Account Administrator's Guide

EdgeWave™

V9.0

ePrism Email Security Suite

(630) 759-9283
www.JIKOmetrix.net

AcctAdmin09.0.0.001

Contents

CHAPTER 1 Overview

This document is a general guide for planning, configuring, and operating the EdgeWave Email Security system. It describes the features and applications of the system, to assist administrators in effectively deploying the EdgeWave solution in their environment.

Overview of Services

EdgeWave offers a complete suite of email security services. The Email Security Suite 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.

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

- **Hosted**: With the hosted solution, EdgeWave 's customers do not install any client software. They do not need to modify any of their servers, or train their staff in the use of EdgeWave technology. You enjoy lower bandwidth costs, lower mail server utilization, and lower archival capacity demands.
- **Appliance**: EdgeWave offers a full family of ePrism appliances. The ePrism appliance leverages the resources of the EdgeWave Security Operations Center to provide redundancy and managed service.

Email Filtering (EMF)

The EdgeWave email filter provides email defense against internal and external threats such as spam, viruses, spyware, phishing schemes, identity theft, and other dangerous or offensive content. Our services include inbound/outbound Spam and Antivirus filtering, policy categorization and automated seamless directory integration. EdgeWave 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. EdgeWave '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 – We host the applications and infrastructure required to protect your organization in a fully managed solution requiring zero administration.
- Disaster recovery protection – EdgeWave Email Security spools all email for up to 160 hours, in case of unexpected events, so you never lose your business-critical email.
- Proactive monitoring – EdgeWave engineers continually monitor email processes to assure they are performing at peak efficiency.
- Zero Minute Defense – This feature assures that as soon as an emerging threat is identified, our engineers deploy a specific rule to block it. No other solution has it.
- TLS Encryption – Our TLS Encryption works by establishing 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 - EdgeWave'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 EdgeWave 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. It allows users to review blocked spam messages and release them to their email inbox.

EdgeWave '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. EdgeWave 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.

EdgeWave 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. Three key differentiators of the EdgeWave solution are:

- A managed appliance solution
- Industry-leading block rate without any IT staff maintenance
- Dynamic resource allocation and service redundancy

Archive

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

Continuity

Continuity is a service that enables continuous web-based email access, management, and use during planned or unplanned mail server outages. Continuity is enabled easily 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. 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. EdgeWave 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

Specifically, DLP checks the data as follows.

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 a name
- 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.

Documentation Conventions

Bolded 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}

Other Conventions

- All portal procedures other than logging into the system assume that you have already logged into the portal.
- All Administrator Dashboard procedures other than accessing the Administrator Dashboard assume that you have already accessed it.

- There are often several ways to navigate to a specific screen in the portal or Administrator Dashboard. For consistency, these procedures use the Navigation Tree in the portal and menus in the Administrator Dashboard as a starting point.

Supported Browsers

EdgeWave applications support the following Web browsers:

- Microsoft Internet Explorer version 10
- Mozilla Firefox version 20
- Safari version 6
- Google Chrome version 26

Reporting Spam to EdgeWave

Report any spam messages that have passed through the EdgeWave 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 EdgeWave Technical Support:

- Phone:
  - Toll Free: 877-355-0553
  - Direct: 858-676-5050
- Web form: http://www.edgewave.com/forms/support/email_security.asp

For EdgeWave sales or general inquiries, call 800-782-3762.

For ePrism appliance provisioning, call 1-866-778-5644 or 707-568-1300.

Additional Resources

The EdgeWave website provides the latest available documentation for the Hosted and Managed Appliance Email Security Solutions.

CHAPTER 2 Portal Overview

The EdgeWave portal provides administrators with a central location to view and manage their accounts and attendant service licenses. It also provides a front-end to the EdgeWave email filtering service Administrator Dashboard where email domains and mailboxes are managed. Each account administrator has a personal login identity with administrative rights to accounts and domains serviced by EdgeWave.

Note: There are two ways to access the Administrator Dashboard: through the portal or with a direct login. Logging in through the portal gives access to one account (the Accounts tab does not appear on the dashboard).

From the portal you can:

- Create and manage your online identity
- Add new accounts
- Update account information, including technical, administrative, and billing contacts
- Access the Administrator Dashboard

The portal contains the following areas:

1. Navigation Tree
2. Work Area
3. Navigation Icons

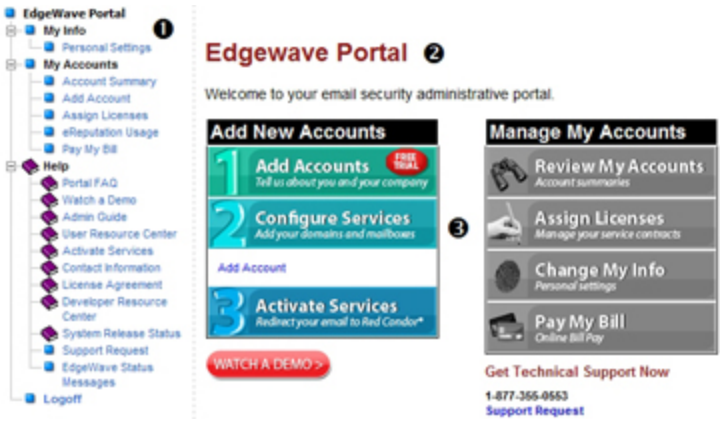

Figure 1. The Portal

Navigation Tree

The Navigation Tree acts like the portal table of contents. It is always visible, and provides quick links to all sections of the portal.

The **Portal** link on the top returns you to the portal home page.

The **My Info** link opens a page with your contact information and a place to change your portal password. This page also lists all of your accounts, and has a hyperlink to the detail pages for each account.

The **My Accounts** section contains links to view and configure the accounts that you have administrative permission for:

- The **Account Summary** page shows all of your accounts and details of their associated service licenses. It shows the type of license, and its start and expiration date. It has hyperlinks for each account detail page, and a hyperlink to configure services.

  Click on the Configure Services section to open a new browser window with the EdgeWave Administrator Dashboard for that account. From the Administrator Dashboard, you can administer domains and users for that account. When you have finished configuring services from the Administrator Dashboard, close the window to return to the portal.

- The **Add Accounts** page provides the form to add a new account. Provide the primary, technical, administrative, and billing contact information for the account.

- The account details links open the Account Details page for each individual account. Each page allows you to view and modify the primary, technical, administrative, and billing contact information for the account. It also shows the service licenses and users associated with the account.

The Help section contains the following links:

- **FAQ**: opens a very handy FAQ pop-up window to answer frequently asked questions
- **Watch a Demo**: opens a browser page with links to simulated demonstrations of the most frequently performed portal tasks.
- **Admin Guide**: A searchable HTML version of this manual.
- **Activate Services**: Gives a quick overview of how to activate EdgeWave email filtering services.

Use the **Logoff** button to close your portal session.

Work Area

The contents of the work area change depending upon the task you are working on. Upon entering the portal, the work area displays the welcome page that contains a welcome message. In the future it may contain news and security alerts.

Navigation Icons

The navigation icons provide quick access to the most common account administration tasks.

