP address, or an IP range in CIDR format..
Override DMARC Policy	Selects the action to take when a message does not pass DMARC verification.

Display Name Spoofing Option

Use this option to manage messages that contain a sender address and display name pair not found in the approved list. You only see the two options below when Block, Quarantine or Markup are selected as the Action.

Option	Description
Display Name	Enter the name displayed in the email client
Allowed Senders	Enter the email addresses for the sender using that display name.

Filter by Sender

The Friends list, also called a whitelist, is a list of domain/IP-level trusted mail sources. You can choose to exempt any messages sent by anyone on this whitelist that are caught by the phishing category.

The Enemies list, also called a blacklist, is a list of domain/IP-level sources to automatically quarantine.

GoSecure does not recommend using whitelists or blacklists. See [Best Practices](#) for more information.

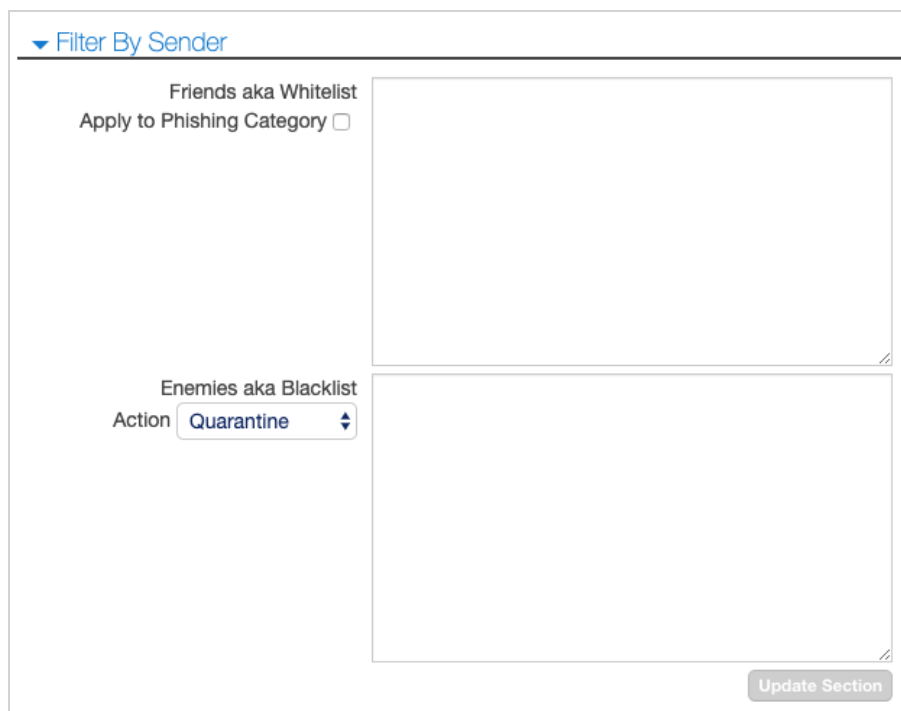


Figure 37. Filter by Sender in Domain Settings

For both types of lists, each entry must appear on a separate line. You can also paste in the entries from another application. To remove an entry, delete the line. There is no restriction on the number of whitelist or blacklist entries for a domain.

To add a note or comment after an entry, precede the comment with // (two slash marks). For example, spam.com //known sender of spam

Valid options are:

- Email address
- Domain (includes all subdomains)
- IP address
- IP address / mask in the format: xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/xx
- Country code

Select how blacklist entries will be handled.

Action	Description
Quarantine	Messages are saved in the quarantine for review.
Block	Messages are deleted immediately.

Notes:


- If you are on a non-hosted system, you can whitelist your own outbound IP address, if the appliance is used as an outbound relay without filtering. You cannot whitelist your own outbound IP on a hosted system.

- The maximum character count in the Whitelist text box is 200,000. If your whitelist is longer than this, you can use the XML API to do the import.
- Each user can maintain their own whitelist from their Personal Dashboard.
- If there is a conflict between the whitelist entry for the user and a blacklist entry for the entire domain, the domain-level setting takes precedence.

Filter Exceptions

You can prevent a spam filter rule from applying to a specific sender or domain (which will also apply to all subdomains). This is useful for inbound email when you don't want to whitelist email from a sender. It's also useful for outbound email when a sender can't be whitelisted.

To prevent a spam filter rule from applying to a sender or domain:

1. Enter the **Rule ID** number. This number appears in the message header X-MAG-INFO in a filtered email message or in the Detail field in the Advanced Report.
2. Enter the **Sender's** email address or domain.
3. Click the Add icon .
4. Select the **Action** to perform:
 - **Add** – Append to existing exceptions.
 - **Replace Items** – Replace all existing exceptions with the new one.
 - **Remove Items** – Check and remove matching exceptions: `<rule>:<senders>`.
 - **Remove All** – Remove all existing exceptions.
5. Click **Update Section**.

Delivery Status Notification

When a message within the domain is quarantined by a Compliance filter, you can choose to send a notification to the recipient or to other email accounts, such as mail administrators or other reviewers. If you enter multiple addresses into the Other text box, separate them with commas. The notification is automatically sent to the sender of the message.



Note: This option is only available if you have a Data Loss Protection (DLP) license.

Message Annotation

This section allows you to define a custom email header, also called an "X-header," that will be added to all incoming messages for the domain. For example, if you want to differentiate between internal and external messages, you can add a header to all incoming messages that identifies external messages. You can also add a markup subject to inbound messages.

Enter the header name in **Header** and the header contents in **Value**. Email header convention is that headers start with "X-". In the example above, a custom header to identify external messages might use the header "X-External" and the value "True", resulting in the header "X-External:True" being added to messages.

To add markup text to the message subject, enter the desired word or phrase in **Markup text**.

Mailbox Discovery

This section allows you to configure the methods for discovering new mailboxes within a domain. For deleting mailboxes that were active at one time, but are no longer active, enable automatic mailbox deletion.

If you don't want to create mailboxes, see [Bulk Email Filtering](#) for instructions.

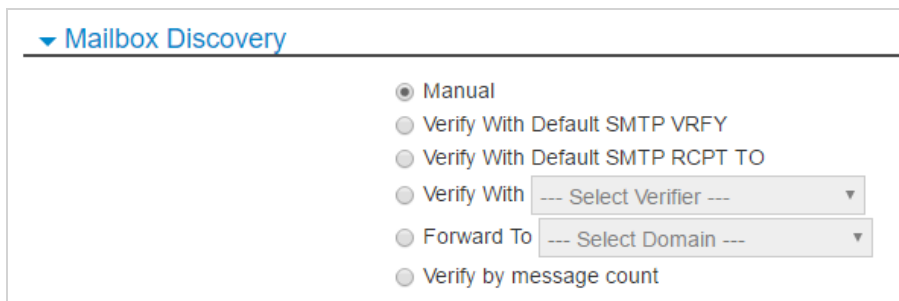


Figure 38. Domain Settings - Mailbox Discovery


Option	Description
Manual	No level of automation, you must manually enter and delete mailboxes as needed. Any time a mailbox is added or removed from your mail server, you must update the Email Security product.
Default SMTP VRFY	Uses the SMTP VRFY command to validate mailbox addresses. If the mailbox does not exist, it creates it. A valid VRFY response is 250.
Default SMTP RCPT TO	Uses the SMTP RCPT TO command to validate mailbox addresses. If the mailbox does not exist, it creates it. A response of 250 indicates a valid mailbox. Some mail servers may respond with 250 even for invalid addresses; in this case, the verifier is not created for that address. A response of 550 means the mailbox has not been validated.
Verify with	Uses a previously defined verifier.

Option	Description
Forward to	Forwards mail addressed to an unrecognized recipient to another domain in your account.
Message count	<p>Creates a new mailbox and assigns a PENDING status to it when a message arrives addressed to an unknown recipient.</p> <p>The mailbox is changed to ACTIVE status if a second message is received within a specified period of time. If a second message is not received within that time period, the mailbox will be deleted</p> <p>You can also choose to delete a mailbox if no legitimate messages have been received after over a specified number of days.</p>

If you choose Default SMTP VRFY, Default SMTP RCPT TO, or Verify with {verifier}, additional options are available.

Option	Description
Create mailboxes for valid recipients	If this box is checked, a mailbox is created; if it is unchecked, a mailbox is not created.
Automatically remove mailboxes	Select this option to enable automatic mailbox deletion for invalid addresses, then choose the number of days to wait before deleting the mailbox. This affects active and unprotected mailboxes.



Note: If a mailbox fails verification, a warning icon  appears next to the mailbox name in the mailboxes list and the mailbox settings page. If the option to automatically remove mailboxes is selected, mailboxes that fail multiple verification attempts are deleted. Mailboxes that fail verification can also be deleted immediately.

The Email Security product also provides an API for mailbox provisioning. See the *Provisioning API Guide* for more information.

Authentication

This section sets your methods of verifying logins. If internal authentication is used, you can also specify the password policies.

Valid options for login verification are:

Option	Description
Internal	ID and password are stored on the Email Security server. Select one of the options from the table below.
SMTP AUTH to Server	Uses SMTP for authenticating the user. Specify the mail server where the ID and password are stored.
Verifier With...	Uses the verifier you select to authenticate the user. The ID and password are stored on the verification server.

Additional Options - Internal Authentication Only

Use Default Settings

Dashboard Inactivity Timeout 60 minutes (System Default Maximum)

0 minutes

Expire password after Never Expire

0 days

Protect accounts with captcha None

3 number of failed login attempts

Password Strength

Minimum Password Length

Require Uppercase Disable

Require Lowercase Disable

Require Number Disable

Require Special Characters (Non Alpha Numeric) Disable

Require Spaces (Multiple Words) Disable

Figure 39. Domain Settings - Internal Authentication

The options for Internal Authentication are:

Option	Description
Use Default Settings	Deselect this checkbox to specify your own settings in this section.
Dashboard inactivity timeout	The number of minutes of inactivity before the dashboard returns to the login screen.
Expire password after	The number of days before a user must specify a new password.
Protect accounts with captcha	The number of failed tries that generates a captcha challenge.
Password strength	Specify the minimum number of characters, then enable/disable each option to specify the types of characters that are required in each password.

Unrecognized Recipient Handling

This section allows you to configure how a message to an unknown user is handled.

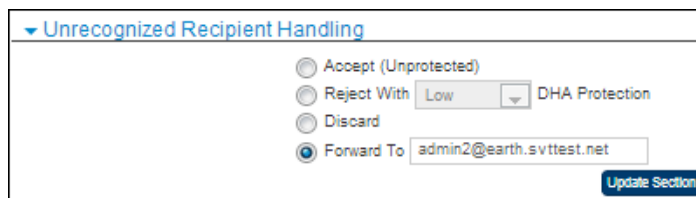


Figure 40. Domain Settings - Unrecognized Recipient

Options are:

Option	Description
Accept (Unprotected)	Forward the message to the customer’s mail server without spam/virus filtering. When this option is selected spooling is set to 1 hour.
Reject with DHA protection (available on unhosted systems)	All messages to unknown recipients are rejected in the SMTP session when DHA protection is set to None. For DHA protection a selectable portion of the messages are randomly accepted and the legitimate ones are bounced. See Directory Harvest Attack Protection .
Reject in session (available on hosted systems only)	All messages to unknown recipients are rejected in the SMTP session.
Discard	Delete the message without sending notification.
Forward to	Send to a specific email address, such as your mail administrator. This email address does not have to be in a domain in the Email Security system.

Directory Harvest Attack Protection

A Directory Harvest Attack (DHA) is an attempt to derive valid email addresses from a domain by flooding the domain with a large volume of email using combinations of common user names, letters and numbers. If mail addressed to an unknown recipient is returned to the sender with the standard 550 unrecognized recipient response, the bounced message can be compared to the sent message list, and the names that were not bounced would be considered valid. They can then be added to a list for spam campaigns.



Note: If you have just created a new alias with DHA, there may be a delay until mail can be delivered to the aliased email address. Until the verifier has verified the new alias, a 551 error will be returned against the alias and the email will be rejected; if you have just created the alias, wait 15 - 45 minutes and try again.

With DHA protection, you configure the amount of unrecognized mail that is rejected by the system. With None, all unrecognized recipient mail is rejected during the SMTP session. This method informs all senders, including spammers, which addresses are valid.

By randomly accepting some mail to invalid recipients the spammer cannot fully determine which email addresses are valid. Only legitimate messages to unrecognized recipients are bounced back to the sender. You can configure DHA protection for Low (some unrecognized recipient mail is accepted), Medium (most), or High (accepts all messages).

Alias Handling

This section allows you to either preserve the mailbox alias before sending the message to the mail gateway or rewrite the alias with the primary SMTP address. For example, the primary SMTP address for Joe Schmo is jschmo@somewhere.com, the alias is joe@somewhere.com. The Email Security product can overwrite the RCPT TO: field in the message envelope sent to joe@somewhere.com so that it appears to have been sent to jschmo@somewhere.com, or leave the alias in the RCPT TO: field.



Notes:

It is assumed that all aliases resolve to the same primary mailbox. Therefore, if one message contains two or more aliases of the same primary address, it is delivered to only one of the recipients. Aliases in individual overrides of outbound rate limits are not supported.

Figure 41. Domain Settings - Alias Handling

Mail Gateways

This setting specifies names or IP addresses of the email servers for the domain. If no port is specified, the system uses the default port 25.

Figure 42. Domain Settings - Mail Gateways

Each entry must appear on a separate line, in one of the following formats:

- Domain

- Domain: Port
- IP address
- IP Address: Port

When multiple servers are configured, select how the mail is distributed in case of server failure.

Option	Description
Failover	Mail is sent the first entered server. If the server is unavailable, mail goes to the second server, and so on.
Random	Mail is evenly distributed between all configured servers.

Boundary Encryption

The options are:

Option	Description
Never Encrypt	Transport Layer Security (TLS) is never attempted during the session.
Attempt to Encrypt	If an encryption session cannot be established, the message is sent in the clear.
Always Encrypt (any certificate)	The server accepts any certificate from the gateway.
Always Encrypt (valid certificate)	The server accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	The server accepts only certificates issued by a trusted Certificate Authority (CA), there exists a complete chain to the CA, and the host name is not an IP address.

Test Connection

Sends an inbound test message from the Email Security product to a mailbox on the domain to validate the boundary encryption settings. Enter a valid mailbox name.

Routing and Session Management

In this section, you can block messages larger than a certain size; spool messages for a period of time; send copies of every message to an SMTP collection address; and keep copies of messages delivered to the mail gateway.

▼ Routing and Session Management

Limit message size

Block messages exceeding megabytes

Spool messages for up to hours


Force redelivery of all spooled messages

Send copy of every delivered message to

Keep a copy of messages delivered to the Mail Gateway

Domains required to use TLS

Figure 43. Domain Settings - Routing and Session Management

Option	Description
Limit message size	Limit the maximum size of an individual message.
Block messages	Enter the maximum message size in megabytes, from 1-100. Messages larger than this are rejected by the system. If an attachment is larger than 10MB, the bounce message notification includes only the message headers and not the attachment itself. Note: This option is available only if Limit Message Size is selected.
Spool messages	Configure spooling of messages for a period of time, measured in hours, in case of server failure. You can specify from 1 through 320 hours.
Force redelivery of all spooled messages	Immediately deliver messages that are currently being spooled.
Send a copy of every delivered message	Enter a valid email address.
Keep a copy of messages delivered to the Mail Gateway	Enable this setting for access to delivered messages either for releasing to an inbox or when Email Continuity is active. Note: If Email Continuity is active, this option is automatically checked and cannot be changed.
Domains required to use TLS	TLS must be used for messages coming from the domains listed here. If TLS is not used, the message is rejected. Click the Add icon  to add a domain to the list.

Email Continuity

If you have a license for Email Continuity, use this section to activate and deactivate it or setup automatic activation/deactivation. The last several status changes (activation or deactivation) are listed with dates and times.

▼ **Email Continuity Settings**

Email Continuity was last manually deactivated on 7/21/2014 3:13:00 pm
 Email Continuity was last manually activated on 7/21/2014 3:12:33 pm

Activate Email Continuity (only use during downtime)

Automatic Settings

Enable Automatic Activation

Activate Email Continuity after continuous minutes of failure to connect to the mail gateway

Do not automatically activate if deactivated less than minutes ago

Enable Automatic Deactivation

Test Email Account @mail.mozdom.com

Deactivate Email Continuity after continuous minutes of successful mail delivery

Do not automatically deactivate if activated less than minutes ago

Figure 44. Domain settings - Email Continuity

Option	Description
Enable Email Continuity	If your organization has licensed Email Continuity, you can enable it here. For details see Email Continuity .
Enable Automatic Activation	If you want Email Continuity to be enabled automatically, select this checkbox and specify the following parameters.
Activate Email Continuity after x minutes	Enter the number of minutes after server failure that Email Continuity will be automatically enabled.
Do not automatically activate if deactivated less than x minutes ago	Enter the number of minutes Email Continuity is to be turned off before it can be automatically enabled again.
Enable Automatic Deactivation	If you want Email Continuity to be disabled automatically, select this checkbox and specify the following parameters.

Deactivate Email Continuity after x continuous minutes	Enter the number of minutes after the server comes back online, that Email Continuity will continue to be activated. After this time, it will be automatically deactivated.
Do not automatically deactivate if activated less than x minutes ago	Enter the number of minutes Email Continuity is to be activated before it can be automatically deactivated.



Tip: You can add a notification to alert you when Email Continuity is automatically enabled or disabled. For details, see [Adding a Notification](#).