There are two sets of navigation icons:

- **Add New Accounts**: Tasks associated with adding, configuring, and activating account services:
  - **Add Accounts**: Links to the Add Accounts page. See Adding an Account for more information.
  - **Configure Services**: Existing accounts link to the Administrator Dashboard for domain configuration tasks. See Domainsfor more information.
  - **Activate Services**: Links to the Activate Services page for a quick overview of how to activate EdgeWave email filtering services.
- **Manage My Accounts**: Tasks associated with reviewing account information, assigning services licenses, and changing your personal information:

- **Review My Accounts**: Links to the Account Summary page that shows all of your accounts and details of their associated service licenses. It shows the type of license, and its start and expiration date. It has hyperlinks for each account detail page, and a hyperlink to configure services.
- **Change My Info**: Links to the Personal Settings page. See Changing Your Personal Information for more information.

Getting Started

Get started with the portal by logging into the system (portal.edgewave.com). First time users must register before accessing the portal.

Logging into the portal for the first time

The first time you log into the EdgeWave portal (portal.edgewave.com) you must register with the system. During registration, you enter your contact information and select a portal password.

EdgeWave requests your personal information in order to provide timely and accurate technical support. Please keep this information current so that we can serve you better. Be assured that we will keep all of your personal information strictly confidential.

Tip! Click **Watch A Demo** to see a simulation of the registration and login process in your browser.

To log in to the portal for the first time and register:

1. At the Login screen, click **Register** in the New Customers column. The registration welcome screen opens.
2. Complete the registration form and click **Register**. The Terms and Conditions screen opens. EdgeWave also sends a confirmation letter to your email address.
3. Read the terms and conditions, and click **Accept** to continue. The portal home page opens.

Logging into the portal after registration

After you have registered with the EdgeWave portal, log in as follows:

1. At the Login screen, enter your email and portal password in the text boxes in the Existing Customers column.
2. Click **Login**. The portal home page opens.

Changing Your Personal Information

You can change your personal contact information as circumstances require. EdgeWave strongly suggests that you keep this information current so that we can serve you better. You can also change your password as needed.

To change your personal information:

1. On the Navigation Tree, click **Personal Settings**. The Login Identity Details screen opens in the work area. Alternatively, click on the **Change My Info** navigation icon in the work area.
2. Edit the information as needed.
3. Click **Update Details** to save your changes.

To change your portal password:

1. On the Navigation Tree, click **Personal Settings**. The Login Identity Details screen opens in the work area. Alternatively, click on the **Change My Info** navigation icon in the work area.
2. Enter and re-enter your new password.
3. Click **Update Details** to save your changes.

Configuring Accounts

The portal is designed for account administration. An account represents a single company or organization. An account is the combination of the identity of your company (physical location) and its contacts with EdgeWave (primary, technical, administrative, and billing).

The creator of the account is automatically assigned the role of Account Administrator. An account can have one or more domains. Each domain can have one or many mailboxes. Each account must have a service license associated with it to become active.

CHAPTER 3 EdgeWave Administrator Dashboard

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

The Administrator Dashboard runs in a separate window than the portal.

Accessing the Administrator Dashboard

You can access to the Administrator Dashboard in one of three ways:

- **Portal Home Page**: Click **EdgeWave Portal** on the Navigation Tree to display the portal home page. The navigation icon **Configure Services** has a list of all your accounts.
  - Accounts with a green button have one or more valid licenses. Click on the account name to gain access to its configuration Administrator Dashboard.
  - Accounts with a red button do not yet have a service license associated with them.
- **Account Summary Page**: Click the link on the Navigation Tree to open this page that displays all of your accounts.
  - Accounts with valid licenses display a **Configure Service** button on the right. Click that button to gain access to its configuration Administrator Dashboard.
  - Accounts without a valid license display an **Assign Licenses** button on the right.
- **Account Detail Pages**: Select any account from the Navigation Tree on the left of the portal.
  - Accounts with valid licenses display a **Configure Service** button on the top. Click that button to gain access to its configuration Administrator Dashboard.
  - Accounts without a valid license display an **Assign Licenses** button on the top.

Tip! From the portal Navigation Tree, click **Watch A Demo** to open a browser with a page with a list of simulations. Click **Accessing the Dashboard** to see a simulation of each of these procedures.

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). 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, just 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 in the lower right corner of the screen.

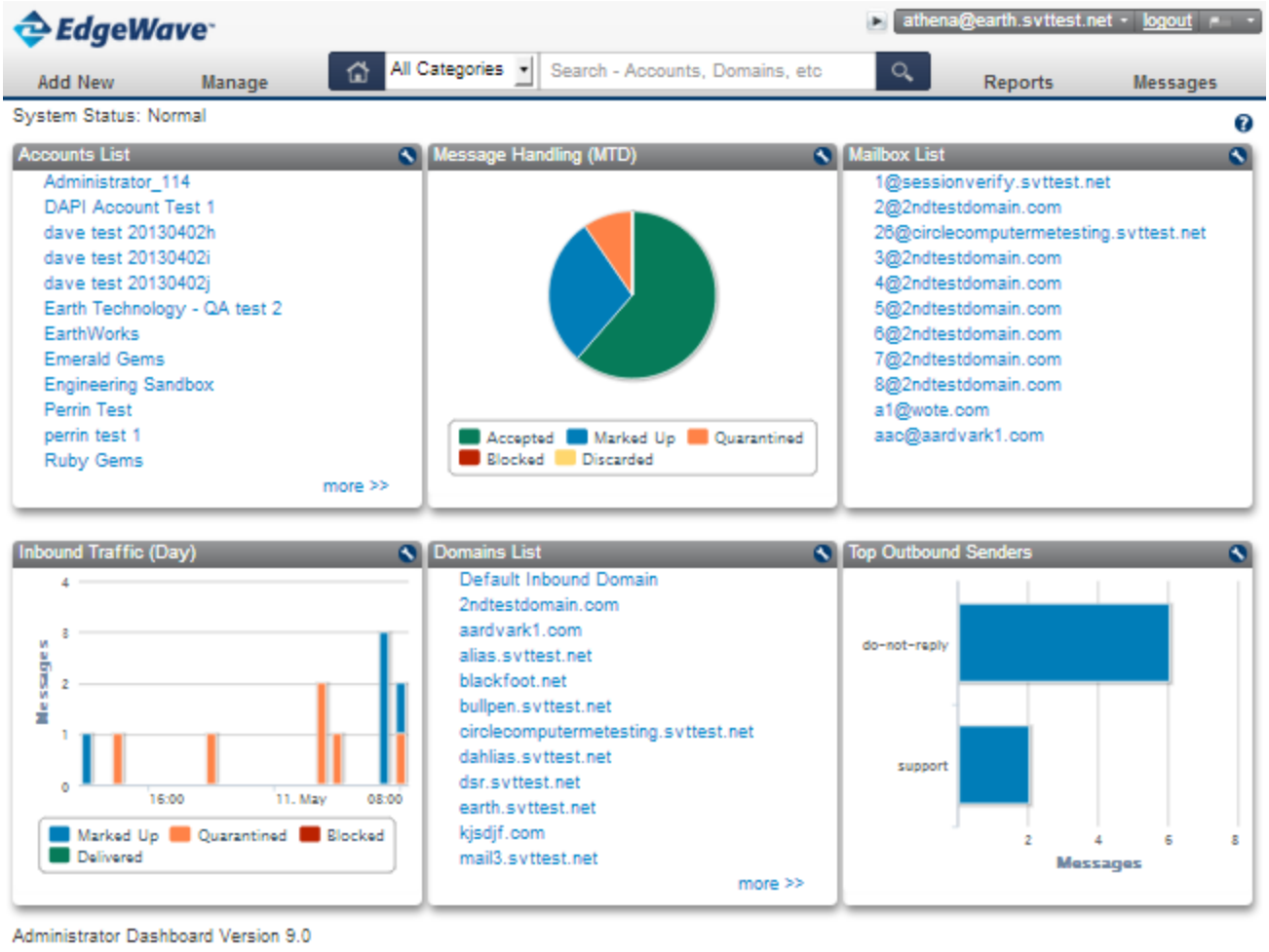

Figure 2. Administrator Dashboard

Customizing the Dashboard Tiles

The home page of the Administrator Dashboard has space for six tiles. These tiles can show system data or lists. 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.

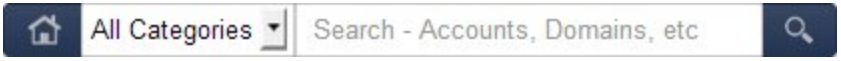

Figure 3. OmniSearch

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**.
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, but do not have to be, different.
4. Click **Save** to save the new password.

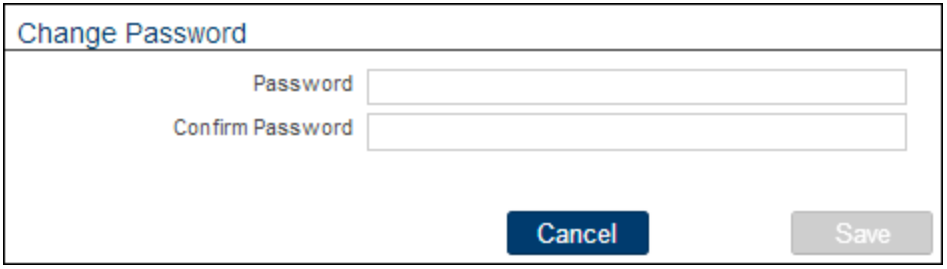

Figure 4. Changing your password

CHAPTER 4 Accounts

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.

Note: Portal users manage accounts on the Portal.

Best Practices

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

Configuring with Other Spam Filter Clients

EdgeWave 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 EdgeWave solution, such point solutions of blocking email addresses within the Outlook client are not required.

Whitelists and Blacklists

EdgeWave 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.

EdgeWave 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 EdgeWave 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.

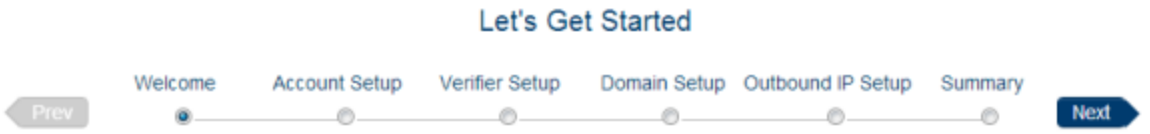

Figure 5. Getting Started Wizard

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 and Encryption Service are enabled or disabled based on the account license. Email continuity, if licensed, can be turned on/off for all domains 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.

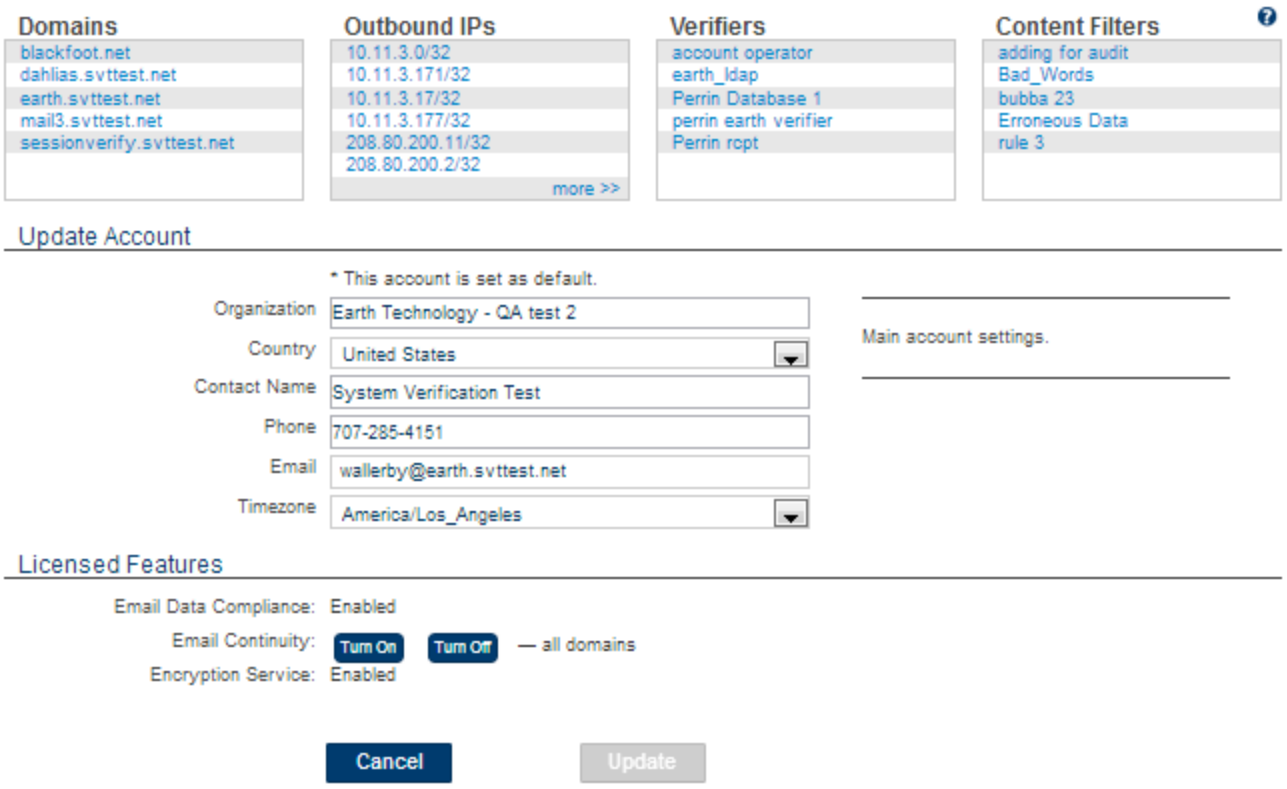

Figure 6. Account information

Managing Administrators

There are several different types of administrators in Email Security. 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** (ePrism 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 EdgeWave. They must have a valid email account (in any domain) to receive informational and administrative messages.