Anti Virus Engines

This section specifies which antivirus engines to use. The Email Security product offers both Kaspersky and Clam filtering engines. You can choose to use one or both of them, or deactivate them.

To configure antivirus engines:

Manage >> Domains >> {Domain}

- In the Antivirus area, select the checkboxes for the antivirus engines you want to use.

Moving Domains Between Accounts

A domain can be moved to a different account if it doesn't have any content filters or account-level verifiers. If it does, delete these first, then move the domain.

To move a domain from one account to another:

Manage >> Domains >> {Domain}

1. Click the **Move** link. The **Move Domain** screen opens.

2. Select the new account for the domain.
3. Click **OK**.

Deleting a Domain

Once you delete a domain, you cannot undelete it. You must manually recreate the domain to reactivate it.

Manage >> Domains >> {Domain}

1. Click **Delete**. A confirmation message appears.
2. Click **Yes**.

Viewing Domain Status

You can view the configured DNS Mail Exchanger (MX) records and Domain Status for domains.

See [External DNS Configuration](#) for details on setting up management of the MX records.

Manage >> Domains >> {Domain}

- Click the **Status** link. The **Domain Status** screen opens.

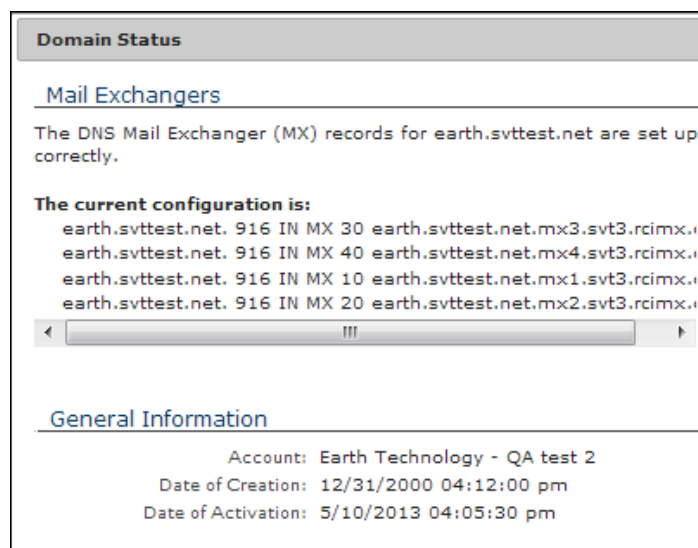


Figure 45. Domain Status

Bulk Email Filtering

You can configure the system to support two types of users:

- Premium:** Provisioned users that can optionally receive the Spam Digest and have access to their Personal Dashboard to manage their accounts.
- Bulk:** Users that are not defined on the appliance. These users do not receive the Spam Digest or have access to a Personal Dashboard to manage their accounts.

Spam and other filtered messages are held in the quarantine for 35 days for all users. Account administrators can generate reports and search filtered messages for the bulk account and for individual users.

Bulk email filtering allows administrators to offer class-of-service options on a per-domain or per-user basis. Bulk filtering can significantly lower the processing requirements and cost of user account. Premium filtering allows you to offer a service differentiator by enabling user access to the Spam Digest and Personal Dashboard.

To enable bulk email filtering, in the Domain Settings, Mailbox Discovery section, deselect **Create mailboxes for valid recipients**.

Add individual mailboxes for premium services to bulk-filtered domains as you would mailboxes in any other domain. See [Adding a Mailbox](#) and the [Provisioning API Guide](#) for more information.

Email Continuity

Email Continuity gives users access to their email when the email server is down. If your organization has licensed this feature, Email Continuity can be activated automatically or manually. Users can use the Messages tab of their Personal Dashboard to manage and respond to all of their incoming and previously received messages.



Note: When Email Continuity is active, the Outbound Authenticated Relay settings are applied to outbound messages.

When the email server comes back up, Email Continuity can be deactivated automatically or manually so that copies of all sent messages are relayed to the mail server. These messages contain the header 'user-agent:GoSecure/Email Continuity (console)' for identification by the mail server. The server can then place these messages in the sender's Sent folder.

Configuration

The following steps are recommended for configuring Email Continuity:

- Use a Composite verifier for authentication. This verifier should include the verifier you already have configured plus a static verifier. When the mail server is down, users can still log in by authenticating with the static verifier.
- Add a notification to alert you when Email Continuity is automatically activated or deactivated. For details, see [Adding a Notification](#).
- Increase spool time up to 60 days. A message is bounced after the spool time is exceeded so the spool time should be as long as possible.
- Add a filter to the mail server to place all messages containing the header 'user-agent: GoSecure/Email Continuity (console)' in the mailbox Sent folder. To separate read and deleted messages, messages that have been read have the header X-MAG-EMAIL-CONTINUITY-READ and messages that have been deleted have the header X-MAG-EMAIL-CONTINUITY-DELETED.
- Activate and deactivate Email Continuity, and set up automatic activation/deactivation in the [Email Continuity](#) section of Domain Settings.

Reporting

Messages sent while Email Continuity is active will show in the reports for the first Outbound IP in the list of Outbound IPs.

The Email Security product offers an outbound email filtering service. Similar to inbound filtering, the outbound filter blocks spam, phishing schemes, viruses, and offensive content. Additionally, you can limit the number of messages sent by each user to prevent spam broadcasts from your domain.

Adding an Outbound IP Address

You can view information about where to route your outbound mail (the outbound host) and general information on your outbound IP on the Outbound status page. See [Viewing Outbound IP Status](#) for more information.

Add New >> Outbound IP

1. Select the account.
2. Select the outgoing IP type:
 - IP Address Range - If you do not use a shared provider, select this option and then enter the IP address or range. This is the IP address of the server that delivers email to the Email Security server. You can add a range of servers in CIDR format.
 - Shared Provider - Use this option if you use a hosted email system such as Google Apps or Office 365.



Note: If you use a shared provider other than Google Apps or Office 365 or if you want your mail server to be a shared provider, contact GoSecure for support. See [Contacting Us](#).

3. Click **Add**.

The screenshot shows a dialog box titled "Add Outbound IP". It contains the following fields and options:

- Account:** A dropdown menu with "Earth Technology - QA test 2" selected.
- Outbound Type:** Two radio buttons: "IP Address Range" (unselected) and "Shared Provider" (selected).
- Shared Provider:** A dropdown menu with "Google Apps" selected.
- Buttons:** "Cancel" and "Add" buttons at the bottom right.

Figure 46. Adding an outbound IP

Outbound Authenticated Relay Settings

These settings are used to filter outbound traffic from senders not located in any of the configured outbound IP ranges. The Outbound Authenticated Relay settings are the same as the outbound IP settings but they are only used for these senders.

**Notes:**

Outbound Authenticated Relay is only available for the Email Security appliance, and can only be used on IP addresses configured to use the SMTP Out only service.

Authentication must be configured for the relay to be functional.

Manage >> Outbound IPs >> Outbound Authenticated Relay

- Update the settings as needed and click **Update**.

Outbound IP Settings

The Outbound IP Settings section has sections for configuring the Delivery Status Notification (DSN), rate limiting, special routing, and outbound mail filtering options. See [Filtering Options](#) and [Outbound Filtering](#) for information about filtering.

Manage >> Outbound IPs >> {Outbound IP}


- Configure the settings as needed and click **Update**.

Member Domains

For certain shared providers, such as Office365, you must list the domains that are permitted to send outbound mail from that shared provider through the Email Security product

Figure 47. Specifying Member Domains

Manage >> Outbound IPs >> {Outbound IP}

1. In the Member Domains section, use the arrow buttons to move domains between the Available and Selected lists.
2. Use the External Domain section to specify one or more external domains. The external domain specified includes all subdomains. Enter the domain name in the text box, then click the Add icon .
3. Click **Update Section**.

Outbound Filtering

Outbound filtering is a defensive measure against internal network zombies that may send out spam and cause the domain to be blacklisted. This allows you to be sure that none of your users violate the terms of their accounts.

Outbound filtering has most of the same filtering options as inbound filtering, with the addition of:

- Recipient White List
- The option to add a disclaimer (Message Annotation)
- Rate Limits
- The ability to route mail based on message content



Note: If Email Data Compliance is licensed, there are additional health, finance, and profanity filters available to aid in following compliance laws such as SOX and HIPAA.

Outbound filtering does not have:

- Foreign language and junk filters

As with inbound email, outbound filtering has the option of managing the maximum size of an individual message. See [Routing and Session Management](#) for more information.

At a high level, configuring outbound filtering requires the following steps:

- Create an outbound IP profile for each mail server that will relay outbound mail through the Email Security server. This profile sets the remediation policy for detected spam and viruses. You can configure the policy for risky attachments and set a whitelist of users that are allowed to send email without outbound filtering for high-volume and bulk email senders.
- For each outbound filtered domain, set the domain mail server to relay all outbound email to the Email Security server.
- Change the firewall settings to block all outgoing email that attempts to bypass the domain's mail server and the Email Security's outbound filtering.

Outbound Filtering Options

Depending on how aggressively you want to filter outgoing email, you can configure how messages in each of the filtering categories are handled.

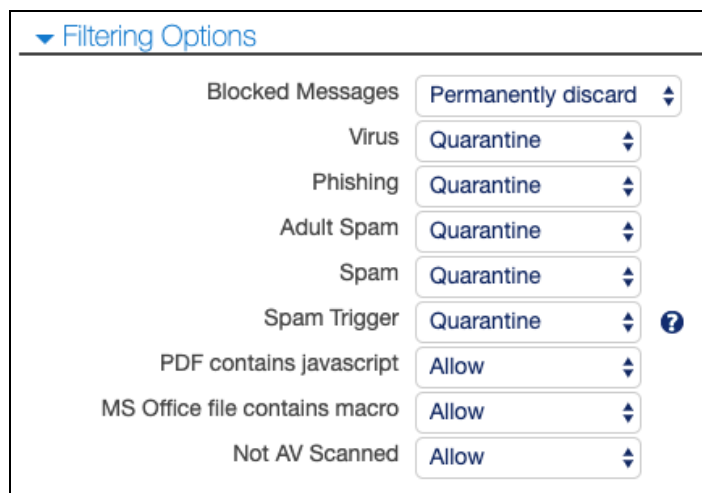


Figure 48. Outbound Filtering Options



Note: If you are using the hosting service, the following filters do not allow you to select Allow or Markup. This is to help protect IPs from being blacklisted unintentionally.

- Virus
- Phishing
- Adult Spam
- Spam
- The ability to categorize mail based on message content

To specify message handling:

Manage >> Outbound IPs >> {Outbound IP}

1. Select how blocked messages will be handled: you can put them in the system quarantine, or permanently discard them. See [Blocked Messages](#) for details.
2. For each category, select how it will be handled.

Action	Description
Allow	Messages pass directly to the mailbox without a tag.
BCC	Messages are sent via BCC to one or more recipients. Separate multiple email addresses with a comma.
Special Routing	Messages are routed according to the instructions you set up in the Special Routing section below. See Special Routing for details.
Attach Encrypted	If your organization has licensed this feature, messages can be sent as encrypted attachments. The text of the accompanying message instructs the recipient to log in to the secure server to decrypt and view the content of the attached message.

Markup	<p>Messages are forwarded to the mailbox with a subject tag. Subject tags can be up to 20 characters. They are prepended to the subject line of the email message to alert you that it has been flagged as suspicious.</p> <p>Note: GoSecure recommends enclosing the text with brackets; for example, use [ADV] to denote an email classified as Junk.</p>
Strip	<p>Applies to attachments only. The attachment is stripped (permanently deleted) and the message is delivered with an annotation specifying how many attachments were stripped. Stripped attachments cannot be recovered.</p>
Quarantine	<p>Messages are saved in the quarantine for review.</p>
Block	<p>Messages are handled according to the Block setting above - either saved in the system quarantine or permanently deleted.</p>

- If you select **Special Routing** or **Encrypted** for a category, the checkbox **Override Compliance** appears. Select **Override Compliance** to have this content filter's action override the Compliance filter actions.
- If you select **Markup** for a category, a text entry box appears on the right. Enter the subject tag in the box.



Note: GoSecure recommends ending the subject tag with a colon. When most mail programs sort on the subject line they ignore the text before a colon and sort on the content of the subject line.

Outbound Filtering Categories

The Email Security product flags messages that have suspicious content, and sorts them into one of the following categories.

Standard Categories

- Virus:** The Email Security product uses traditional signature-based filtering for virus detection. Each email message is analyzed by two separate third-party virus definitions: ClamAV and Kaspersky. By default, the system blocks all emails that have viruses detected in them.
- Phishing:** Phishing fraudulently tries to lure the user into giving up personal information such as credit card numbers, passwords, social security numbers, and account information. Phishing messages often claim to come from banks, department stores, and online merchants such as eBay. By default, the system places this type of email in quarantine.
- Adult Spam:** The Adult Spam category is reserved for spam messages exhibiting sexually explicit characteristics (words, images, hyperlinks, etc.). By default, the system blocks adult content so that it is not available within user quarantine.
- Spam:** Spam is unsolicited or unwanted bulk electronic messaging. By default, the system places this type of email in quarantine.
- Spam Trigger:** Stops "tip of the spear" spam campaigns. By default, the system places this type of email in quarantine. You can change the handling to Markup and then provide a phrase such as [TRIPWIRE] to be prepended to the email subject.

- **PDF contains Javascript:** Portable document format (PDF) files can optionally contain and execute Javascript code. If a PDF file that contains Javascript is attached to an incoming message, by default the system allows these messages.
- **MS Office file contains macro:** Files created with Microsoft Office applications can optionally contain and execute a macro, which is a series of commands and instructions. If a Microsoft Office file that contains a macro is attached to an incoming message, by default the system allows these messages.
- **Not AV Scanned** For messages that cannot be scanned with the Email Security antivirus scanner or filtered, you can specify how the messages will be handled.

Compliance Categories: GoSecure Email Data Compliance (a separate license) filters on five additional categories. The Compliance license includes built-in health and finance lexicons that prevent accidental or malicious exposure of health and financial information - a critical factor in complying with regulatory requirements. For details about Compliance filtering, see the Data Loss Protection (DLP) section of [Overview of Services](#)

- **Social Security:** Scans the message and text attachments for Social Security numbers.
- **Credit Card:** Scans the message and text attachments for credit card numbers.
- **Health:** Scans messages and text attachments using the Health lexicon.
- **Finance:** Scans messages and text attachments using the Finance lexicon.
- **Profanity:** Screens outgoing email for profanity to prevent harassment. You can also specify exceptions, if required.

Other Options

- **Attachments:** For each type of attachment, you can specify how the message will be handled.
- **Content Filters:** Keyword filtering of messages containing specific words, phrases, and regular expressions in the subject line, message body and plain text attachments. Other types of attachments are not filtered. Messages containing blank headers can also be filtered. Content filtering is primarily used as a security measure to prevent data leaks in outgoing mail. Administrators create one or more content filters in an account, then activate filters on individual domains and outgoing IPs as needed.

Filter By Sender

This section enables you to filter by three different sets of lists.

Friends (whitelist) is a list of addresses or domain names of trusted mail sources. Mail sent from these addresses or domains will not be subject to spam filtering.

Enemies (blacklist), is a list of email addresses, domain names, or IP addresses that send mail you want to stop. You can select how blacklist entries will be handled:

Action	Description
Quarantine	Messages are saved in the quarantine for review.
Block	Messages are deleted immediately.

Recipient Friends (whitelist) is a list of a email addresses or domain names of mail recipients who should always receive mail sent from this outbound IP. Mail sent to these recipients will not be subject to spam filtering if ALL recipients of the email are on this whitelist. If your organization is using GoSecure's Encryption or DLP, those features will override a whitelisted recipient.


GoSecure does not recommend using whitelists or blacklists. See [Best Practices](#) for more information.

For all lists, each entry must appear on a separate line. You can also paste in the entries from another source. To remove an entry, delete the line. There is no restriction on the number of whitelist or blacklist entries.

Filter Exceptions

You can prevent a spam filter rule from applying to a specific sender or domain (which will also apply to all subdomains). This is useful for inbound email when you don't want to whitelist email from a sender. It's also useful for outbound email when a sender can't be whitelisted.

To prevent a spam filter rule from applying to a sender or domain:

1. Enter the **Rule ID** number. This number appears in the message header X-MAG-INFO in a filtered email message or in the Detail field in the Advanced Report.
2. Enter the **Sender's** email address or domain.
3. Click the Add icon .
4. Select the **Action** to perform:
 - **Add** – Append to existing exceptions.
 - **Replace Items** – Replace all existing exceptions with the new one.
 - **Remove Items** – Check and remove matching exceptions: `<rule>:<senders>`.
 - **Remove All** – Remove all existing exceptions.
5. Click **Update Section**.

Delivery Status Notification

Use this section to notify a sender when a message has been quarantined or sent encrypted for a specific reason. You can also set the number of notifications per hour per mailbox. The notification consists of a Delivery Status Notification (DSN) message. If you allow access to the outbound quarantine, the message includes a link to release the message from the quarantine.

By default, DSNs are only delivered to senders whose domain is filtered on the system. You have the option to enable delivery of DSNs to senders from unknown domains.



Caution! During an outbound spam campaign a large number of DSNs could be sent to forged senders, possibly causing the server to be blacklisted.