The administrator hierarchy is as follows:

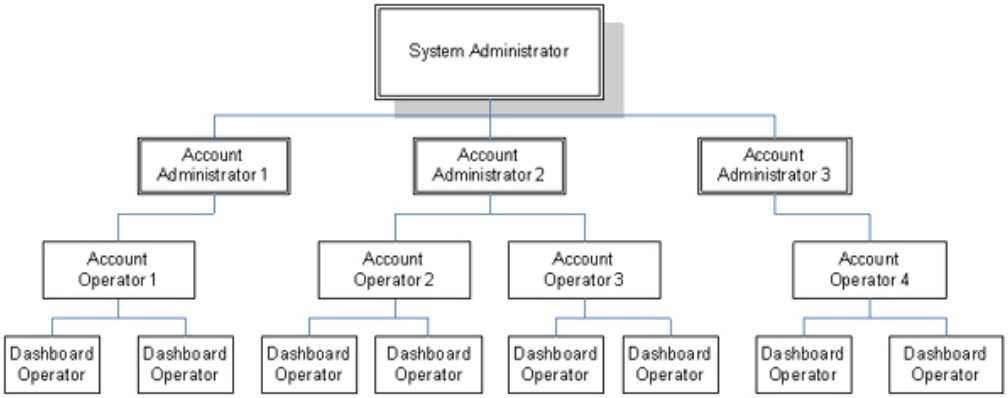

Figure 7. Administrator Types

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.
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.

CHAPTER 5 Domains

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.

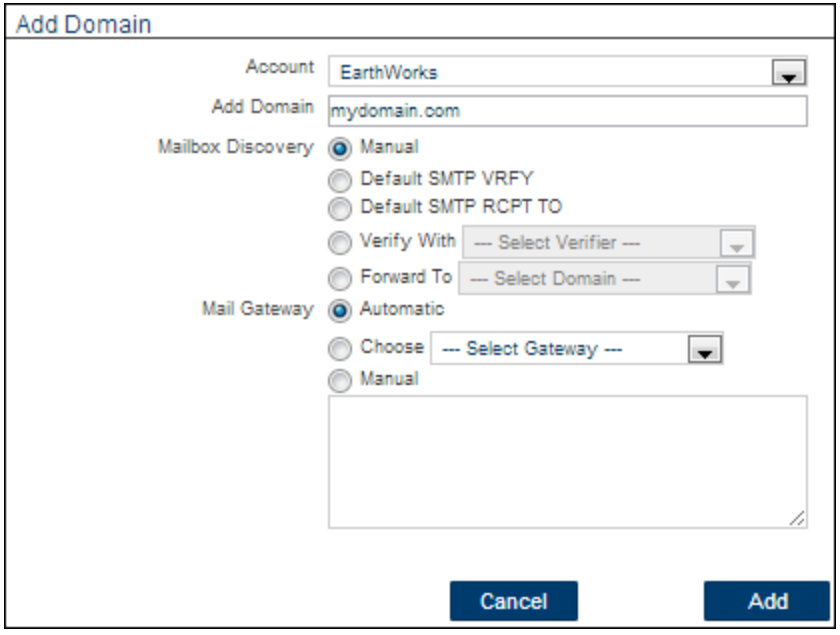

Figure 8. Adding a Domain

3. Select the type of mailbox discovery. See Mailbox Discovery for a description of the discovery options.
4. 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

5. Click **Add**.

Note: It takes a few minutes for EdgeWave to process the new domain.