▼ **Delivery Status Notification (DSN)**

Send a notification to known senders

Quarantine Notifications

When a message is quarantined by non-Compliance filters

Also send non-Compliance notifications to

When a message is quarantined by a Compliance filter

Also send Compliance notifications to

Encryption Notifications

When a message is sent encrypted

Also send Encryption notifications to

Other Options

of notifications per hour per mailbox

Include senders from unknown domains

[Update Section](#)

Figure 49. DSN settings

To enable Delivery Status Notification:

Manage >> Outbound IPs >> {Outbound IP}

1. Select the checkboxes you want to enable when a message is quarantined. Selecting any option displays a text box below it. By default, a notification is sent to the message sender. If you wish to also notify someone else, enter their email address in the text box below the option.
 - Quarantined by non-compliance filters
 - Quarantined by compliance filters
 - Sent as an encrypted message



Note: An alias that is not attached to an actual Email Security email address is considered an unknown sender. These addresses will not receive a notification if sent messages are quarantined.

2. Select the maximum number of messages to be delivered per hour, per mailbox. Options are 1 through 10, or unlimited.
3. Optional: For appliances, select the checkbox to include senders from unknown domains. This option is only visible to system administrators.

Rate Limits

Administrators have the option of setting rate limits on outbound mail on a per-user basis. Rate limits set the maximum number of outbound messages each known user, and the total of all unknown users, can send per hour. You can also limit the number of recipients users can send to in a six (6) minute period.

Rate limiting is primarily a means of preventing users from knowingly or unknowingly sending out spam blasts, which can result in your IP address becoming blacklisted. If a user exceeds the messages-per-hour or recipients per-six-minute limit, mail is not accepted by the Email Security product, with either a 451 (temporary) or 550 (permanent) error code.



Notes:

- (1) If the outbound mail is load balanced between multiple mail exchangers, the limit applies to each exchanger. Therefore, the effective limit will be the configured rate times the number of outbound mail exchangers.
- (2) If rate limits are turned on for an individual user but turned off for the domain, the system default error messages are used if an error is encountered.
- (3) Blacklisted senders are not counted against the message rate limits.

Once outbound filtering has been configured, rate limiting can be configured as follows:

- **System administrators:** Can enable or disable rate limiting, specify rate limits per mailbox that override the default settings for the Outbound IP, enter the maximum permitted number of messages per hour (1 - 99999) and six (6) minute period (1 - 99999), select the type of error code returned to the mail server (451 or 550), and enter the text of the error message. By default, rate limiting is disabled. Known senders can be exempted from rate limiting.



Note: Outbound messages that receive 550-series errors can be sent to the administrator for review.

- **Hosted administrators:** Can configure message rate limits but not disable them, and select the maximum permitted number of messages per hour. Options are 100, 200 or 300. They can also select the type of error returned to the mail server and enter the text of the error message. By default, the limits are set to 300 messages per hour for known and unknown senders. The recipients limit can be enabled/disabled and configured by entering a value in the respective text box.

▼ Rate Limits

Messages per Known Sender

Unlimited

Accept Only messages per hour per known sender.

When the limit is exceeded return:

Messages per Unknown Sender

Unlimited

Accept Only messages per hour per unknown senders.

When the limit is exceeded return:

Recipients per Sender

Unlimited

Accept Only recipients per sender every six minutes.

When the limit is exceeded return:

[Update Section](#)

Figure 50. Rate Limits

To add rate limits to outbound mail:

Manage >> Outbound IPs >> {Outbound IP}

1. Select which rate limits to set.

Messages per Known Sender	Enter the number of messages you want to accept per hour for each single known sender. To exempt known senders from rate limiting, select the Unlimited checkbox.
Messages per Unknown Senders	Enter the number of messages you want to accept per hour for all unknown senders. To exempt unknown senders from rate limiting, select the Unlimited checkbox.
Recipients per Sender	Enter the number of recipients per sender you want to accept per six (6) minute period. To allow unlimited recipients per sender in a six minute period, select the Unlimited checkbox.



Note: An alias email address is considered an unknown sender.

2. For each rate limit you are using, select the error to return when the limit is exceeded.

451	Temporary
550	Permanent

3. Type the text of the error message returned to the mail server when the limit is exceeded.

Message Annotation

Annotation entries for all outbound messages for a given outbound IP are handled as follows:

- By default, an HTML editor is enabled for message entry.
- You can switch to plain text for message entry.
- You can choose whether to insert the annotation at the beginning or the end of the message.
- Messages forwarded as attachments do not have a disclaimer added within the forwarded message body.
- Quarantined messages that are released and delivered include the disclaimer.
- Multi-part messages are supported.
- Senders are exempted from appending the disclaimer on the Mailboxes page.
- The disclaimer can be up to 1000 characters in length.

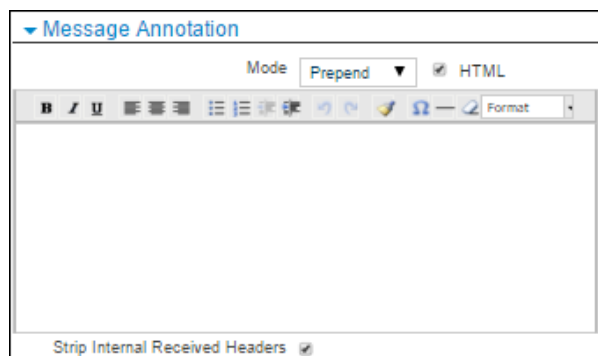


Figure 51. Message Annotation

To annotate messages:

Manage >> Outbound IPs >> {Outbound IP}

1. Select the **Mode** (Prepend or Append) and type the desired message.
2. **HTML** format is checked by default, allowing HTML formatting. This includes bold, italics, underlining, etc. Uncheck **HTML** to format the message in plain text.



Note: The annotation of a message may not be rendered by the recipient's email client when it is sent using Outlook in RTF format. To avoid this problem, the Exchange server can be configured to convert RTF messages to HTML format.

3. If you want the internally-generated headers to be stripped from outgoing messages, select the **Strip Internal Received Headers** checkbox.

Encryption

You can configure the various encryption settings for outgoing messages, and specify encryption settings from the outbound IP to the Email Security product and from the Email Security product to the Internet.

To configure special routing and attachment encryption, see [Configuring the Encryption Service](#).

To configure encryption for outbound mail:

Manage >> Outbound IPs >> {Outbound IP}

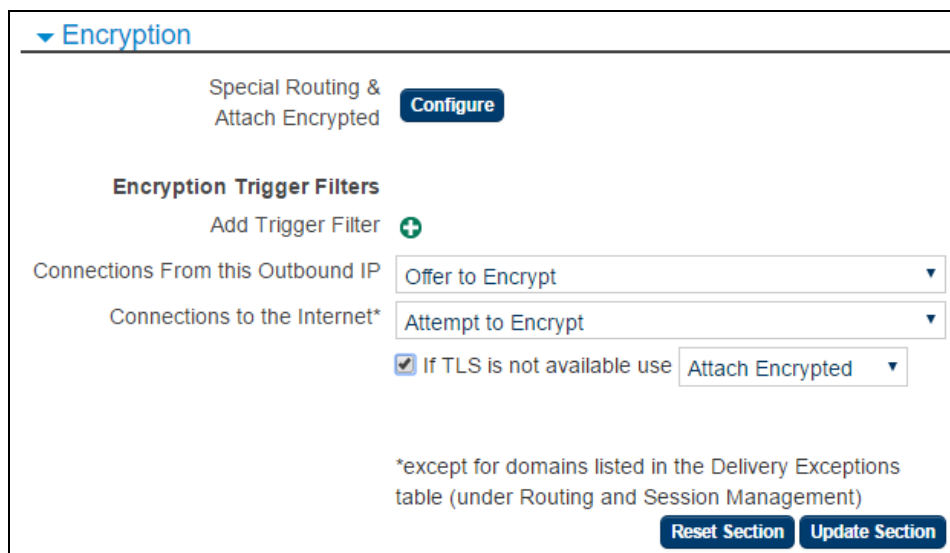


Figure 52. Encryption

1. Encryption can be triggered based on the content of a message's subject. In **Add Trigger Filter**, enter a name for the filter, the word in the subject that will trigger the filter, and select the action: **Attach Encrypted** or **Special Routing**.
2. Select the encryption method for mail from the outbound IP to the Email Security server:

Never Encrypt	Transport Layer Security (TLS) is never offered during the session.
Offer to Encrypt	If an encrypted session cannot be established, the message is received in the clear.
Always Encrypt	If an encrypted session can not be established the connection is closed. The sender can connect and authenticate in the clear but cannot proceed with sending the message.

3. Select the default encryption method for mail from the Email Security server to the Internet. To encrypt all outgoing messages, select Always Encrypt for the default encryption method, and then select the Encryption option.

Never Encrypt	Transport Layer Security (TLS) is never attempted during the session.
Attempt to Encrypt	If an encryption session cannot be established, the message is sent in the clear.
Always Encrypt (any certificate)	Accepts any certificate.

Always Encrypt (valid certificate)	Accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	Accepts only certificates issued by a trusted Certificate Authority (CA), there is a complete chain to the CA, and the host name is not an IP address.

Configuring the Encryption Service

There are four sections to the Encryption configuration section:

- Delivery
- Email Message View
- Attach Encrypted
- Notification Message

Delivery Options

Delivery

Use best method of delivery

Trust Policy: Always Encrypt (any certificate)

Message annotation: *** This message was sent via an encrypted connection using TLS.

Outlook Plug-in Method: Special Routing

Override Compliance

Send read receipt (Special Routing only)

Figure 53. Delivery Options

1. If you want TLS (if available) to override the Encryption service, select the **Use best method of delivery** checkbox and then select the type of certificate that will be accepted.
2. Use the **Message Annotation** text box to customize the default message that will be added to special routed messages and encrypted messages.
3. Select the encryption method to use for messages sent using the Outlook plug-in.
4. If the Outlook plug-in is used, select **Override Compliance** to have messages sent using the plug-in not be subject to compliance filtering.
5. To provide a read receipt for special routed messages, select the **Send Read Receipt** checkbox.

Email Message View Options

Email Message View

Logo **Browse...**

Dashboard banner link

Can Reply

Can Reply All

Can Forward

Can Download

Can Print

Secure All Replies

Figure 54. Email Message View Options

1. Select the logo (maximum size 156 x 41 pixels).
 - This logo appears on the Encryption portal login and message list pages.
 - It can also appear in the notification message (see below).
2. Specify a link where the user will be sent if they click on the logo.
3. Select which actions the user will be able to take on Special Routed and Attach Encrypted messages:
 - Can Reply
 - Can Reply All
 - Can Forward
 - Can Download
 - Can Print
4. If you want all replies to remain on the encryption server as well, click **Secure All Replies**.

Attach Encrypted Options

Attach Encrypted

Expire After (days)

Require Login

Instruction Message

```
<div style="color: #ffffff;"><p align="center";><b>View Secure Message Attachment</b> <img src=cid:paperclip></p><p> To view the secured message click on the attached file and log in.<br>If the file does not open, save it to your hard drive, then open it and log in.<br></div>
```

Figure 55. Attach Encrypted Options

1. Select the amount of time to keep messages that are sent as encrypted attachments. After this time, the messages will be permanently deleted for security purposes.



Note: You can change the deletion date for a specific message after it has been sent. See Encrypted Attachment Report for details.

2. To require the user to log in to view encrypted attachments, select that checkbox.
3. If you want to edit the instruction message that is sent to users for Attach Encrypted messages, change the text for the HTML and/or text version of the message.
4. To override the "from" address used to send PIN code notification, enter an email in the **PIN code sender** text box.

Notification Message Options



Figure 56. Attach Encrypted Options

1. To customize the appearance of the notification message that is sent to users for Special Routed and Attach Encrypted messages:
 - For Special Routed messages, this notification informs the user that a message is available for pickup.
 - For Attach Encrypted messages, the message is encrypted and attached to the notification.

You can customize the notification message as follows:

- Enter the header/footer text for the HTML and/or text version of the message.
- If you want the logo selected above to appear in the notification message, the HTML code in the header or footer needs to refer to it in the same way that the default footer content does. For example:

```
<img src='cid:logo' border='0' alt='GoSecure Encryption Service'>
```


Routing and Session Management

You can define individual encryption settings for each domain, then validate your settings by initiating a test connection to a valid domain.

Figure 57. Routing and Session Management

To configure outbound routing and session management parameters:

Manage >> Outbound IPs >> {Outbound IP}

1. Select the **Limit message size** checkbox.
2. Enter the maximum size for an individual email message. Valid options are 1 through 100. Messages larger than the defined maximum are rejected by the system. Note that if an attachment is larger than 10MB, the bounce message notification does not include the attachment, it only includes the message headers.
3. Enter the number of hours to spool mail before it bounces back to the sender (default is 1), in case of server failure. From 1 through 320 hours.
4. If you want a copy of every delivered message sent to a particular email address, enter the address in **Send a copy of every delivered message to**.
5. If you want to keep copies of messages, check **Keep a copy of messages delivered to the Mail Gateway**.
6. In the Routing area, do the following:
 - Select **Use external DNS resolution** in the unlikely case that the system is unable to deliver mail to multiple domains and you don't want to create delivery exceptions.
 - Select **MX** to use MX routing, or select the second radio button and enter the host name or IP address in the text box.
7. To configure delivery exceptions, click the add icon  next to Add Delivery Exception and enter the domain, routing, and encryption. Click **OK** to add the domain. For details, see [Domain-Specific Delivery Exceptions](#).
8. If you want to send a test message from the product to validate the settings, enter a valid mailbox name in the Test Connection text box and click **Test**.

Domain-Specific Delivery Exceptions

For individual domains, you can specify delivery options that differ from the outbound IP default.


The Email Security product executes a connection test for each domain exception. The test initiates an SMTP session on the Administrator Dashboard server with the destination domain's mail server and attempts to establish an encrypted session. If the test fails, an exclamation point (!) displays to the left of the domain name. Click the exclamation point to show details of the error, including the error message and error code.

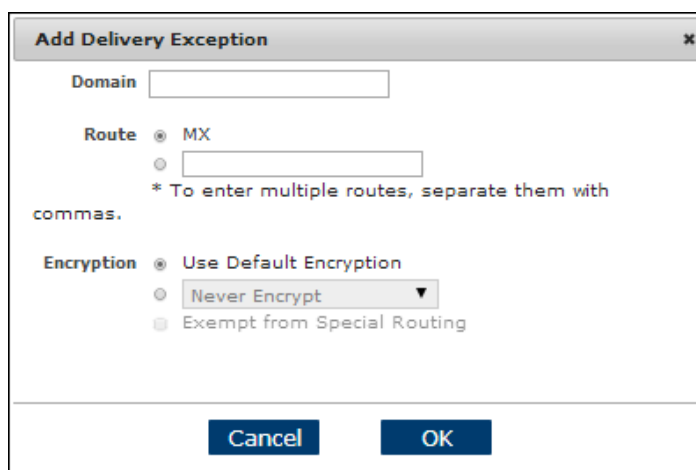
To use TLS in place of SMD, the domain must be added to the Delivery Exceptions list with Encryption set to Always Encrypt

If the error is a certificate validation error, you can view the certificate and elect to trust it. If you do so, the encryption type changes to Manual. Click the triangle next to View Certificate to expand the window. Click the triangle again to contract the view.

To configure domain-specific delivery exceptions for outbound mail:

Manage >> Outbound IPs >> {Outbound IP}

1. In the Routing and Session Management section, click the add icon  next to Add Delivery Exception



2. In the **Domain** text box, enter the name of the domain exception. The expression *.domain.com will cover all sub-domains for the specified domain.
3. For the **Route**, select the second radio button and enter the host name or IP address in the text box.
4. From the **Encryption** drop-down list, select the encryption option.

Option	Description
Never Encrypt	Transport Layer Security (TLS) is never attempted during the session.
Attempt to Encrypt	If an encryption session cannot be established, the message is sent in the clear.
Always Encrypt (any certificate)	Accepts any certificate from the gateway.

Always Encrypt (valid certificate)	Accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	Accepts only certificates issued by a trusted Certificate Authority (CA), there is a complete chain to the CA, and the host name is not an IP address.
Always Encrypt (check hostname)	The certificate is trusted and contains the listed hostname.

- If you select **Always Encrypt (check hostname)**, another text box opens. Enter the hostname to locate the CN or SAN fields of the certificate.
- If you want this domain to be exempt from special routing, select the checkbox.
- Click **OK**.

Authentication

Use this section to choose how to verify mail senders before sending their messages.

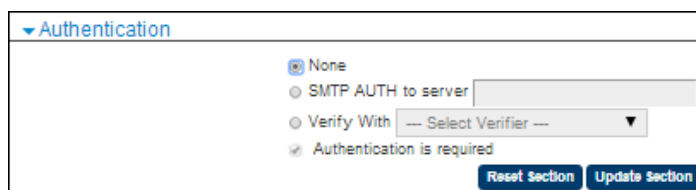


Figure 58. Authentication

To configure outbound authentication:

Manage >> Outbound IPs >> {Outbound IP}

- Select the type of authentication. Options are:

Option	Description
None	No encryption is done
SMTP AUTH to server	Enter the hostname:port or IP address:port
Verify with	From the drop-down list, select a verifier that supports authentication

- If authentication is required, select the checkbox. This will require all senders to be authenticated. To make sender authentication optional, deselect this checkbox.

Special Routing

Special Routing is an option for some types of outgoing messages. If this action is chosen for the message type on the Outbound IPs screen, messages are routed according to the instructions you set up.

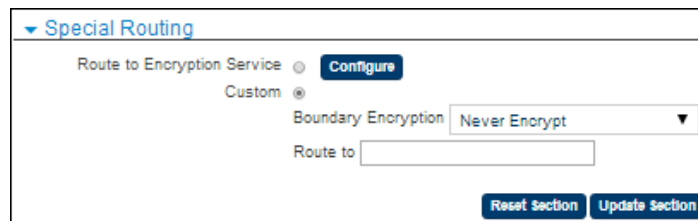


Figure 59. Special Routing

The Route category is included on reports that show message categories for outbound IPs, such as the Message Categories report. Reports that show possible email actions include the Special Routing action.

When configuring special routing, keep in mind the following:

- If you choose Special Routing, you must also configure the special routing parameters. If these are not defined, the system uses the Routing and Delivery Exceptions settings.
- To exempt a specific domain from special routing, use the Delivery Exceptions table. See [Domain-Specific Delivery Exceptions](#) for details.
- To use TLS in place of Encryption Service, add the domain to the Delivery Exceptions list with Encryption set to **Always Encrypt**.

To configure outbound special routing:

Manage >> Outbound IPs >> {Outbound IP}

- In the Special Routing area select how messages with the Special Routing action are to be handled.

Encryption Service

This option sends messages to the Encryption Service.

To configure the Encryption Service:

1. Click **Route to Encryption Service** in the Special Routing section.
2. Click **Configure**. See [Configuring the Encryption Service](#) for details.

Custom Routing

This option allows you to define whether messages are encrypted and to route them to a specific server.

To configure custom routing:

1. Click **Custom** in the Special Routing section.
2. Choose the type of encryption.

Type	Description
Never Encrypt	Transport Layer Security (TLS) is never attempted during the session.
Always Encrypt (any certificate)	Accepts any certificate from the gateway.

Always Encrypt (valid certificate)	Accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	Accepts only certificates issued by a trusted Certificate Authority (CA), there is a complete chain to the CA, and the host name is not an IP address.

- If you want messages with the Special Routing disposition to be sent to another server, enter the address in the **Route to** text box.

Anti Virus Engines

This section specifies which antivirus engines to use. The Email Security product offers both Kaspersky and Clam filtering engines. You can choose to use one or both of them, or deactivate them.

To configure antivirus engines:

Manage >> Outbound IPs >> {Outbound IP}

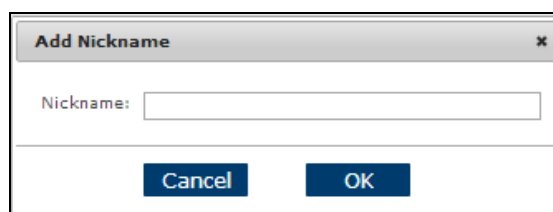
- In the Antivirus area, select the checkboxes for the antivirus engines you want to use.

Nicknaming an Outbound IP

Nicknames make it easier to identify each outbound IP in the system. To give an outbound IP a nickname:

Manage >> Outbound IPs >> {Outbound IP}

- Click the **Nickname** link. The **Add Nickname** window opens.



- Enter the nickname.
- Click **OK**.

Viewing Outbound IP Status

You can view information about where to route your outbound mail (the outbound host) and general information on your outbound IP.

Manage >> Outbound IPs >> {Outbound IP}

- Click the **Status** link. The **Outbound IP Status** screen opens.

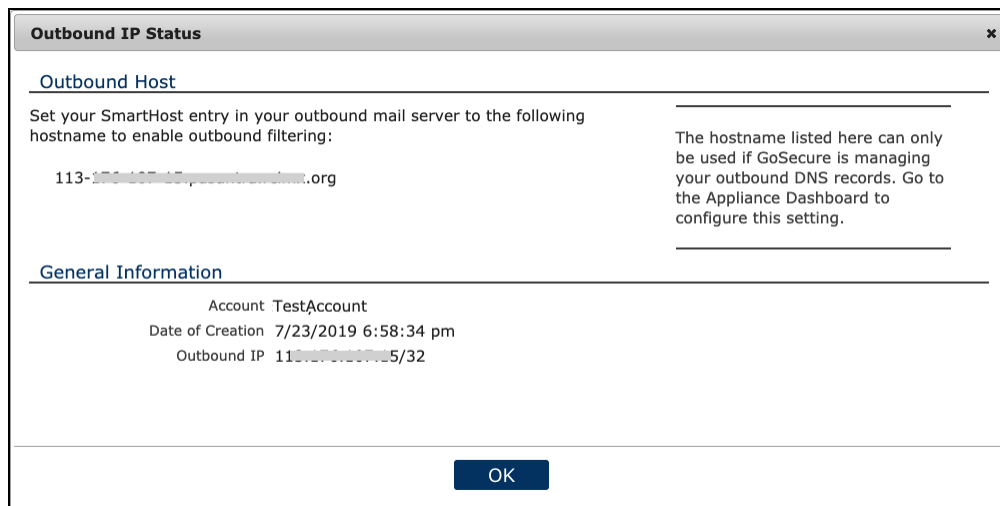


Figure 60. Outbound IP Status

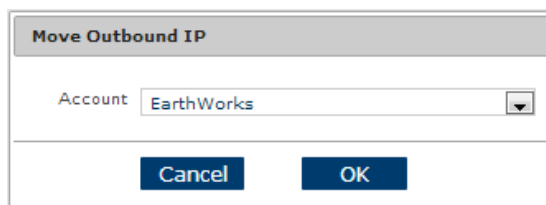
Moving Outbound IPs Between Accounts

An outbound IP can be moved to a different account if it doesn't have any content filters or account-level verifiers. If it does, remove these from the Outbound IP before moving it.

To move an outbound IP from one account to another:

Manage >> Outbound IPs >> {Outbound IP}

1. Click the **Move** link. The **Move Outbound IP** screen opens.



2. Select the new account for the outbound IP.
3. Click **OK**.

Mailboxes are user email accounts managed by the Email Security product. Mailboxes can have one of three states:

- **Active:** Email accounts that are processed for spam and virus filtering.
- **Inactive:** Email and accounts named and configured in the product database that are not currently in use. This mail is not processed and is returned to sender (bounced).
- **Unprotected:** Mail to unprotected mailboxes passes directly through to the user. Unprotected mailboxes do not receive the Spam Digest.

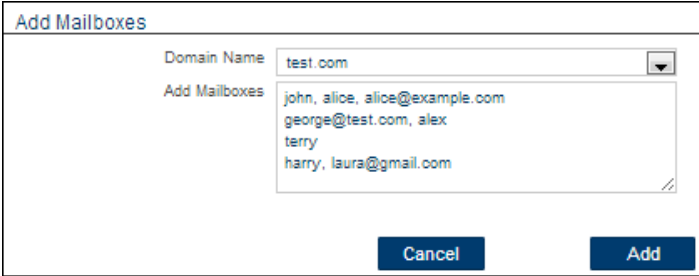
Each mailbox additionally has three permission levels for access to the Personal Dashboard and Spam Digest delivery. These settings override the default settings configured on the domain level. Options are:

- **Full:** Mailbox owner can access their Personal Dashboard and receive the Spam Digest
- **None:** No access to the Personal Dashboard and Spam Digest
- **Default:** Use the default domain settings

Adding a Mailbox

Add New >> Mailbox

1. Select the domain.
2. In the Add Mailboxes text box, enter the name of the new mailbox.
 - To add multiple mailboxes, use a separate line for each mailbox. You can import a list of mailboxes and aliases by copying the list and then pasting it into the text box. Only new mailboxes will be saved; existing mailboxes will be ignored.
 - Use a comma to list multiple aliases. Aliases can be alternate domains.
3. Click **Add**.



The screenshot shows a dialog box titled "Add Mailboxes". It has a "Domain Name" dropdown menu currently showing "test.com". Below it is a large text area labeled "Add Mailboxes" containing the following text: "john, alice, alice@example.com", "george@test.com, alex", "terry", and "harry, laura@gmail.com". At the bottom of the dialog are two buttons: "Cancel" and "Add".

Figure 61. Mailboxes

Configuring Individual Mailboxes

When a mailbox is created, it inherits the default mailbox settings for the domain. You can configure the settings, including mailbox access permissions, for an individual mailbox. If, after changes have been made here, the administrator wants the domain settings to take precedence, the administrator must manually change each mailbox setting.

Manage >> Mailboxes >> {Mailbox}



Note: If the mailbox failed verification, a warning icon with a verification failed message appears at the top of the settings page.

General Settings

▼ General Settings

Mailbox: 1007@futz4.svttest.net

Status: Active

Aliases:

Do Not Auto-Remove:

Add Groups: testgroup

Update Section

Figure 62. General settings for an individual mailbox

Option	Description
Status	The status of the mailbox can be set to Active, Inactive, or Unprotected.
Aliases	Type aliases here. Separate multiple aliases with commas.
Do Not Auto-Remove	Enable to ensure that the mailbox is not automatically removed even if invalid for the time specified in the domain setting for Mailbox Discovery/Automatically Remove Mailboxes. In Bulk Mailbox Settings , select Keep as is to ensure that your previous Do Not Auto-Remove setting is preserved.
Password	The password can be changed here if Authentication is set to Internal.
Add Groups	Select a group to include this mailbox in the group. Group settings override domain and outbound IP settings.

Change Login Password

If authentication is handled internally for the domain, the mailbox password can be changed here.

Figure 63. Change password for an individual mailbox

Digest Options

The Digest Options allow you to specify when and how the spam digest is sent to this mailbox, as well as the type of content it includes.

Figure 64. Digest Options

Option	Description
Frequency	How often the spam digest is sent. By default, the spam digest is sent out daily.
Ordering	The sort order of messages in the spam digest. To sort in ascending order, select the checkbox. If the checkbox is not selected, messages are sorted in descending order.
Report Format	The format of the spam digest.
Report Content	The level of detail and type of messages to be included in the spam digest for this mailbox.

The report content types are based on zones, as follows:

Content Type	Description
Summary	Includes only the total number of each message type
Green Zone	Junk (bulk email)
Yellow Zone	Foreign, Attachments
Red Zone	Spam, Virus, Adult Spam, Phishing, Bot

Personal Dashboard Options

Select Default, Enable, or Disable for each option. If Default is selected, the domain setting applies. If Enable or Disable is selected, the domain setting for this option is overridden by the new selection.

▼ Personal Dashboard Options	
Description	Enable
Allow access to the Personal Dashboard and digest delivery	Default ▼
Allow Delete of Messages	Default ▼
Allow Release of DLP Messages	Default ▼
View/Edit Attachments	Default ▼
View/Edit Foreign	Default ▼
View Outbound Quarantine	Default ▼
View/Edit Policies	Default ▼
View Inbound Quarantine	Default ▼
Allow Release of Inbound Messages	Default ▼
Allow Release of Outbound Messages	Default ▼
View/Edit Friends/Enemies Lists	Default ▼
View/Edit Settings	Default ▼
View message body	Default ▼
Allow setting of SPF exceptions	Default ▼
Allow Recipient Whitelisting	Default ▼

[Update Section](#)

Figure 65. Personal Dashboard Options

Option	Description
Allow access to the Personal Dashboard and digest delivery	Administrators can allow users in this domain to access their Personal Dashboard and digest delivery. Enable is checked by default; if unchecked, the remaining Personal Dashboard options are not available. Note: Changes made to mailboxes in the Personal Dashboard override this domain setting. The administrator must view each mailbox to determine the appropriate setting.
Allow Delete of Messages	Users can delete messages from the Personal Dashboard. If disabled, the Delete icon/button does not appear on the Personal Dashboard.

Allow Release of DLP Messages	Enables releasing of DLP messages. If disabled, the Release icon/button does not appear on the Personal Dashboard for DLP messages.
View/Edit Attachments	Users can view attachments when they view messages.
View/Edit Foreign	Users can view messages tagged as Foreign.
View Outbound Quarantine	Users can view outgoing messages that were quarantined.
View/Edit Policies	Users can view mailbox policies.
View Inbound Quarantine	Users can view incoming messages that were quarantined.
Allow Release of Inbound Messages	Enables releasing of incoming messages. If disabled, the Release icon/button does not appear on the Personal Dashboard.
Allow Release of Outbound Messages	Enables releasing of outgoing messages. If disabled, the Release icon/button does not appear on the Personal Dashboard.
View/Edit Friends/Enemies Lists	Users can view and change their friends and enemies lists. If disabled, the system lists apply.
View/Edit Settings	Users can view and change their Personal Dashboard settings. If disabled, the default settings apply.
View message body	Users can view the body of the message in their Personal Dashboard. If disabled, a message displays when the user clicks the "contact the administrator" message.
Allow setting of SPF exceptions	Users can set enabled Sender Policy Framework (SPF) options. See Sender Policy Framework Options .
Allow Recipient Whitelisting	Users can override filtering of outgoing mail to recipient addresses or domains.

Filtering Options

Use these settings to set up email filtering to be either more or less aggressive. These settings are available for individual mailboxes and in [Bulk Mailbox Settings](#).

These options are available in each filtering category. For category definitions, see [Filtering Categories](#).

Option	Description
Allow	Passes messages directly to the mailbox without a tag.

Markup	<p>Forwards messages to the mailbox. When you select this option, a text box is displayed next where you can enter text. This text is added to the beginning of the subject line of the message. A Subject Tag can be up to 20 characters.</p> <p>Note: GoSecure recommends enclosing the text with brackets; for example, use [ADV] to denote an email classified as Junk.</p>
Quarantine	Sends messages to quarantine for review.
Block	<p>Immediately deletes messages.</p> <p>Note: Individual mailbox users cannot override this setting.</p>

Spoof Options

This section explains the options to protect individual mailboxes against spoofing.

Protecting Against Internal Domain Spoofing

Use the options in this section to configure how to protect against internal domain spoofing.

Option	Description
Global Protection Check	Specifies handling for all incoming messages with an envelope or MIME sender address that contains this domain (spoofing).
Sender Exceptions	<p>Lists exceptions to accommodate mail that your domain sends through a service such as Salesforce. These exceptions can be email addresses, an individual IP address or an IP range in CIDR format. To exempt internal mail from spoof protection add 0.0.0.0/32 to the exception list.</p> <p>Note: This setting is not displayed when Global protection check is set to Allow.</p>
Smart Protection Check	<p>Specifies handling for incoming messages that appear to be from this domain, if no mailbox exists.</p> <p>Note: Mailbox discovery must be set to Manual to use this option.</p>
Domain Fuzz Check	Specifies handling for messages coming from domains that are very similar to this one (for example, googel.com instead of google.com).
Domain Fuzz Exceptions	<p>Lists exceptions for domains of allowed message senders. These exceptions can be domain names only.</p> <p>Note: This setting is not displayed when Domain fuzz check is set to Allow.</p>

SPF Options

You can set the following options for Sender Policy Framework (SPF). When you enable the **Allow** setting of SPF exceptions option in the Personal Dashboard Options section, these options are available. Also, when **SPF Envelope Check** is set to **Allow**, the other options do not display.

Option	Description
SPF Envelope Check	Specifies how messages are handled when the sender is not explicitly authorized by SPF.
SPF MIME Check	Enables SPF for the sender displayed in the email client.
SPF SoftFail	Action to take when the sender may not be authorized by SPF.
SPF PermError	Action to take on a permanent SPF error; for example, a badly formatted SPF record.
No SPF Record	Action to take when there is no SPF record.
SPF Exceptions	Sets any exceptions for the domain. You can enter a domain name, an individual IP address, or an IP range in CIDR format.

DMARC Options

Use this option to manage Domain-based Message Authentication, Reporting and Comformance (DMARC). You only see the Exceptions and Policy options when you enable DMARC verification.

Option	Description
Enable DMARC	Enables the DMARC verification of inbound messages.
DMARC Exceptions	Specifies any exceptions for the domain. You can enter a domain range, an individual IP address, or an IP range in CIDR format.
Override DMARC Policy	Selects the action to take when a message does not pass DMARC verification.

Filter by Sender

A whitelist is a list of trusted mail sources. A blacklist is a list of sources to automatically quarantine. For both types of lists, each entry must appear on a separate line. You can also paste in the entries from another application. To remove an entry, delete the line. There is no restriction on the number of whitelist or blacklist entries for a mailbox.

Note: GoSecure does not recommend using whitelists or blacklists. See [Best Practices](#) for more information .

Valid options are:

- Email address
- Domain
- IP address
- IP address / mask in the format: xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/xx
- Country code

Notes:

- The maximum character count in the Whitelist text box is 200,000. If your whitelist is longer, you can use the XML API to do the import.
- If there is a conflict between the whitelist entry for the mailbox and a blacklist entry for the entire domain, the domain-level setting takes precedence.

Authentication

If internal authentication is used by the domain, this section specifies the password requirements for this mailbox. Use it to override the general password policy that is set for the domain, group, and/or brand.

Option	Description
Use Default Settings	Deselect this checkbox to specify the settings for this mailbox.
Dashboard inactivity timeout	The number of minutes of inactivity before the dashboard returns to the login screen.
Expire password after	The number of days before the user must specify a new password.
Protect accounts with captcha	The number of failed tries that generates a captcha challenge.
Password strength	Specify the minimum number of characters, then enable/disable each option to specify the types of characters that are required in the password.

The screenshot shows the configuration interface for mailbox password policies. It includes a 'Use Default Settings' checkbox, radio buttons for 'Dashboard Inactivity Timeout' (60 minutes), 'Expire password after' (Never Expire), and 'Protect accounts with captcha' (3 failed login attempts). Under the 'Password Strength' section, there is a 'Minimum Password Length' field set to 3, and several options with dropdown menus: 'Require Uppercase', 'Require Lowercase', 'Require Number', 'Require Special Characters (Non Alpha Numeric)', and 'Require Spaces (Multiple Words)', all currently set to 'Default' and 'Disable'.

Figure 66. Mailbox Password Policies

Outbound Mail Options

This section allows you to modify the outbound mail options for this individual mailbox.