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 EdgeWave servers that receive incoming email, and list their priority relative to each other. When configured correctly for use with Email Security, 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.
```

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 Digest Options

The Digest Options settings include the default frequency, sort order, format, and type of content of the spam digest that is sent to each user.

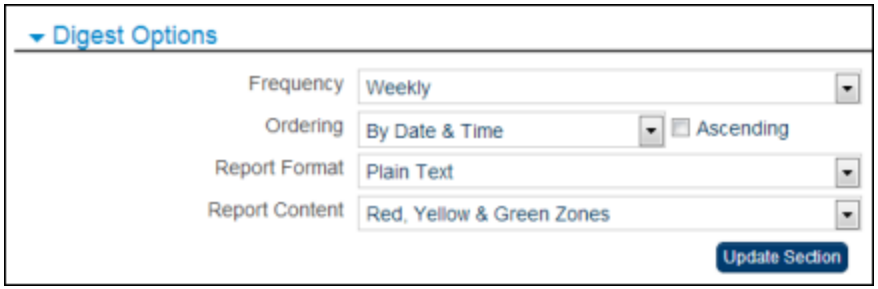

Figure 9. Digest Options

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 that users receive in their spam digest.

The report content types are as follows:

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

Yellow Zone	Forged, Foreign, Attachments
Red Zone	Spam, Virus, Adult, 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.

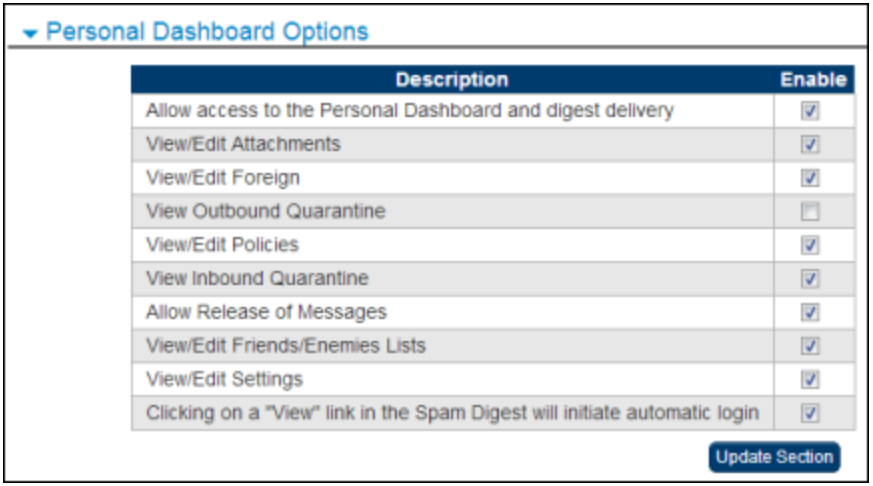

Figure 10. Personal Dashboard Access

Check each option to turn it on, uncheck to turn it off.

Option	Description
Allow access to the Personal Dashboard and digest delivery	The administrator can allow users in this domain to access the Personal Dashboard and digest delivery. Enable is checked by default; if unchecked, the remaining Personal Dashboard options are no longer available. Note: Changes that have been made to mailboxes in the Personal Dashboard override this domain setting. The administrator must view each mailbox to determine the appropriate setting.
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 have been quarantined.
Allow Release of Messages	Enables releasing of messages. If this is disabled, the Release icon/button does not appear on the Personal Dashboard.
View/Edit Friends/Enemies Lists	Users can view and change their own friends and enemies lists. If disabled, the system lists apply.
View/Edit Settings	Users can view and change their own Personal Dashboard settings. If disabled, the default settings apply.
Clicking on a "View" link in the Spam Digest will initiate automatic login	When allowed, users 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.

Filtering Options

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

To specify message handling:

Manage >> Domains >> {Domain}

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.

Allow	Messages pass directly to the mailbox without a tag.
Markup	Messages are forwarded to the mailbox. A subject tag is prepended to the subject line of the email message to indicate that it has been flagged as suspicious. Subject tags can be up to 20 characters.
Quarantine	Messages are saved in the quarantine for review.
Block	Messages are deleted immediately.

Note: If the account operator has defined the filtering option of an intercepted message category as Block, an individual mailbox user cannot override this setting. See Blocked Messages for more information.

3. If you select **Markup** for a category, a text entry box appears on the right. Enter the subject tag in the box.

Note: EdgeWave recommends ending the subject tag with a colon. Most mail programs ignore the text before a colon, to sort on the content of the subject line.

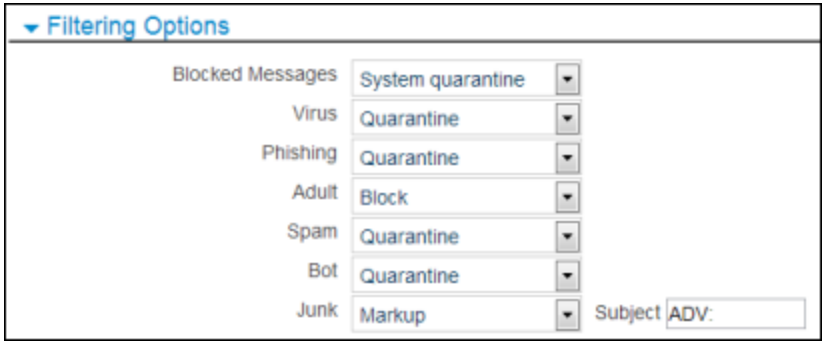

Figure 11. Subject Tag

4. Click **Update Section**.

Filtering Categories

EdgeWave flags messages that have suspicious content, and sorts them into one of the following categories.

Note: The default settings can be manually changed for a domain or individual mailbox.

- **Virus:** EdgeWave uses traditional signature-based filtering for virus detection. Each email message is analyzed by two separate third-party virus definitions: ClamAV and Avast. 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:** The Adult 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.
- **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.

- **Foreign:** EdgeWave provides the option to block email that has foreign characters because a large volume of spam is transmitted using Russian, Cyrillic, Chinese, Korean, and Japanese non-English character sets. If you normally receive email in these languages, configure your settings so that these messages pass through the filters. This option does not filter mail using the English character set in a different language such as Spanish or French. By default, the system blocks mail with non-English language character sets. Foreign language filtering options can be applied individually on a per-language basis.
- **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. 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.

Blocked Messages

There are two types of quarantine: **Quarantine**, which is accessible to both the user and the administrator; and **System Quarantine**, which is available only to the administrator.

Blocked messages can be permanently discarded or placed in a system quarantine that is not user-accessible. All quarantined messages are stored for 35 days.

For end users, blocked messages are not included in the quarantine or digest, regardless of whether the administrator has elected to keep them in the System Quarantine.

Foreign Language

You can filter messages with foreign language content. To remove a language from special treatment, delete the language. Deleting the language means that EdgeWave processes the message as it would any other message, without any special rules. You can later add a language that has previously been deleted.

To add a language:

1. Select the language from the list.
2. Click the Add icon .
3. Select the action to apply.
4. Optional: Delete or change the prepended subject line of marked up languages.

5. Click **Update Section**.

Attachments

Some attachments contain potentially harmful programs, such as viruses, spyware, and keyboard capture, that can cause loss of data and/or personal information. EdgeWave 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.

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.
2. Click the Add icon .
3. Select the action to apply.
4. Optional: Delete or change the prepended subject line of marked up languages.
5. Click **Update Section**.

Content Filters

Once you have set up content filters, you can use them to filter messages.

To use content filters:

1. Select the content filter from the list
2. Click the Add icon .
3. Select the action to apply.
4. Optional: Delete or change the prepended subject line of marked up languages.
5. Click **Update Section**.

Filter by Sender

A whitelist is a list of domain/IP-level trusted mail sources.

A blacklist is a list of domain/IP-level sources to automatically quarantine.

EdgeWave does not recommend using whitelists or blacklists. See Best Practices for more information.

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.

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:

- 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. This is not applicable to hosted systems.
- 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.
- 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.

Figure 12. Domain Settings - Whitelist

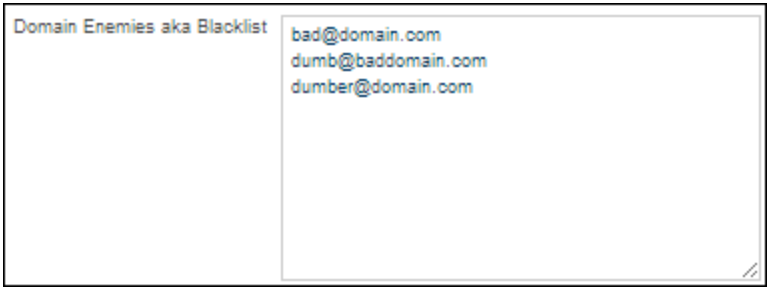

Figure 13. Domain Settings - Blacklist

Authentication

This section sets your method of logging into the dashboard. Valid options are:

Option	Description
Internal	ID and password are stored on the EdgeWave server.
SMTP	Uses SMTP for authenticating the user. Specify the mail server where the ID and password are stored.
Verifier	Uses a verifier for authenticating the user. The ID and password are stored on the verification server. Select the verifier to be used.

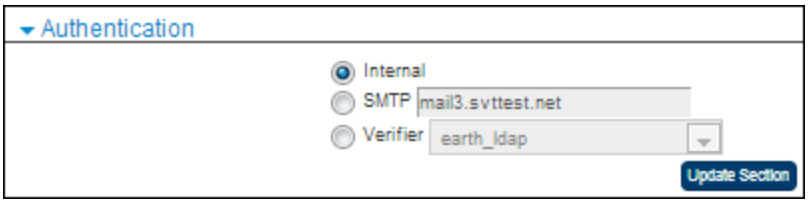

Figure 14. Domain Settings - Authentication

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.

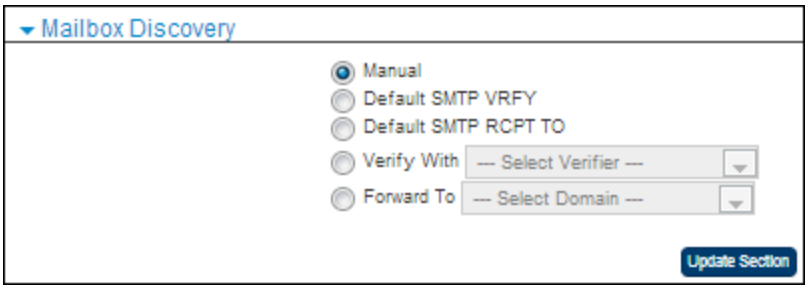

Figure 15. Domain Settings - Mailbox Discovery

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 EdgeWave system.
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.

Option	Description
Default SMTP RCPT TO	Uses the SMTP RCPT TO command to validate mailbox addresses. If the mailbox does not exist, it creates it. A valid response is 250.
Verify with	Uses a previously defined verifier.
Forward to	Forwards mail addressed to an unrecognized recipient to another domain in your account for your review.

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

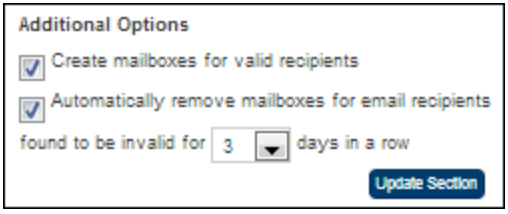

Figure 16. Additional Options

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. This affects active and unprotected mailboxes.

Additionally, EdgeWave provides an API for mailbox provisioning. See the *Provisioning API Guide* for more information.

Unrecognized Recipient Handling

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

Figure 17. Domain Settings - Unrecognized Recipient

Options are:

Option	Description
Accept (Unprotected)	Forward the message to the customer's mail server without spam/virus filtering.
Reject with DHA protection	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.
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 EdgeWave system.

Important: When Unrecognized Recipient Handling is set to **Forward to**, Alias Handling must be set to **Rewrite Aliases to mailbox address**.

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. EdgeWave 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 18. Domain Settings - Alias Handling

Mail Gateways

Email Servers

The names or IP addresses of the email servers in the following formats. If no port is specified, the system uses the default port 25.

Each entry must appear on a separate line. To remove an entry, delete the line.

- 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.

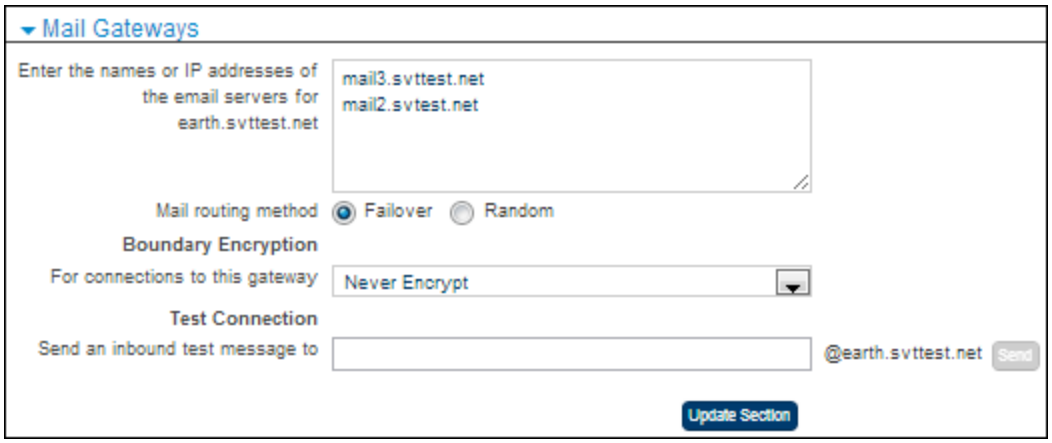

Figure 19. Domain Settings - Mail Gateways

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 ePrism appliance accepts any certificate from the gateway.
Always Encrypt (valid certificate)	The ePrism appliance accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	The ePrism appliance 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 ePrism appliance 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 a copy of messages delivered to the mail gateway.

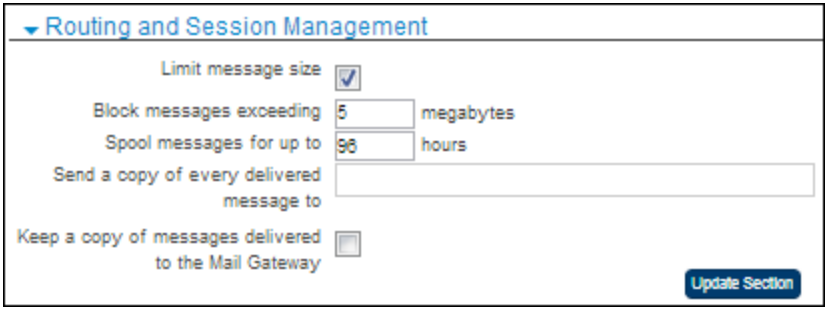

Figure 20. Domain Settings - Routing and Session Management

Option	Description
Limit message size	Limit the maximum size of an individual message.
Block messages	If the above checkbox is selected, enter the maximum message size in megabytes, from 1-100. Messages larger than this 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.
Spool messages	Configure spooling of messages for a period of time, measured in hours, in case of server failure. From 1 through 160 hours.