The screenshot shows the 'Outbound' settings for a mailbox. It features three main sections:

- Annotation:** A dropdown menu set to 'Accept Default'.
- Messages per hour:** Radio buttons for 'Default' (selected), 'Unlimited', and 'Accept only' followed by a text input field for 'messages per hour'.
- Recipients Rate Limit:** Radio buttons for 'Default' (selected), 'Unlimited', and 'Accept only' followed by a text input field for 'messages per six minutes'.

Figure 67. Outbound mail settings for an individual mailbox

Option	Description
Annotation	Select Accept Default as determined by the domain settings (see Message Annotation), or Disable (do not annotate messages).
Messages Per Hour	Select Default to use the domain level setting (see Rate Limits), Unlimited to remove the limit, or specify the number of messages per hour for this mailbox.
Recipients Rate Limit	Select Default to use the domain level setting (see Rate Limits), Unlimited to remove the limit, or specify the number of messages per 6 minutes for this mailbox.

Mailbox Aliases

A mailbox alias is an alternative name for a user in a same domain. For example, user Joe Schmo may have a mailbox `joe.schmo@yourdomain.com`, but also have aliases of `joe@yourdomain.com`, `joes@yourdomain.com`, or `jschmo@yourdomain.com`.

The alias handling assumes that all aliases resolve to the same primary mailbox. It handles aliased messages as follows:

- If a message is addressed to two or more aliases of the same primary mailbox, it is delivered to only one of the recipients.
- If a message is addressed to the primary mailbox and an alias of that mailbox, it is delivered to only one of the addresses.
- If a message addressed to an alias is quarantined and then later released by the user, it is delivered to the primary mailbox. This is true even if the Preserve Aliases when Sending to Gateway option is in use.
- The `username@domain.com` mailbox automatically receives mail for messages sent to all addresses of the form `username+xxx@domain.com`, even if the address has not been defined as an alias in the system.

Creating Mailbox Aliases

There are three ways to create aliases:

- Add the alias at the same time you create the mailbox (see [Adding a Mailbox](#))
- Add an alias to a single existing mailbox.
- Bulk add aliases to multiple mailboxes.

To add an alias to a single mailbox that already exists:

Manage >> Mailboxes >> {Mailbox}

1. Enter the alias in the **Alias** field. To add multiple aliases to the mailbox, separate them with commas.
2. Click **Update**.

To add aliases to multiple mailboxes:

Add New>> Aliases

1. Select the domain.
2. Enter the aliases in the **Alias** field.
 - To add multiple aliases to a mailbox, separate them with commas.
 - You can import a list of aliases by copying the list and then pasting it into the text box.
 - Only aliases for existing mailboxes are saved; aliases that reference nonexistent mailboxes are ignored.
3. Click **Update**.

The screenshot shows the 'Add Aliases' dialog box. The 'Domain Name' dropdown is set to '--- Select Domain ---' and is marked as 'Required'. The 'Add Aliases' text input field is also marked as 'Required'. A tooltip on the right explains: 'This operation can be used to add aliases to existing mailboxes. Use a separate line for each mailbox. Use a comma to list multiple aliases. See the tooltip for examples.' The 'Add' button is disabled, while the 'Cancel' button is active.

Figure 68. Add New Aliases

Autodiscovering Aliases

If you are using a Mailbox Discovery method that has alias awareness (LDAP or SMTP VRFY), when an alias mailbox is autodiscovered it is added as an entry in the Aliases field for the master mailbox.

Reversing Autodiscovered Alias Relationships

The LDAP feature in the product does not automatically re-learn alias relationships. If the LDAP directory needs to be changed to reverse alias relationships, the adjustments must be done manually in Mailbox Settings to avoid bouncing emails. See [Configuring Individual Mailboxes](#) for details.

An example of reversing an alias relationship is as follows:

- mailbox1@domaina.com is autodiscovered along with a cross domain alias of mailbox2@domainb.com
- mailbox2@domainb.com is added as an alias to mailbox1@domaina.com

To manually reverse the alias relationship in the LDAP directory:

1. Remove mailbox2@domainb.com from the Alias field of mailbox1@domaina.com
2. Add mailbox2@domainb.com
3. Add mailbox1@domaina.com to the Alias field of the mailbox2@domainnb.com mailbox

Accessing the Personal Dashboard

To access the Personal Dashboard:

Manage >> Mailboxes >> more

- In the Mailboxes list, click the **Personal Dashboard** link next to the name of the mailbox. Alternatively, you can right-click to select the version - **Personal Dashboard** or **Personal Dashboard Light**.

The Personal Dashboard has four tabs:

- **Messages:** View, delete, and release filtered messages. You can use the following icons to manage messages:
 - Inbound Quarantine
 - Outbound Quarantine
 - Release
 - Delete
 - Select All
 - Download Message
 - Print Message
- **Settings:** Manage Spam Digest settings, including frequency of digest, format, content, sort order, and time zone.
- **Policies:** Control how intercepted messages are processed. You can filter by message type or sender.
- **Status:** View reports of mailbox name, aliases, digest status and history, and monthly activity.

Unprotecting a Mailbox

Unprotected mailboxes do not have their mail filtered through the Email Security product. The mail passes directly to the user's mailbox.

To unprotect a mailbox:

Manage >> Mailboxes >> {Mailbox}

1. In the General Settings section, **Status** field, select **Unprotected** from the list.
2. Click **Update**.

Deactivating a Mailbox

Deactivated mailboxes are email accounts named and configured in the product database that are not currently in use. This mail is not processed and is returned to the sender (bounced).

To deactivate a mailbox:

Manage >> Mailboxes >> {Mailbox}

1. In the General Settings section, **Status** field, select **Inactive** from the list.
2. Click **Update**.

Deleting Mailboxes

You can manually delete mailboxes. Alternatively, if your mailbox discovery method is Default SMTP VRFY, Default SMTP RCPT TO, or uses a verifier, you can enable automatic mailbox deletion to delete mailboxes that are no longer active.



Note: Once you delete a mailbox, you cannot undelete it. You must manually recreate the mailbox to reactivate it.

To manually delete a mailbox:

Manage >> Mailboxes >> {Mailbox}

- Click **Delete**.



Note: If the mailbox you are deleting has aliases associated with it, you see a warning that includes the list of aliases for the mailbox. You can confirm or cancel the delete action.

To automatically delete inactive mailboxes:

Manage >> Domains >> {Domain}

1. In the Mailbox Discovery section, select the **Automatically remove mailboxes for email recipients found to be invalid for days in a row** checkbox.
2. Select the number of days the mailbox must be invalid before it is deleted. Options are 3, 7, 14, 21, or 28. This setting affects mailboxes with a status of active or unprotected.
3. Click **Update Section**.

A verifier is an object used in domain configuration. It consists of settings used for communicating with the verification server. Verifiers define a method for determining the validity of an email address and/or authenticating a user.

The Email Security product supports two levels of verifiers:

- **Account-level:** For mailbox discovery and authentication for both appliances and hosted systems. Account-level verifiers can be applied to domains within a single account. Account-level verifiers are managed by system or account administrators.
- **System-wide:** Available to domains and IP addresses across multiple accounts. You can create multiple system-wide verifiers. System-wide verifiers are managed by system administrators.

Verifiers are created through the Administrator Dashboard or through the Provisioning API. See the [Provisioning API Guide](#) for more information.

The Administrator Dashboard supports the following types of verifiers:

Verifier Type	Description
LDAP	Lightweight Directory Access Protocol.
VERFY	SMTP command for verifying an email address or authenticating a user.
RCPT TO	SMTP command for verifying an email address or authenticating a user.
Communicate CLI	Command Line Interface (CLI) for server communications.
POP - Authentication Only	POP3 protocol for dashboard login authentication.
Database	MySQL-based database servers containing email addresses for all valid mailboxes, and optionally, passwords.
Static	List of users and passwords is stored in a local database.
Composite	Verifier made up of two or more verifiers. If one verifier in the list fails to respond the system tries to use the next one for verification.
Custom	Use XML code to define the verifier.


Adding a Verifier

Add New >> Verifier

1. Select whether this is a system-wide or account-specific verifier.
2. If this is an account verifier, select the account.
3. Enter a descriptive name for the verifier.
4. Enter the verifier information (see sections following this one for specific information on each type of verifier).
5. To test the connection, enter the information for validation. See [Testing the Verifier Connection](#) for details.
6. Click **Add**.

Figure 69. Adding a Verifier

The verifier options are:

Option	Description
Type	Select the type of verification. Type-specific options appear so that you can further define the verifier.
Notes	Optional: Enter notes about this verifier configuration. This field holds an unlimited number of ASCII characters.
Add Server(s)	Enter the public IP address or host name for the verification server. Use a colon followed by the port number for services with non-standard ports. For example: example-domain.com:228. You must enter at least one server. Click  to save the entry. For LDAP, SMTP VRFY, SMTP RCPT TO, Communigate CLI, and Database, to enable verification on the optional Vx network failover service: <ul style="list-style-type: none"> • If the system is hosted, all server addresses must be external. • If the system is on an appliance and not licensed for Vx, the addresses can all be internal.

	<ul style="list-style-type: none"> If the system is on an appliance and licensed for Vx, at least one address must be external. <p>Repeat as needed for multiple verification servers.</p>
SSL	<p>Select the SSL for each verification server. Options vary depending on the verifier.</p> <ul style="list-style-type: none"> True: A secure connection is made using TLS. False: A non-secure connection is used. StartTLS: After a non-secure connection is used, Start TLS is attempted. If it fails, the connection is dropped. Try StartTLS (default): After a non-secure connection is used, Start TLS is attempted. If it fails, a non-secure connection is used. <p>Note: A connection using PLAIN authentication over an insecure connection is not supported.</p>
Multiple Server Priority	<p>For systems with multiple verification servers, select the server prioritization. For an ordered list, the priority is the order in which the servers are entered. Delete servers and reenter in the proper order as desired.</p>
Verifier-specific settings	<p>Depending on the verifier type, select additional options as applicable.</p>
Enable authentication caching	<p>Select this checkbox to keep a hashed copy of passwords on the system for use when the Verification server is not available.</p>



Note: Changes made on a non-SMTP verification server are reflected in the system when the verifier cache is refreshed.

LDAP Verifier

All necessary settings are automatically generated based on the Verifier options selected. For more granular control of your settings, use the additional LDAP options.

Figure 70. LDAP Verifier

- Optional: Select the **Allow Anonymous Users** checkbox to bind anonymously to the LDAP directory.
- If the **Allow Anonymous Users** checkbox is not selected, enter the following data:

Option	Description
Bind Name	The ID of the user permitted to search the LDAP directory.
Bind Password	The password of the user permitted to search the LDAP directory.

The following options apply for all LDAP verifiers:

Option	Description
Directory Type	The type of directory. Options are Active Directory, Generic, Zimbra, and Domino.
Add Search Base	The location in the directory from which the LDAP search begins.
Mail Attribute Names	The names of the attributes that contain the email address of the user.
Filter Query	The query to use to locate the user in the directory by email address. %d = domain, %u - user.
Enable Group Support	If you want to use LDAP groups, select this checkbox. See below for descriptions of the additional group options.
Maximum Connections	The maximum number of simultaneous connections between the Email Security product directory and the LDAP directory.

Cache Refresh Interval	The minimum number of minutes between queries by the Email Security server to the LDAP directory to update its local cache of the user list. The actual time will vary between 0.5 and 1.5 times the interval.
Request Timeout	The maximum number of seconds to wait for a response from the directory server before the connection times out.

If groups are enabled, the following options are available:

Option	Description
Group Type	The group type: <ul style="list-style-type: none"> • Static: group membership is contained in each group record, listing each user, mostly by user's DN. • Dynamic: group membership is contained in each user's record, listing each group they are a member-of, by group DN. • Hierarchical: works on the assumption that each user's DN lists all groups they are a member of. This usually uses the attribute OU.
Group Member Attribute	The attribute used to designate the group.
Group Name Attribute	The friendly name for the group.
Group Filter Query	The query that will generate the list of groups available for selection on the Add Group page.
Sync Group Members	Click this button to update group membership for all mailboxes in the domains using the verifier. Once the sync is complete, the Group settings are used for the mailboxes in the group.

VRFY Verifier

Figure 71. VRFY Verifier

Option	Description
Maximum Connections	The maximum number of simultaneous connections between the Email Security server and the mail server.
Request Timeout	The maximum number of seconds to wait for a response from the mail server before the connection times out.

RCPT TO Verifier

Figure 72. RCPT TO Verifier

Option	Description
Use Brackets	Optional: Select this checkbox to indicate that the mail server requires brackets (<>) to surround the email address.
Maximum Connections	The maximum number of simultaneous connections between the Email Security server and the mail server.
Request Timeout	The maximum number of seconds to wait for a response from the mail server before the connection times out.

Communicate CLI Verifier

Figure 73. Communicate CLI Verifier

Option	Description
Name	The name of the account that will communicate with the Communicate server.
Password	The password of the account that will communicate with the Communicate server.
Maximum Connections	the maximum number of simultaneous connections between the Email Security server and the Communicate server.
Cache Refresh Interval	The minimum number of minutes between queries by the Email Security server to the Communicate server to update its local cache of the user list. The actual time will vary between 0.5 and 1.5 times the interval.
Request Timeout	The maximum number of seconds to wait for a response from the Communicate server before the connection times out.

POP - Authentication Only Verifier

Figure 74. POP Verifier

Option	Description
Maximum Connections	The maximum number of simultaneous connections between the Email Security server and the POP server.
Request Timeout	The maximum number of seconds to wait for a response from the POP server before the connection times out.

Database Verifier

Figure 75. Database Verifier

- Optional: Select the **Allow Anonymous Users** checkbox if you want to bind anonymously to the database server.
- If the **Allow Anonymous Users** checkbox is not selected, enter the following data:

Option	Description
Name	The name of the account that will communicate with the database server.
Password	The password of the account that will communicate with the database server.
Database Name	The name of the MySQL database.

The following options apply for all database verifiers:

Option	Description
Authentication Query	The SQL query to search the user password.

Domain Query	The SQL query to retrieve the list of valid domains.
ENUM Query	The SQL query to retrieve the list of valid recipients.
VRFY Query	The SQL query to retrieve a specified mailbox.
Maximum Connections	The maximum number of simultaneous connections between the Email Security server and the database server.
Cache Refresh Interval	The minimum number of minutes between queries by the Email Security server to the database server to update its local cache of the user list. The actual time will vary between 0.5 and 1.5 times the interval.
Request Timeout	The maximum number of seconds to wait for a response from the database server before the connection times out.

Static Verifier



Figure 76. Static Verifier

- Enter the list of users and passwords to be used for recipient verification and/or dashboard authentication.
- Place a comma between each user name and password, and a line break after each user name/password pair.

For example:

```
myname1@mydomain.com, my1password
anothername@myotherdomain.com, password
```

Composite Verifier

This is a verifier made up of two or more verifiers. A composite verifier gives you the ability to combine different data sets. You can use a composite verifier when you have two verifier servers that do not contain overlapping mailbox lists or you have one verifier server and a static email list.

If a verifier in the list returns a negative response, the system tries to use the next one for authentication. If none of the verifiers find the recipient, the recipient is flagged as unknown and handled accordingly.

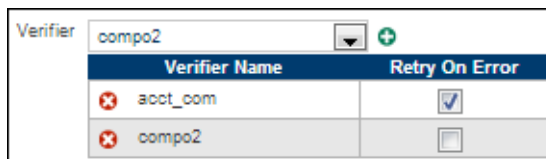


Figure 77. Composite Verifier

- Select a verifier from the **Verifier** list and click to add it to the Composite Verifier list.

- Do this for each verifier you want to include in your composite list.
- For each verifier chosen, select **Retry on error** if you want the system to retry that server until it returns either a positive or negative response to the verification inquiry. With this option selected, if no response is received, the system continues to query the server until it responds rather than failing over to the next server in the list.

**Notes:**

For the next verifier to be checked, with **Retry on error** turned on, the response must be received. If the verification server is down it will not send a response and the system will not move on to the next verifier in the list.

If you are setting up a composite verifier to be used for Email Continuity, deselect the **Retry on error** checkbox. This will ensure that requests fail through to the static verifier when the primary verifiers are down.

This verifier is not designed to provide fallback for servers with identical data sets. Instead, you should use one verifier and specify multiple servers in the list of backend servers.

Custom Verifier

Figure 78. Custom Verifier

- Enter the XML code that defines the verifier.



Note: Once a verifier of type Custom has been saved, it cannot be changed to a different type of verifier. To change it, delete the custom verifier and add a new verifier of a different type.

Microsoft/Office365 Verifier

To configure this verifier, you must provide the Email Security product with access your Office365 account.

To set up the verifier:

1. Click the **Authorize** button to display the Microsoft Authorization page where you can select the account you want to connect to.



Note: The Office365 account must have Administrator permissions.

2. When authorization has been completed, you will be returned to the Add Verifier page.

G-Suite Verifier

To configure the G-Suite verifier, you must provide the Email Security product with access to your G-Suite directory using these steps:

1. Go to the Administrator console of your G-Suite domain.
2. Select **Security** at the bottom of the controls. If it is not visible, you may need to select More (gray bar at bottom of screen).
3. Select **Advanced Settings**.
4. In the Authentication section, select **Manage API Client**.
5. In the Client Name field, enter this Client ID: **102883203975641214119**
6. In the One or More API Scopes field, enter the following value:
 - <https://www.googleapis.com/auth/admin.directory.user.readonly>
7. Click the Authorize button.