Send a copy of delivered messages to	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 enabled. Note: This option only appears if Email Continuity is not available (disabled or not licensed). If Email Continuity is enabled, this option appears in that section and is automatically turned on.

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.

Manage >> Domains >> {Domain}

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

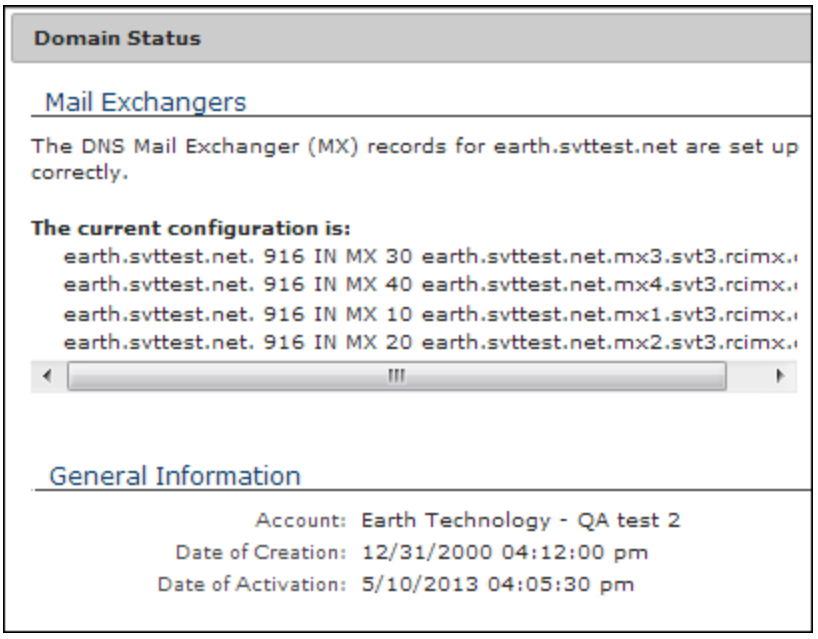

Figure 21. Domain Status

Email Continuity

Email Continuity gives users access to their email when the email server is down. If your organization has licensed this feature, when the email server goes down, Email Continuity can be enabled 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 turned on, the Outbound Authenticated Relay settings are applied to outbound messages.

When the email server comes back up, disable Email Continuity so that copies of all sent messages are relayed to the mail server. These messages contain the header 'user-agent:EdgeWave/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.
- Specify whether Email Continuity is to activate automatically after a specified period of down-time, or if you want to activate it manually. The Email Continuity settings are in the Routing and Session Management section of Domain Settings.
- Add a notification to alert you when Email Continuity is automatically enabled. For details, see Adding a Notification.
- Enable keeping a copy of legitimate messages so that a 35 day email history will exist should the email server go down.
- Increase spool time to 160. 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: EdgeWave/Email Continuity (console)' in the mailbox Sent folder.

Reporting

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

CHAPTER 6 Outbound IP Addresses

EdgeWave 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

Add New >> Outbound IP

1. Select the account.
2. Enter the IP address or range. This is the IP address of the server that delivers email to the EdgeWave filtering system. You can add a range of servers in CIDR format.
3. Click **Add**.

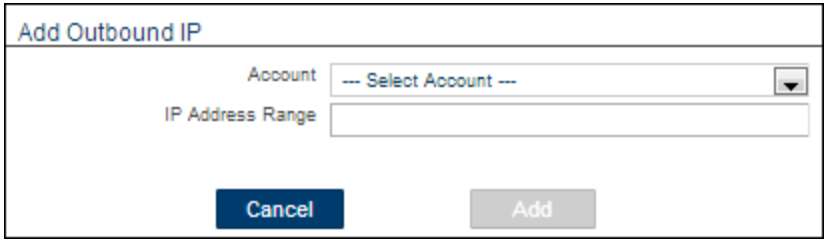

Figure 22. Adding an outbound IP

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**.

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.

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

- Credit card, social security number, and compliance filters
- Recipient White List
- The option to add a disclaimer (Message Annotation)
- Rate Limits
- The ability to route mail based on message content

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 EdgeWave. 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 EdgeWave.

- Change the firewall settings to block all outgoing email that attempts to bypass the domain's mail server and the EdgeWave outbound filter.

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.

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. Options are:

Allow	Messages pass directly to the mailbox without a tag.
Special Routing	Messages are routed according to the instructions you set up in the Special Routing section below. See Special Routing for details.
Markup	Messages are forwarded to your 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.
Quarantine	Messages are saved in the quarantine for review.
Block	Messages are handled according to the Block setting above - either saved in the system quarantine or permanently deleted.

3. If you select **Markup** for a category, a text entry box appears on the right. Enter the subject tag in the box.

Note: EdgeWave 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.

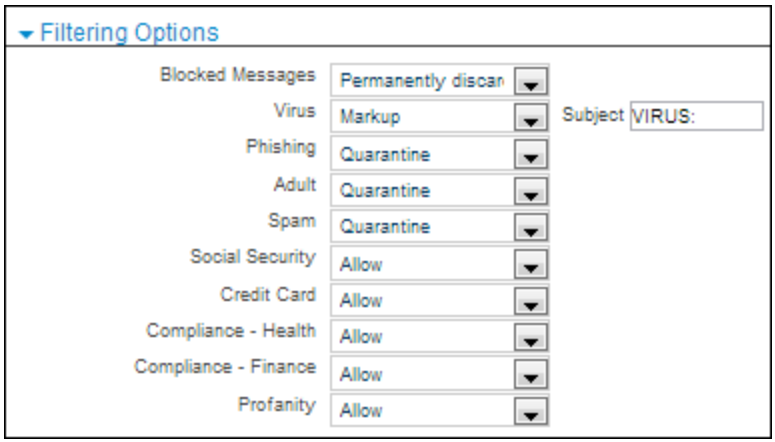

Figure 23. Outbound Filtering Options

Outbound Filtering Categories

EdgeWave flags messages that have suspicious content, and sorts them into one of the following categories.

- **Virus:** EdgeWave uses traditional signature-based filtering for virus detection. Each email message is analyzed by two separate third-party virus definitions: ClamAV and Avast. 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:** The Adult 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.
- **Social Security:** Scans the message and text attachments for Social Security numbers. The default is to allow.
- **Credit Card:** Scans the message and text attachments for credit card numbers. The default is to allow.

- **Compliance - Health and Finance:** A lexicon is an XML file that contains a list of specialized vocabulary and phrases unique to a specific subject. EdgeWave Email Data Compliance includes built-in lexicons for the financial and healthcare industries that prevent accidental or malicious exposure of personal health or financial information – a critical factor in complying with regulatory requirements. For details about Health and Finance filtering, see the Data Loss Protection (DLP) section of Overview of Services

  

  Note: Email Data Compliance is a licensed feature.

- **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. 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.

Outbound IP Whitelists and Blacklist

The sender whitelist and blacklist are similar to those for inbound domains. See Filter by Sender for more information.