Testing the Verifier Connection

When you configure or change a verifier you can also test the connection to make sure the settings are properly configured.

To test the connection:

1. Set up the verifier.
2. In the **Test Connection** text box, enter the email address of a valid user included in the verification server.



Note: The domain must already be in the system.

3. Enter the user password. This is optional and is needed only to test authentication.

Test Connection	
Email	<input type="text" value="sally@mydomain.com"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Test"/>	

Figure 79. Test connection

4. Click **Test**.

A test query is sent to the specified address. The results are shown at the bottom of the screen as follows:

- Green indicates that verification succeeded on all servers. The servers are listed for reference.
- Yellow indicates that verification succeeded on some servers and not on others.
- Red indicates that verification failed on all servers tested.

The result for each server is listed. You can click on a server name for more information about why it failed verification.

Modifying Verifiers

You can modify a pre-defined verifier in the Administrator Dashboard. Custom verifiers can be created through the Provisioning API. You can also convert other standard verifiers to Custom verifiers.



Note: You cannot convert Static or Communicate verifiers to a Custom verifier.

Custom verifiers created through the Provisioning API cannot be modified through the Administrator Dashboard unless the verifier type is changed from Custom to one of the predefined types. Custom verifiers can be modified directly through the Provisioning API.

Manage >> Verifiers >> {Verifier}

- Change the settings as needed and click **Update**.

Deleting a Verifier

You can delete verifiers that are no longer needed by the system. If a verifier is used by one or more domains, a warning screen lists the domains using it. Once deleted, all information from the verifier is purged from the Email Security product. Domains using a deleted verifier convert to using manual mailbox discovery.

To delete a verifier:

Manage >> Verifiers >> {Verifier}

1. Click **Delete**. A confirmation screen opens.
2. Select the **Permanently delete** checkbox and click **Delete**.

When Verification Servers Fail

If your verification server goes down for any reason, messages for unknown recipients are handled according to the [Unrecognized Recipient Handling](#) setting. No mailbox discovery is performed until the server comes back online.

The optional content filtering feature can detect messages containing specific words, phrases, and regular expressions in a message's header, body, and plain text attachments. Other types of attachments are not filtered. Messages containing blank headers can also be filtered. Content filtering is primarily used as a security measure to prevent data leaks in outgoing mail. Administrators create one or more content filters in an account, then activate filters on individual domains or outbound IPs as needed.

The content filter consists of one or more rules. In each rule you can select whether to filter the whole message and/or one or more headers. A content filter set to **Accept** or **Block** is run after the antivirus and Friends and Enemies filters, and before all other filters.

Administrators can create multiple content filters to check for specific content. For example, you might create filters for financial terms, discrimination, profanity, or sexual content. Individual domains and outbound IPs can use a combination of content filters according to their need.

When words or phrases are used, content filtering matches the exact text string. Therefore the keyword **confidential** would filter a message with the word Confidential, but not the word **confidentially**. You can use A-Z, a-z, 0-9, hyphen (-), or underscore (_) to match words and phrases. Keywords are not case-sensitive.

Regular Expressions provide a concise and flexible means for matching strings of text, such as particular characters, words, or patterns of characters. For more information, see:

- General information about regular expressions: <http://www.regular-expressions.info>
- An online tool to test regular expressions: <http://regexpal.com>

Creating a Content Filter

For keyword filtering you create a content filter in an account. You can create as many individual filters as needed, then assign one or more content filters to individual domains or outbound IPs as appropriate.

You can enter the keywords, phrases, and regular expressions individually or copy/paste text from a text editor or word processor. You can use A-Z, a-z, 0-9, hyphen(-), or underscore(_) to match words and phrases. Keywords are not case-sensitive. Content filters support POSIX regular expression syntax. See [POSIX Regular Expression Syntax](#) for details.



Note: If the filter contains multiple rules, one match in the list will activate the filter.

To add a content filter:

Add New >> Content Filter

1. Select the account.
2. Enter a descriptive name for the content filter.

Add Content Filter

Account: Mozdom Account

Name: My Account

Scan Outbound Attachments:

Match Blank Headers:

--- Select Header ---

Add Rule

Cancel Add

3. To scan outbound mail attachments, select **Scan Outbound Attachments**. The entire message, including text, headers/footers, etc. will be scanned. This option is only available if DLP is licensed.
4. To filter for blank message headers, select **Match Blank Headers** and then choose the headers to be filtered.
5. Add rules to define the content filter (see below).
6. Click **Add**.

To add a rule:

1. Click to add a rule.
2. In the **Filter expressions** text box:
 - Paste the list from an external application.or
 - Enter the keywords individually to filter. Press Enter to separate keywords.

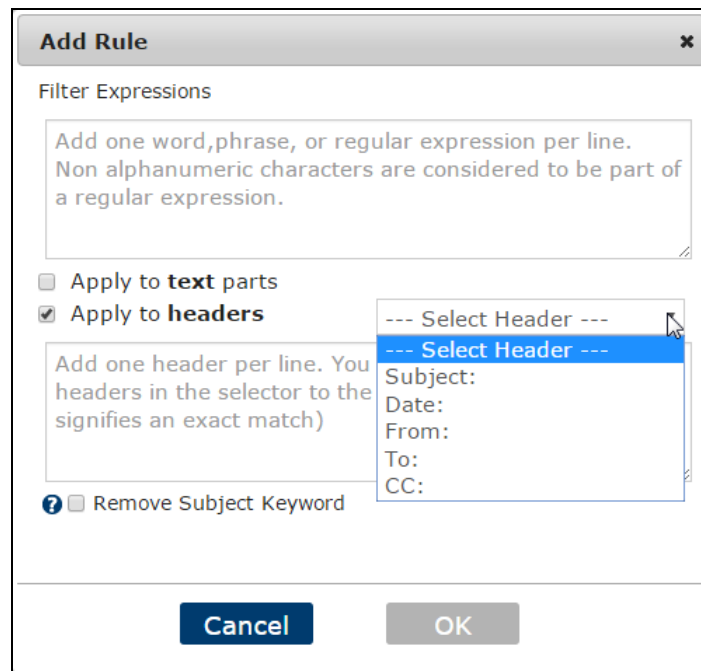


Figure 80. Defining Content Filter Rules

3. If you want the rule to apply to the text of the message, select the corresponding checkbox.
4. If you want the rule to apply to the message headers, select the checkbox and then either select or enter the header items to be checked.



Note: When a header rule is added with no specific headers defined, the system looks for the content in any header. If the header is defined and the content is empty, the system looks for the header and ignores the value. If you are specifying a phrase (multiple words) for a header content filter, prepend the phrase with the period and asterisk characters (.*).




5. If you want the subject keyword to be removed from the header when the message is delivered, select the corresponding checkbox. For this option, the content filter action must be Special Routing or Attach Encrypted.
6. Click **OK** to save the rule.

Modifying a Content Filter

Add, delete, or modify rules in a content filter as needed. You can add, delete, or modify the keywords and phrases individually or copy/paste a revised list from a text editor or word processor. You can use A-Z, a-z, 0-9, hyphen(-), or underscore(_) to match words. Keywords and phrases are not case-sensitive.

Manage >> Content Filters >> {Content Filter}

- Make changes as needed and click **Update**.
 - To change the name, edit the **Name** text.
 - To scan outbound mail attachments, select **Scan Outbound Attachments**. The entire message, including text, headers/footers, etc. will be scanned. This option is only available if DLP is licensed.
 - To filter for blank message headers, select **Match Blank Headers** and then choose the headers to be filtered.


- To add a rule, click the add icon  and define the rule. See [Creating a Content Filter](#) for details.
- To change a rule, click the edit icon  to the left of the rule name.
- To remove a rule, click the delete icon  to the left of the rule name.
- If you want to delete the content filter, click **Delete** and then click **OK** to confirm.

Adding a Content Filter to a Domain or Outbound IP

Add one or more content filters created at the account level to apply keyword filtering to message headers and/or content in a specific domain or outbound IP.

Manage >> Domain >> {Domain}

Manage >> Outbound IPs >> {Outbound IP}

1. In the Filtering Options section, Add Content Filter field, select a content filter and click the add icon .
2. Select the action to apply to the message.

By default, if you choose Markup, CONTENT: is prepended to the subject line of these messages.
3. Optional: Delete or change the prepended subject line of marked up attachments.
4. Click **Update Section**.

POSIX Regular Expression Syntax

Regular expressions (often referred to simply as "regex") can be much more complex than expressions that use the wildcard characters which were discussed in the previous section. Unlike wildcards, regular expressions will match character sequences containing the patterns that they specify regardless of where that pattern appears in a word. As explained later in this section, you can use the anchor symbols '^' (beginning of word) and '\$' (end of word) to restrict where in a word a regular expression will be matched, or to restrict that match to entire words by specifying both anchor symbols.


Regular expressions assign special meaning to various characters, which are often referred to as **metacharacters**:

- period, dot, or full-stop (.) - matches any single-width ASCII character in an expression, with the exception of line break characters. To match multi-byte characters with a single period, you must use Perl-compatible regular expressions, as discussed in [Perl Compatible Regular Expression Syntax](#).

Because Watson Explorer Engine's regular expression support is term-oriented, the '.' will also not match the space or tab by default, which are word breaking characters. For example, the regular expression 'f.rm' will match any words containing character sequences such as 'farm', 'firm', and 'form', including 'farmer', 'firmament', and 'conform' - any word that contains a sequence of characters consisting of an 'f', followed by any other character, followed by with the characters 'rm'.

Tip: The '.' symbol is the equivalent of the '?' character in a wildcard expression. The '.*' sequence is the equivalent of the '*' in a wildcard expression.

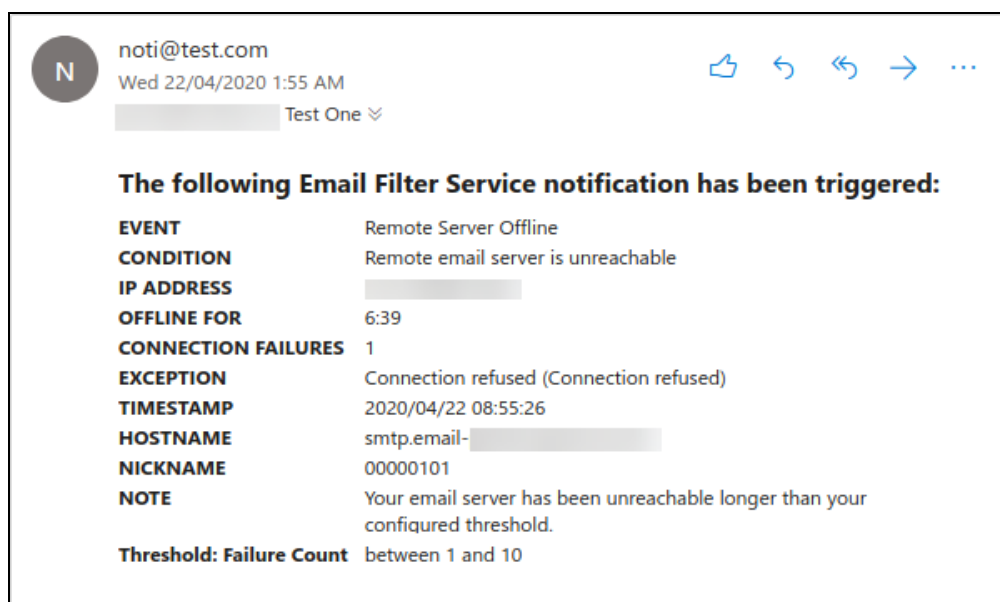
- asterisk or star (*) - matches the preceding token zero or more times. For example, the regular expression 'to*' would match words containing the letter 't' and strings such as 'it', 'to' and 'too', because the preceding token is the single character 'o', which can appear zero times in a matching expression. The regular expression 'f[aio]*t' would match the words 'fat', 'fit', 'fait', 'fiat', and 'foot' because the preceding token is the character class consisting of any of 'a', 'i', or 'o'.

- plus sign (+) - matches the preceding token one or more times. In contrast to the example given in the previous bullet, the regular expression 'to+' would only match words containing the character sequences 'to' and 'too', because the preceding token is the single character 'o', which must appear at least once in a matching expression. The regular expression 'f[ai]o+t' would match words containing the character sequences 'fit', 'fat', 'fait', 'fiat', and 'foot' because the preceding token is the character class consisting of any of 'a', 'i', or 'o', and at least one character from that character set must be present to match the regular expression.
 - question mark (?) - identifies the preceding character as being optional. For example, the regular expression 'too?' would match words containing the character sequences 'to' and 'too'.
 - vertical bar or pipe (|) - separates tokens, one of which must be matched, much like a logical OR statement. For example, the regular expression 'fa|i|ot' matches words containing the character sequences 'fa', 'i', 'fat', or 'fit' because it can be viewed as any of 'fa' or 'i' or 'ot', or the sequence 'f and (a or i or o) and t'. Any portion of a regular expression that uses the '|' symbol is often enclosed in parentheses to disambiguate the tokens to which the '|' applies. (See the next bullet for an example.)
 - open and close round bracket or parenthesis ('(' and ')') - groups multiple tokens together to disambiguate or simplify references to them. For example, the regular expression 'f(a|i|o)t' matches words containing the character sequences 'fat' or 'fit' but not the word 'fa', because matching sequences must now consist of three characters where the middle character has been restricted to being one of the letters 'a or i or o'.
 - open square bracket ([) and close square bracket (]) - enclose specific characters or a range of characters to be matched. The characters enclosed inside square brackets are known as a character class. For example, the regular expression 'f[i]o[rm]' will match words containing the character sequences 'firm' and 'form', but will not match any other word containing other sequences that begin with 'f' and ending with 'rm'. A character class only matches a single character unless it is followed by another character that has special meaning in a regular expression.
 - caret (^) - the caret has two different meanings in a regular expression, depending on where it appears:
 - As the first character in a character class, a caret negates the characters in that character class. For example, the regular expression 'f[^io]rm' will match any word containing a sequence of characters beginning with 'f' and ending with 'rm', except where either 'i' or 'o' is the second character. It will therefore match words containing the character sequence 'farm', but not words containing the sequences 'firm' or 'form'.
 - As the first character in a regular expression, a caret identifies the beginning of a term. In this context, the caret is often referred to as an anchor character.
 - dollar sign (\$) - as the last character in a regular expression, a dollar sign identifies the end of a term. In this context, the dollar sign is often referred to as an anchor character.
-  **Note:** Anchor characters are very important if you want to restrict regular expression matches to entire words. For example, the regular expression 'f[air]rm' will match words containing any of the strings 'farm', 'firm', and 'form', including words such as 'farmer', 'infirm', 'former', and 'conform', while the regular expression '^f[air]rm' will only match the words 'farmer' and 'former' from these examples, and the regular expression '^f[air]rm\$' will only match the words 'farm', 'firm', and 'form'.
- backslash (\) - used to invoke the actual character value for a metacharacter in a regular expression. For example, the regular expression 'Comin?' will match the words 'Coming', 'Comint', and the question 'Comin?'. The regular expression 'Comin\?' will only match the question 'Comin?'

Regular expression syntax also supports a number of special character sequences to match non-printable characters, special character classes such as digits and alphabetic characters, and so on. Discussing complete regular expression syntax is outside the scope of the Watson Explorer Engine documentation. For a complete discussion of regular expressions, see the [Regular Expressions Information](#).

A notification email message is sent on a specific event. You define which events trigger notifications, how often the notification is sent for the event, event thresholds, and the message recipient. You can also receive text message notifications using your wireless provider's email SMS feature.

You set notifications in the Administrator Dashboard. Available event types display based on your Admin role. Notifications contain information about the event type based on conditions. This example email notification shows the information returned on a Remote Server Offline event.



The screenshot shows an email notification interface. At the top left is a circular profile icon with the letter 'N'. To its right is the sender's email address 'noti@test.com' and the timestamp 'Wed 22/04/2020 1:55 AM'. On the right side of the header are icons for thumbs up, reply, reply all, forward, and a more options menu. Below the header is a recipient name 'Test One' with a dropdown arrow. The main body of the email contains a bold heading: 'The following Email Filter Service notification has been triggered:'. Below this heading is a list of event details in a key-value format:

EVENT	Remote Server Offline
CONDITION	Remote email server is unreachable
IP ADDRESS	[REDACTED]
OFFLINE FOR	6:39
CONNECTION FAILURES	1
EXCEPTION	Connection refused (Connection refused)
TIMESTAMP	2020/04/22 08:55:26
HOSTNAME	smtp.email-[REDACTED]
NICKNAME	00000101
NOTE	Your email server has been unreachable longer than your configured threshold.
Threshold: Failure Count	between 1 and 10

Adding a Notification

Add New >> Notification

1. Enter the **Subject**. This is the notification name, and appears in the Subject field of the message.

2. Select the **Event Type** that triggers the notification message.





Note: Available event types are role dependent.

Event type	Event Occurs When...
Outbound Deferred Messages	Filtered messages are waiting to be delivered to the mail gateway or the Internet.
Remote Server Offline	The system cannot successfully connect to the destination mail gateway.
Inbound Hourly Traffic	The number of messages that enter the server for filtering from the Internet exceeds the per-hour limit.
Outbound Hourly Traffic	The number of messages that leave the server for the Internet or mail gateway exceeds the per-hour limit.
Sender Rate Limit	The sender rate exceeds the limit.
Recipient Rate Limit	The recipient rate exceeds the limit.
Email Continuity Enabled/Disabled	Email Continuity is automatically enabled or disabled.
Latency Warning	The average time between message and its readiness for delivery exceeds five minutes.

Event type	Event Occurs When...
ThreatTest Email Submissions	Email messages are submitted to ThreatTest and exceed the Count condition.
ThreatTest Email Confirmations	Email messages are confirmed by ThreatTest and exceed the Count condition.

3. Enter the sender email address. This address appears in the From field of the sent message.
4. Enter the recipients of the notification message; only one recipient per line. These can be regular email addresses or text addresses. Use the following formats for text messaging (where, *phonenumber* is the recipient's mobile number):

Carrier	Address format
AT&T	phonenumber@txt.att.net
AT&T MMS	phonenumber@MMS.att.net
Metro PCS	phonenumber@MyMetroPcs.com
Sprint	phonenumber@messaging.sprintpcs.com
T-Mobile	phonenumber@tmomail.net
US Cellular	phonenumber@email.uscc.net
Verizon	phonenumber@vtext.com
Virgin Mobile	phonenumber@vmobl.com

5. Set **Frequency** to the minimum amount of time between resending notifications for this event.
6. Select the **Account** to monitor.
7. Select the conditions that generate a notification. Options vary depending on event type. For each condition:
 - Select the condition, and click  to add it to the notification. Click  to remove the condition.
 - Enter applicable values.

This screenshot demonstrates adding the Count and OutboundIP conditions to an Outbound Deferred Messages event type.

These are the possible conditions:

Condition	Description
Action	The action taken by the filter on a message.
Category	The message category determined by the filter.
Count	The number of times the item measured must occur before triggering the notification event.
Domain Name	Limit event generation to particular domains.
Enabled	The feature being monitored is turned on.
Failure Count	The number of times the item measured must fail before triggering the notification event.
IP Address	Limit which sending IP addresses to include in event generation by specifying them.
# of Messages	The number of messages that must pass through the filter before triggering the notification event.
Offline Duration	The minimum amount of time that connection attempts to a server must fail before generating a notification event.
Outbound IP	Limit which Outbound IP to include in event generation by specifying them.
Recipient Email	Limit which messages to include in event generation by including only those sent to specific recipients.

Condition	Description
Sender Email	Limit which messages to include in event generation by including only those sent by specific senders.
Size	Limit which messages to include in event generation by including only those in a particular size range (in bytes).

8. Click **Add**.

Units of Measurement

Use these units of time for **Offline Duration**:

w - week
d - day
h - hour
m - minute
s - second
hh:mm:ss.frac

Examples:

1w 3d = 1 week and 3 days (space required)
1:40.35 = 1 min, 40 and .35 seconds
1400 = 1400 milliseconds

Use these units for **Size**:

Ki = 2¹⁰ = 1024
K = 10³ = 1000
Mi = 2²⁰ = 1048576
M = 10⁶ = 1000000
Gi = 2³⁰ = 1073741824
G = 10⁹ = 1000000000
Ti = 2⁴⁰ = 1099511627776
T = 10¹² = 1000000000000

Example:

4.3K = 4.3 * 1000 = 4300

Editing a Notification

Manage >> Notifications >> {Notification}



Tip! Select **Manage >> Notifications >> more >>** to display a list of all notifications. Click the notification link to edit conditions for that event. Click **Delete** to remove the notification.

1. Change the settings.
2. Click **Update**.



Note: You cannot change the account information or the event type. Instead, create a new notification and then delete the original notification.

Manage >> Notifications >> {Notification}

1. Click **Delete**.
2. Click **Delete** again in the confirmation pop-up window.

Bulk Operations allow you to apply settings to multiple domains, outbound IP addresses, or mailboxes on one page within the accounts you manage. Change an option in Bulk Operations to immediately apply that setting to the selected domains, outbound IPs, or mailboxes.



Note: Options set in Bulk Operations settings pages override individual settings. To preserve the current setting, do not select an option from the drop-down menu (leave the option "blank"). This allows you to change some options for multiple domains, outbound IP addresses, or mailboxes, but keep any individual settings.

Bulk Domain Settings

You can configure domain-level settings for multiple domains at one time. Then you can customize settings for each domain and mailbox as needed.

Manage >> Bulk Operations >> Bulk Domain Settings

The settings selected on this page are applied to the domain(s) selected in the Choose Domains section.

To select domains:

1. Filter the domains list using any of the following methods:
 - Click **Select All** to select all domains.
 - Enter text in the Search box.
 - Select a specific account.
2. Use the arrow buttons to move domains from the **Available** list to the **Selected** list.

To permanently delete the selected domains:

1. Click **Delete Selected** in the Choose Domains section.
2. Click **OK** to confirm the deletion.

To change domain settings:

1. Change each setting as needed. Settings are explained in the [Domain Settings](#) section.
2. Click **Update Section** to apply the settings to the selected domains.

Bulk Outbound Settings

You can configure outbound IP-level settings for multiple outbound IPs at one time. Then you can customize settings for each outbound IP as needed.

Manage >> Bulk Operations >> Bulk Outbound Settings

The settings selected on this page are applied to the outbound IP(s) selected in the Choose Outbound IPs section.

To select outbound IPs:

1. Filter the outbound IPs list using any of the following methods:
 - Click **Select All** to select all outbound IPs.
 - Enter text in the Search box.
 - Select a specific account.
2. Use the arrow buttons to move outbound IPs from the **Available** list to the **Selected** list.

To permanently delete the selected outbound IPs:

1. Click **Delete Selected** in the Choose Outbound IPs section.
2. Click **OK** to confirm the deletion.

To change outbound IP settings:

1. Change each setting as needed. Settings are explained in the [Outbound IP Settings](#) section.
2. Click **Update Section** to apply the settings to the selected outbound IPs.

Bulk Mailbox Settings

You can configure mailbox-level settings for multiple mailboxes at one time. Then you can customize settings for each mailbox as needed.

Manage >> Bulk Operations >> Bulk Mailbox Settings

These settings apply to the mailboxes selected in the Choose Mailboxes section.

To select mailboxes:

1. Filter the mailboxes list using any of the following methods:
 - Click **Select All** to select all mailboxes.
 - Enter text in the Search box.
 - Select a specific domain
 - Select a specific account.
 - Select the mailbox status.
2. Use the arrow buttons to move mailboxes from the **Available** list to the **Selected** list.

To permanently delete selected mailboxes:

1. Click **Delete Selected** in the Choose Mailboxes section.
2. Click **OK** to confirm the deletion.

To change mailbox settings:

1. Change each setting as needed. See [Configuring Individual Mailboxes](#) for option definitions.
2. Click **Update Section** to apply the settings to the selected mailboxes.

The Reporting features generates account-level statistical information reports for inbound and outbound connections and messages for both appliance and hosted customers. Additionally, system administrators have access to system-wide reporting.

Running a Report

The interfaces and options vary by report and whether your account is hosted or you have an appliance. Some of the steps in the following procedures may not apply to all reports.

Inbound messaging supports reports for categories for a given domain and advanced reporting for one or more domains.

Reports >> {Report Name}

1. Select the domain or outbound IP.

You can also choose All Inbound Domains, All Outbound IPs, or Outbound Authenticated Relay (senders who are not in any of the defined outbound IP ranges).

2. Select additional options, depending on the report.
3. Click **Run**. The report runs and displays on the screen.

While viewing a report:

- Some reports can be sorted by column. See [Sorting Report Data](#) for details.
- You can download the data in .csv format for use with Excel or another spreadsheet application for sorting and data analysis. See [Downloading Report Data](#) for details.
- You can resend a message to the recipient or the sender. See [Releasing Messages](#).

For reports that return a list of messages:

- To see a preview of a message, click the **View** link next to the message.

Sorting Report Data

Some reports can be sorted by column. Where this is available, the sort order is indicated by arrows next to the column name.

- Click a column name to sort the data.



The double arrow indicates you can sort on the column.

- ▼ The down arrow indicates the data is sorted by this column, in ascending (lowest to highest) order.
- ▲ The up arrow indicates the data is sorted by this column, in descending (highest to lowest) order.

- You can shift + click on another column name to do a secondary sort.

Releasing Messages

Reports that generate a list of messages provide the additional capability to resend the messages to either the recipient or the sender.

To resend messages:

1. Run the report.
2. Select the messages to resend.
 - Select the **All** checkbox to resend all messages listed.

OR

- Select checkboxes next to individual messages

3. Resend the messages.
 - Click **Release** to resend messages to the recipient.

OR

- Click **Release to Sender** to send messages to the sender.

The **Release** and **Release to Sender** options are also available from the Preview Message window.

Downloading Report Data

Reports are shown on the screen in table format. All reports offer the option, once they're displayed, to download the data. When you download the data, all records that meet your selected criteria are included, even if the number exceeds the maximum you entered for display.

Data is downloaded in .csv format so that it can easily be opened in Excel or another spreadsheet application for sorting and data analysis.

To download report data:

1. Run the report.
2. Click **Download**.



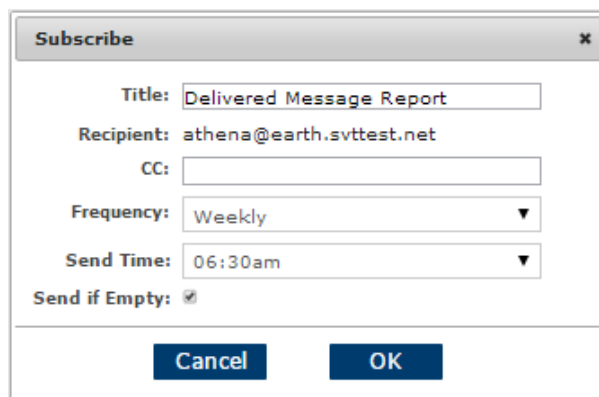
Note: Reports are saved to a file named ReportData.csv. You can rename the file as needed.

Subscribing to a Report

Administrators can subscribe to inbound and outbound reports. When subscribed, the configured report is emailed daily or weekly to the subscriber's email address. Reports are sent as attachments in .csv format; small reports are also contained in the body of the email message. You can unsubscribe from a report at any time.

To subscribe to a report:

1. Run the report.
2. Click **Subscribe**.



The screenshot shows a 'Subscribe' dialog box with the following fields and values:

- Title: Delivered Message Report
- Recipient: athena@earth.svttest.net
- CC: (empty)
- Frequency: Weekly
- Send Time: 06:30am
- Send if Empty:

Buttons: Cancel, OK

3. If you want to rename the report, type in the new name.
4. If you want to specify additional recipients to receive a copy of the report, enter them in the cc list. Separate multiple email addresses with a comma (,).
5. Select the report frequency.
6. Select the time of day when you want to receive the report.



Note: The report will contain data for the time period ending 1-2 hours before the send time. Early morning is 1:30am.

7. If you want to always receive the report, even when there is no data in it, select the checkbox.
8. Click **OK**.

Reports

The following reports are available.

Charts	Charts show data in graphical format and are available for many of the statistics within the system.
Advanced Report	Customizable report providing all possible details relating to messaging for up to 35 days.
Delivered Message Report	If you have enabled the storage of legitimate mail on the server and selected “Keep a copy of messages delivered to the Mail Gateway” (see Routing and Session Management), Delivered Message reports are available for up to 35 days.
Deferred Queue Report	List of messages stored in the deferred queue.
Instant Spam Digest	Spam Digest for one or more users.
Message Category Summary	Summary of messages by category (spam, phishing, etc) and action.
Message Handling Summary	List of messages that have passed through the system over the previous 3 years, by month and action.
Quarantine Report	List of quarantined messages. Messages can be viewed or released directly from the report. Quarantined emails are available for viewing for up to 35 days from the time of processing.
DLP Activity Report	List of messages that were sent (or quarantined) through the encryption service.
Top Senders Report	List of the users who have sent the most mail over the last 24 hours. This report is available for up to 35 days.
Encrypted Attachment Report	Lists messages that have been sent as encrypted attachments. Use this report to change the expiration date of a message.
Audit Trail	Lists all configuration changes made by administrators on the Administrator Dashboard and by end users on their Personal Dashboards.
ThreatTest Report	Lists all messages submitted to the ThreatTest service, including status and categorization.
ThreatTest Summary Charts	Shows ThreatTest data in graphical form.

Charts

Charts show data in graphical format and are available for many of the Email Security product statistics.

Reports >> Charts

- Select the chart type:
 - Message Category: either Month to Date (MTD) or Year to Date (YTD)
 - Inbound Traffic: last 24 hours or Month
 - Outbound Traffic: last 24 hours or Month
 - Top Recipients

- Top Spam Recipients
 - Top Spam IPs
 - Top Outbound Senders
 - Top Outbound Senders by Size
2. Select the domain or outbound IP to be included.
 3. If available (depends on the chart selected), choose the number of days to be shown.
 4. Click **Run**. The chart displays on the screen.

Post-Run Options

After you generate the Inbound Traffic or Outbound Traffic charts, you can download the data that created the chart by clicking on the **Download** button to the right of the Run button. This creates a .csv file on your local machine.

You can also subscribe to the data generated by these reports by clicking on the **Subscribe** button at the top of the chart.

Options for subscribing include:

- Title. This defaults to the chart title.
- Recipients to add as CCs on the subscription email.
- Frequency: Choose daily, weekly, or monthly.
- Cutoff Time: Choose the option you prefer.
- Send if Empty: The chart data will be mailed even if there is no data for the time period you selected as the Frequency.

Advanced Report

The Advanced Report is highly customizable, providing all possible details relating to messaging for domains or outgoing IPs for up to 35 days. To sort the data you can click on a heading, then shift-click on another heading to sort within the initial sort.



Notes:

System reports time out after two (2) minutes and return no results. Tailor your report queries to the specific information you want to analyze.

Administrators can only view headers, not the content, of legitimate messages.

Administrators can release legitimate messages in the same way as quarantined messages (if Keep a copy of delivered messages is enabled).

When you run the Advanced Report, in addition to specifying a domain or outbound IP, you can also:

- Select a time/date or range.
- Filter the data by
 - Message ID
 - Senders
 - Domains: Check the MIME box to include searching by MIME sender.
 - Recipients: Specifying any recipient will include all aliases for that recipient.

- **Subject:** Text strings in the subject line in advanced reports are case-sensitive. If you do not find the results you expect, try varying the case of the search terms
- **Attachments:** Multiple attachments on a message will be indicated by a "...". You can then click on that field to see a list of all attachments for that message.
- **Maximum number of records to show on the screen.** The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Choose the categories to include.
- Choose which actions to include:
 - **Accept:** shows emails that successfully passed through all active filters and were delivered to recipients.
 - **Allow:** shows emails that skipped over one or more filters, because those filters were set to Allow. For example, if the Junk category is set to Allow, then specifying Allow in this report would display all Junk emails that have been allowed to be delivered to recipients.
 - Bcc
 - Block
 - Encrypted
 - Markup
 - Quarantine
 - Special Routing
 - Strip
- Choose which dispositions to include:
 - All
 - Deferred
 - Delivered
 - Bounced
 - Encrypt Override
 - Route Override
 - Delivered BMOD
- Choose the layout (which columns to include). The Details column can be used to show additional information about an email.

**Notes:**

To include all categories, actions, or dispositions, use the All checkbox. To choose which of these options to include, deselect All and then select the options you want.

Delivered Message Report

This report allows the user to track and optionally resend legitimate messages to the recipient if the option "Keep a copy of messages delivered to the Mail Gateway" is enabled. Delivered Messages reports are available for up to 35 days. While viewing the report, you can click on a heading to sort the data.

Reports can be viewed for the entire mail domain or a specific set of users. Administrators can have a report automatically generated and delivered daily, weekly, or monthly.



Notes:

Administrators can only view headers, not the content, of legitimate messages. This report only includes messages that come through while the Keep a copy of messages delivered to the Mail Gateway option is checked.

When you run the Delivered Message Report, in addition to specifying a domain or outbound IP, you can also:

- Select a time/date or range.
- Filter the data by senders, recipients, subjects, and/or attachments. Specifying any recipient will include all aliases for that recipient. When viewing the report, multiple attachments on a message will be indicated by a "..." and you can then click on that field to see a list of all attachments for that message.
- Specify the maximum number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Choose the layout (which columns to include).

Deferred Queue Report

The Deferred Queue report gives a detailed view of outgoing mail that is being held in the queue, for up to seven days.

When you run the Deferred Queue Report, in addition to specifying an outbound IP, you can also:

- Filter the data by senders, recipients, and/or sender or recipient domain, and specify the maximum number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).

Deferred Queue Summary

The Deferred Queue Summary report lists totals, for each domain, of how many messages are currently on the server waiting to be delivered. Delivery has been attempted at least once. The domains are both internal and external (i.e., the messages are headed for the admin's mail server or the Internet).

Instant Spam Digest

Administrators can generate an Instant Spam Digest on demand. The digest is emailed directly to the named user. Spam digests are available for up to 35 days.

When you run the Instant Spam Digest:

- Enter the recipient address.
- Select a time/date range (optional).

Message Category Summary

This report summarizes incoming and outgoing messages for one or multiple domains or outbound IPs.



Note: Messages that have passed through the system unfiltered are shown in the Relay category.

When you run the Message Category Summary, in addition to specifying a domain or outbound IP, you can also:

- Select a time/date range. You can run this report for today, yesterday, the current month to date, any of the previous three months, the current year to date, or any of the previous four years. The default report time span is month to date.

Message Handling Summary

Any Administrator Dashboard administrator can generate a report that shows the total quantity of email messages processed per month for the previous 3 years. This report also shows the action performed on the messages.

Quarantine Report

Quarantined messages are the messages that the system has filtered out based on your filtering options. Quarantine Reports can be viewed for the entire mail domain or a specific set of users. Administrators can have a report automatically generated and delivered daily, weekly or monthly.



Note: Quarantined emails remain in the system for up to 35 days from the time of processing. During this time they show on this report, and they are available for viewing, release from quarantine, or deletion.

When you run the Quarantine Report, in addition to specifying a domain or outbound IP, you can also:

- Select a time/date range.
- Filter the data by senders, recipients, subjects, and/or attachments. Specifying any recipient will include all aliases for that recipient. When viewing the report, multiple attachments on a message will be indicated by a "... " and you can then click on that field to see a list of all attachments for that message.
- Select the type of quarantine (admin or user).
- Specify the maximum number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Choose the categories to include.



Note: To include all categories, leave the All checkbox selected. To choose specific categories to include, deselect the All checkbox and then select the categories.

- Choose the layout (which columns to include).

In addition to the standard option (release, download, subscribe), the Quarantine report provides the option to delete a message from the quarantine. To delete a message:

- Select the checkbox next to the message and then click **Delete**.

DLP Activity Report

The DLP Activity Report lists messages that have been acted upon by the DLP filters, Compliance-Health and Compliance-Finance.



Note: Quarantined emails remain in the system for up to 35 days from the time of processing. During this time they show on this report, and they are available for viewing and release from quarantine.

When you run the DLP Activity Report, in addition to specifying an outbound IP, you can also:

- Select a time/date range.
- Filter the data by senders, recipients, and/or subject, select the message action or disposition, and specify the maximum number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Choose the layout (which columns to include).

Top Senders Report

This report lists the top senders in your system for up to 35 days.

When you run the Top Senders report you can:

- Select a single outbound IP or all.
- Select a time/date range.
- Specify the sender's domain.
- Select how many top senders to list, up to 1000.
- Show the top senders of all, or only delivered messages.
- Show the top senders who were flagged for compliance (health, finance, or profanity).
- Show a sample message subject for each sender.

Encrypted Attachment Report

The Encrypted Attachment Report lists messages that have been sent as encrypted attachments. Use this report to change the expiration date of a message. The recipient cannot view a message past its expiration date.

When you run the Encrypted Attachment Report, in addition to specifying an outbound IP, you can also:

- Select a time/date range.
- Filter the data by senders, recipients, and/or subject, and specify the maximum number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Choose the layout (which columns to include).

While viewing the report, you can change the expiration date for any of the messages on the report.

1. Click **Edit** next to the message.
2. Enter a new **Expire Date** or click **Expire Now** to immediately delete the message.
3. Click **OK**.

Audit Trail

This report lists all changes made by administrators on the Administrator Dashboard and users on their Personal Dashboard. The list can be filtered by account, domain or mailbox and also by the ID of the administrator that made the change.

You can run this report for any time within the last year. The default report time span is yesterday and today.



Note: The amount of time audit log records are stored in the system is configurable. See Administrator Dashboard Preferences for details.

When you run the Audit Trail, in addition to selecting the date range, you can:

- Enter an account name. The query will match on the last account it finds that contains the text specified in this field. For example, if the account parameter is "earth" and there are two existing accounts, earth1 and earth2, the query will match on earth2 only. If no account names match, this parameter is ignored. This parameter is case-insensitive.
- Enter either a domain name or a mailbox name (not both).
- Enter a user ID.
- Limit the number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).

Mailbox Report

This report provides a count of all added, removed, and unprotected mailboxes. It also lists each mailbox that has failed discovery.

You can run this report for any time within the last year. The default report time span is yesterday and today.

When you run the Mailbox Report, in addition to selecting the date range, you can:

- Enter an account name and/or a domain name.
- Filter the data by domain, mailbox, user id, and/or specify the maximum number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Subscribe to the report.

ThreatTest Report

This report lists all messages submitted to the ThreatTest service.

You can run this report for any time within the last 35 days. The default report time span is the current day.

If you have the ThreatTest Add-in and the report shows no results, you can see your ThreatTest usage by logging in to [ThreatTest](#).

When you run the ThreatTest Report, in addition to selecting the date range, you can:

- Filter the data by sender(s) and subject, and/or specify the number of records to show on the screen. The maximum is 10,000. If you need to see more data, you can download the report to a .csv file after running it (all data will be included in the download).
- Choose the categories to include.
- Choose the layout (which columns to include).
- Subscribe to the report.

ThreatTest Summary Charts

ThreatTest summary charts show ThreatTest data in graphical format.

Reports >> ThreatTest Summary Charts

1. Select the chart type.

2. Select the domain or outbound IP to be included.
3. If available (depends on the chart selected), choose the number of days to be shown.
4. Click **Run**. The chart displays on the screen

If you have the ThreatTest Add-in and the report shows no results, you can see your ThreatTest usage by logging in to [ThreatTest](#).

CHAPTER 14 Brand Preferences

System administrators can customize the appearance of the end-user Personal Dashboard and Administrator Dashboard through the Administrator Dashboard.

There are three sections of Dashboard content:

- [Personal Dashboard Preferences](#)
- [Administrator Dashboard Preferences](#)
- [Branding Preferences](#)

Account administrators and system administrators can customize some settings for each account. These include the appearance of the end-user Personal Dashboard and the spam digest. See [Account Preferences](#) for details.

Personal Dashboard Preferences

System Administrators use these settings to define the appearance of the Personal Dashboard.

Manage >> Brand Preferences >> Personal Dashboard

1. For each screen element, enter a value or select the checkbox.
2. Click **Update**.

General Settings

These settings determine the overall look of the Personal Dashboard, including what links are displayed and whether or not access is provided to the low-bandwidth version.

Option	Description
Login ID label	Text displayed on the login page to the left of the first text box. You can specify text for each available language.
Display "About" link	Goes to the Personal Dashboard about screen.
Display "Help" link	Goes to a context-sensitive pop-up help window.
Display "Change Password" link	Allows users to change the Personal Dashboard password.
Display "Logout" link	Logs the user out of the Personal Dashboard.

Display "Signup" link	Link on the Personal Dashboard login page to create a login ID and password.
Display "Forgot Password" link	Emails the password to the given address.
Display link to PD light	Provides access to the other Personal Dashboard (high bandwidth links to low bandwidth, low bandwidth links to high bandwidth). Note that mobile users are automatically directed to the low bandwidth page.
Link to PD light label	Text that appears as the link to the low bandwidth version of the Personal Dashboard.

Policies Tab

These settings determine if the user can view friends and enemies list for the domain.

Option	Description
Display domain's friends list	Allows the user to view the domain friends list
Display domain's enemies list	Allows the user to view the domain enemies list

Inbound and Outbound Preview Message Page

These settings define what the user sees when previewing a message from the inbound or outbound quarantine list.

Option	Description
Display "Personal Dashboard" link	Goes to the Personal Dashboard.
Custom header content	Text you enter here appears at the top of the message preview window. You can specify text for each available language.
Display "Logout" link	Logs the user out of the Personal Dashboard.

Administrator Dashboard Preferences

System Administrators use these settings to define the appearance of the Administrator Dashboard.

Manage >> Brand Preferences >> Admin Dashboard

1. For each screen element, enter a value or select the checkbox.
2. Click **Update**.


Configurable options for the Administrator Dashboard are:

Option	Description
Use GoSecure MX record format	Select the checkbox to validate your MX record format; clear the checkbox to disable validation. Domains with invalid records have an ! displayed next to the name in the Domain list.
Outbound status message	Enter the text to display on the Outbound Status page. Click html if you want to format the message using HTML instead of plain text.
Domain status message	Enter the text to display on the Domain Status page. Click html if you want to format the message using HTML instead of plain text.
Domain status address	Enter the addresses to be listed with the domain status message.
Audit log retention	Enter the number of days that audit log records should be stored.
Display Appliance Dashboard link	Leave this checkbox selected if you want the appliance dashboard to appear on the dashboard landing page. To remove it from the list on this page, clear the checkbox.

Branding Preferences

Configurable branding options allow the system administrator to upload custom logos and banners, configure Personal Dashboard banner links, and customize the appearance of the spam digest.

Manage >> Brand Preferences >> Branding

- For each screen element you can do any of the following:
 - Enter a value or select the checkbox to enable it.
 - Click **Browse...** to select a file.
 - Click the download icon  to save the file listed.
 - Clear the text or the checkbox to disable the option.
 - Select the **Reset** checkbox to reset the option to the system default.
- Click **Update**.

Dashboard Logos

These settings enable you to customize the icons and logos on dashboards.

Option	Description
Application icon	The favorites icon (also known as the favicon or website icon) used in the browser address bar and in the list of bookmarks. Must be in Windows icon 16 x 16 pixel format. Note: You are advised to clear your browser cache to insure the display of the current icon and to test the display on all browser types.
Admin dashboard logo	The banner that displays on the top of the Administrator Dashboard. Must be in .gif format 760 x 77 pixels.
Personal dashboard logo	The banner that displays on the top of the Personal Dashboard. Must be in .gif format 598 x 97 pixels. The bottom 24 pixels must be transparent.
Personal dashboard background fill	A repeated background file that tiles to the right of the logo file and is used as the background for text. Must be in .gif format 97 pixels high and a minimum of 1 pixel wide.
Right justify PD logo	Positions the logo for the Personal Dashboard on the right side. Leave this unchecked to position the logo on the left side.
PD menu font color	Sets the foreground color of the menu on the Personal Dashboard. The menu overlays the logo so you should select a color that is not similar or the same as the color of the logo itself.
Admin dashboard logo area color	Sets the background color of the logo area for the Administrator Dashboard.

Dashboard Content

These options set the URL for dashboards, as well as providing links to help-oriented locations.

Option	Description
Dashboard URL	The URL of the Administrator and Personal Dashboards.
Dashboard URL defaults to the Personal Dashboard	Checking this box sets the default dashboard URL to be that of the Personal Dashboard. When a user logs in, they will go directly to the Personal Dashboard.
Personal Dashboard banner link	The link to the Personal Dashboard banner. Use a valid URL.
Dashboard Help URL	The link to the Admin Dashboard help. Use a valid URL.
Help demo link	Specifies whether the help pages have a link to a demo video.

Help FAQ link	Specifies whether the help pages have a link to the Personal Dashboard FAQ.
Help FAQ link URL	The link to the Personal Dashboard help FAQ. Use a valid URL.
Display Google 3rd party authentication	Display the Google third-party authentication in the Dashboards.
Display Microsoft 3rd party authentication	Display the Microsoft third-party authentication in the Dashboards.
Include Google reCaptcha	Includes Google Captcha code in the login page.

Spam Digest Settings

These options set up how the digest will look and enable you to customize the welcome text sent to new users.

Option	Description
Digest Logo	The logo displayed on the upper left corner of the Spam Digest. Must be in .gif format 160 x 42 pixels.
Digest sender address	The sender address for all automated messages, including the Spam Digest.
Digest sender name	The prefix to be applied to the digest sender address. You can specify a prefix for each available language. The default is \$[period] Digest, where \$[period] the current frequency of the digest. For example, if the digest is sent daily, this field will display "Daily Digest" in this field.
Message subject	Customize the display of the subject in the Spam Digest. You can specify a subject for each available language. You can also customize the subject to include the recipient's name by adding \$[recipient] to this text box. For example "Spam Digest for \$[recipient]" will display "Spam Digest for bill@acme.net" when the Spam Digest is sent to that user.
Welcome text	Customize the text of the welcome message the user receives with the first Spam Digest. You can specify text for each available language.
Include "My Account" link	The link in the digest that takes the user to the Quarantine page of their Personal Dashboard.
My Account	Customize the text of the My Account link. You can specify the link text for each available language.
Include "Settings" link	The link in the digest that takes the user to the Policy page of their Personal Dashboard.

Include "Support" link	The link in the digest that opens an email message from the user's default program addressed to the defined tech support address.
Technical support address	The email contact for technical support. This is shown in the Spam Digest and other notifications.
Columns	Select which data appears in the Spam Digest, and the order of the columns. Note: If the Direction column is included here, the Domain Settings page includes an option for selecting whether outbound spam is included in the digest.
Include "Unsubscribe" link	Adds a link in the digest that the user can click to unsubscribe from the Spam Digest.
Include "Report Spam" link	Adds a link in the digest that takes the user to the GoSecure Web site describing methods for reporting spam.
Include "Change Report Frequency" link	The link in the digest that takes the user to the Personal Settings page of their Personal Dashboard.
Include "Feedback" link and text box	Takes user to the URL specified below this setting. You can provide a feedback form or mechanism at that URL location.
Header text	Add explanatory text at the top of the Spam Digest. You can specify text for each available language.
Footer text	Add explanatory text at the bottom of the Spam Digest. You can specify text for each available language.

Authentication

These settings control the dashboard timeout period, password expiration, CAPTCHA usage, and how passwords must be configured.

Option	Description
Dashboard inactivity timeout	The number of minutes before the dashboard returns to the login screen.
Expire password	The number of days before a user must specify a new password.
Protect accounts with captcha	The number of failed tries that generates a captcha challenge.
Login password requirements	Specify the minimum number of characters, then select the appropriate checkboxes to specify the types of characters that are required in each password.

Account Preferences



Configurable branding options allow the administrator to upload custom logos and customize the appearance of the spam digest uniquely for each account in the system.

Manage >> Brand Preferences >> Account Preferences

1. Select the account and click the **Enabled** button.



Note: To disable account-specific branding, click the **Disabled** button.

2. For each screen element you can do any of the following:
 - Enter a value or select the checkbox to enable it.
 - Click  to select a file.
 - Click the download icon  to save the file listed.
 - Clear the text or the checkbox to disable the option.
 - Select the **Reset** checkbox to reset the option to the system default.
3. Click **Update**.

Account Branding

These settings control the icons and logos used in your Email Security product installation and in the Personal Dashboard.

Option	Description
Application icon	The favorites icon (also known as the favicon or website icon) used in the browser address bar and in the list of bookmarks. Must be in Windows icon 16 x 16 pixel format. Note: You are advised to clear your browser cache to insure the display of the current icon, and to test the display on all browser types.
Admin dashboard logo	The banner that displays on the top of the Administrator Dashboard. Must be in .gif format 760 x 77 pixels.
Personal dashboard logo	The banner that displays on the top of the Personal Dashboard. Must be in .gif format 598 x 97 pixels. The bottom 24 pixels must be transparent.
Personal dashboard background fill	A repeated background file that tiles to the right of the logo file and is used as the background for text. Must be in .gif format 97 pixels high and a minimum of 1 pixel wide.

Right justify PD logo	If you want the logo to appear on the right of the dashboard, select this checkbox.
PD menu font color	The color of the text on the menu.
Admin dashboard logo area color	The color to fill the area where the logo is placed.
Dashboard URL	The URL of the Personal Dashboard.
Personal Dashboard Banner Link	Specifies the URL the user will be redirected to when they click on the banner of the Personal Dashboard.
Display Google 3rd party authentication	Display the Google third-party authentication in the Dashboards.
Display Microsoft 3rd party authentication	Display the Microsoft third-party authentication in the Dashboards.
Include Google reCaptcha	Includes Google Captcha code in the login page.

Spam Digest Settings

These settings control the logo and other information for the Spam Digest.

Option	Description
Digest Logo	The logo displayed on the upper left corner of the Spam Digest. Must be in .gif format 160 x 42 pixels.
Digest sender address	The sender address for all automated messages, including the Spam Digest.
Technical support address	The contact address for technical assistance listed in the Spam Digest and other notifications.
Welcome text	Customize the text of the welcome message the user receives with the first Spam Digest. You can specify text for each available language.

X-headers are typically used to record status information about an email message. To assist administrators in evaluating email traffic, The Email Security product adds custom X-headers to its filtered email before routing it to the mail gateway or after releasing it from quarantine. The custom headers are:

- **X-MAG-PROFILE** (optional): the user or domain profile that defined the filter policy. This field is blank if the profile is system-defined.
- **X-MAG-FILTER**: the filter that flagged the message.
- **X-MAG-CATEGORY**: the full name of the category used (see [X-MAG-Category Descriptions](#))
- **X-MAG-INFO** (optional): category-dependent (may contain applicable information such as rule ID, virus name, friends/enemy entry, etc.)

X-MAG-Category Descriptions

ADULT	category used for RuleType PORN
ATTACHMENT	category used by AttachmentFilter
BOT	category used for RuleType BOT
COMPLIANCE	category used for RuleType COMPLIANCE
CREDIT	category used for CreditCardFilter
DEBOUNCE	category used by DebounceFilter, which discards bounces on blacklist (was: BLOCK)
DIGEST	category used by DigestFilter for digests and subscribed reports
FOREIGN	category used by LanguageFilter
JUNK	category used by RuleFilter for RuleType JUNK
KEYWORD	category used by ExpressionFilters
NDR	category used by NDRFilter
PHISH	category used for RuleType PHISH and PhishFilter
PROFANITY	category used for RuleType PROFANITY
RBL	category used by RBLFilter

RECIPIENT	category used by RecipientFilter for messages addressed to exceptional outbound recipients
RELAY	category used by RelayFilter (e.g., for unprotected or inactive users)
SENDER	category used by Sender Filters
SPAM	category used for RuleType SPAM
SPOOF	category used by Spoof, SPF, and Fuzz Filters
SSN	category used for SSNFilter
VIRUS	category used for RuleType VIRUS and VirusFilter

In the SMTP session, connections can be rejected in response to the RCPT TO command for several reasons. Conditions and their associated error codes and messages are listed below.

Condition	Error code	Message
Syntax issues	501	Syntax
Sequence issues	503	Sequence
Invalid domain	550	Relay
Invalid recipient	550	Rejected
Message too big	552	Size {<msg size>} > {<max size>}