The recipient whitelist for outbound email should include individuals and organizations that you want to ensure receive mail when it is sent from this Outbound IP. Mail that is sent to these addresses will not be subject to spam filtering as long as all recipients are on the whitelist.

EdgeWave does not recommend using whitelists or blacklists. See Best Practices for more information.

There is no restriction on the number of whitelist entries for a domain. Each entry must appear on a separate line. To remove an entry, delete the line and click **Save**.

Valid options are:

- Email address
- Domain

Configuring Delivery Status Notification

You can optionally set the number of times a Delivery Status Notification (DSN) message can be sent to the user alerting them that an outbound message has been quarantined. The notification consists of a DSN with the message attached. 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. DSN delivery to senders from unknown domains can be enabled.

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

To enable Delivery Status Notification:

Manage >> Outbound IPs >> {Outbound IP}

1. Select the **Send a notification to known senders when a message is quarantined** checkbox.

   Note: An alias that is not attached to an actual ePrism 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 ePrism appliances, select the checkbox to include senders from unknown domains.

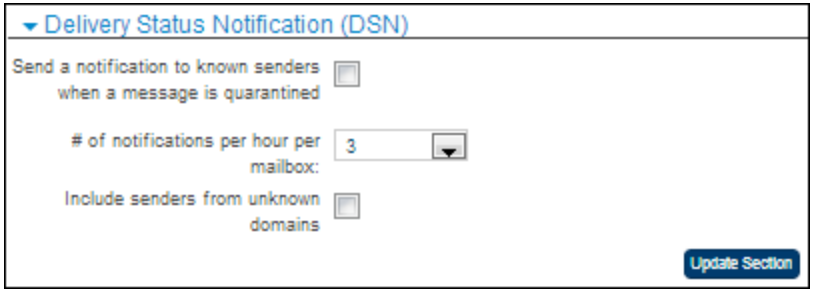

Figure 24. DSN settings

Setting 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 EdgeWave, with either a 451 (temporary) or 550 (permanent) error code.

Notes:

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.

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.

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.

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.

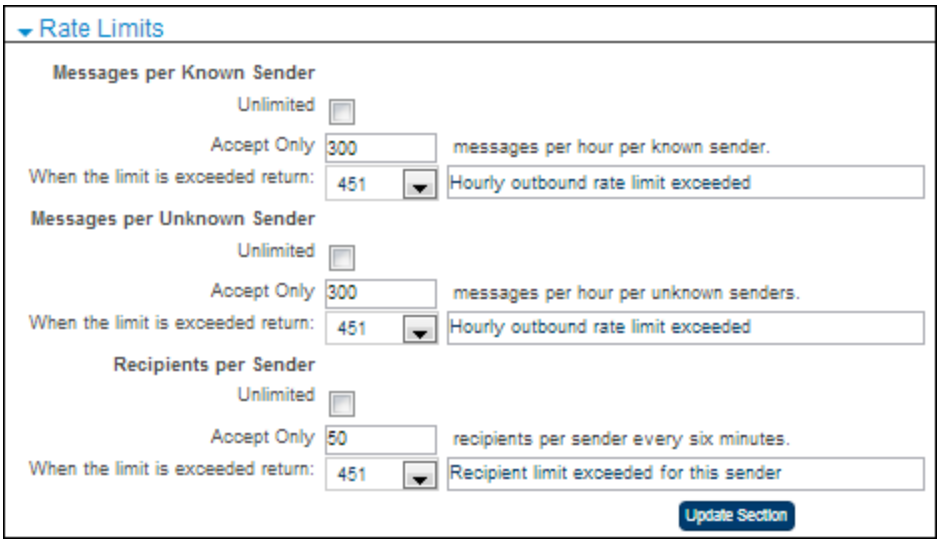

Figure 25. Rate Limits

Message Annotation

The following is true for all outbound messages for a given Outbound IP. For annotation entries:

- 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 that are 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.

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.

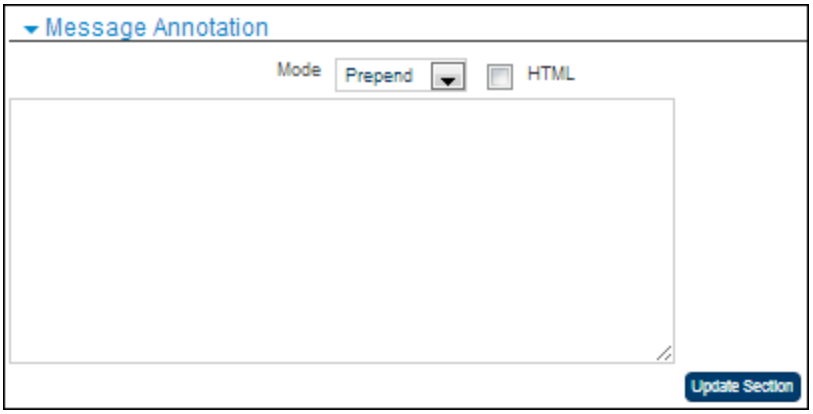

Figure 26. Message Annotation

Boundary Encryption

You can configure account-wide boundary encryption settings from the outbound IP to the ePrism appliance, and from the ePrism appliance to the Internet. Additionally, you can define individual encryption settings for each domain that differ from the default. You can validate your settings by initiating a test connection to a valid domain. See Routing and Session Management for details on setting up exceptions for specific domains.

To configure boundary encryption for outbound mail:

Manage >>Outbound IPs >> {Outbound IP}

1. In the Boundary Encryption section, select the encryption method for mail from the outbound IP to the ePrism appliance.

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.

2. Use the drop-down list to select the default encryption method for mail from the ePrism appliance to the Internet.

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 ePrism appliance accepts any certificate.
Always Encrypt (valid certificate)	The ePrism appliance accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	The ePrism appliance 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.

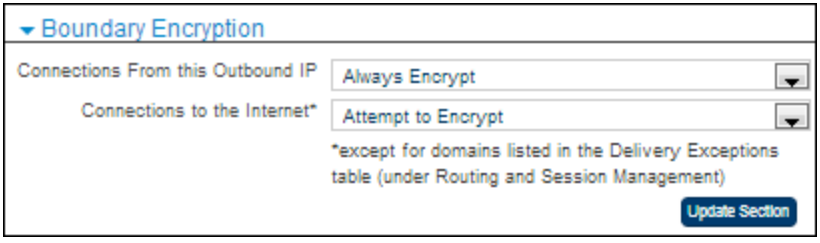

Figure 27. Boundary Encryption

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.

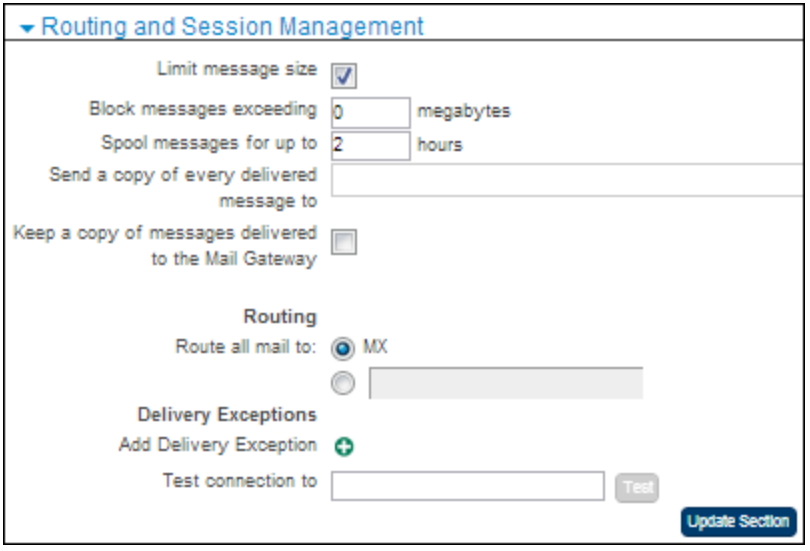

Figure 28. Routing and Session Management

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 160 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, 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 ePrism appliance 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 ePrism appliance 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

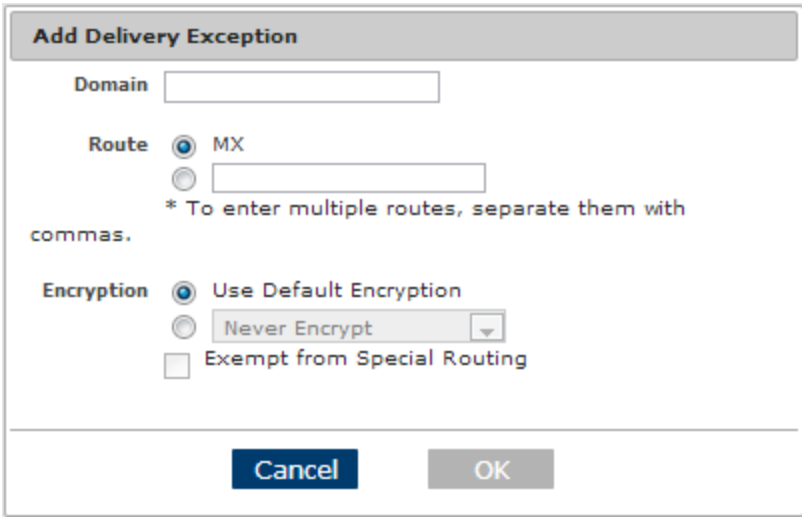

Figure 29. Adding a delivery exception

2. In the **Domain** text box, enter the name of the excepted domain. The expression *.domain.com excepts multiple sub-domains.
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.

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 ePrism appliance accepts any certificate from the gateway.
Always Encrypt (valid certificate)	The ePrism appliance accepts any valid, non-expired, certificate that has the proper form and syntax.

Always Encrypt (trusted certificate)	The ePrism appliance 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.
Always Encrypt (check hostname)	The certificate is trusted and contains the listed hostname.

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

Authentication

To configure outbound authentication:

Manage >> Outbound IPs >> {Outbound IP}

1. Select the type of authentication. Options are:

None	
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

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

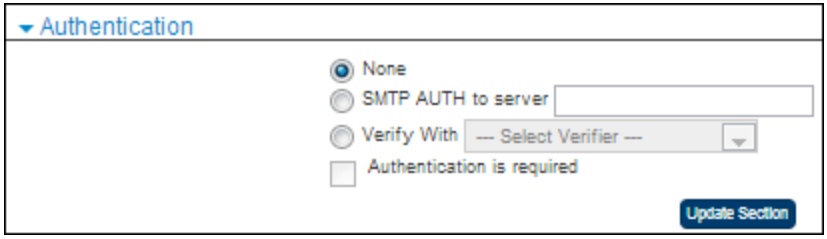

Figure 30. Authentication

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.

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/define 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.

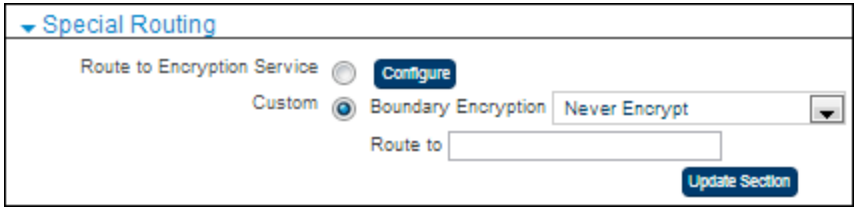

Figure 31. Special Routing

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**.

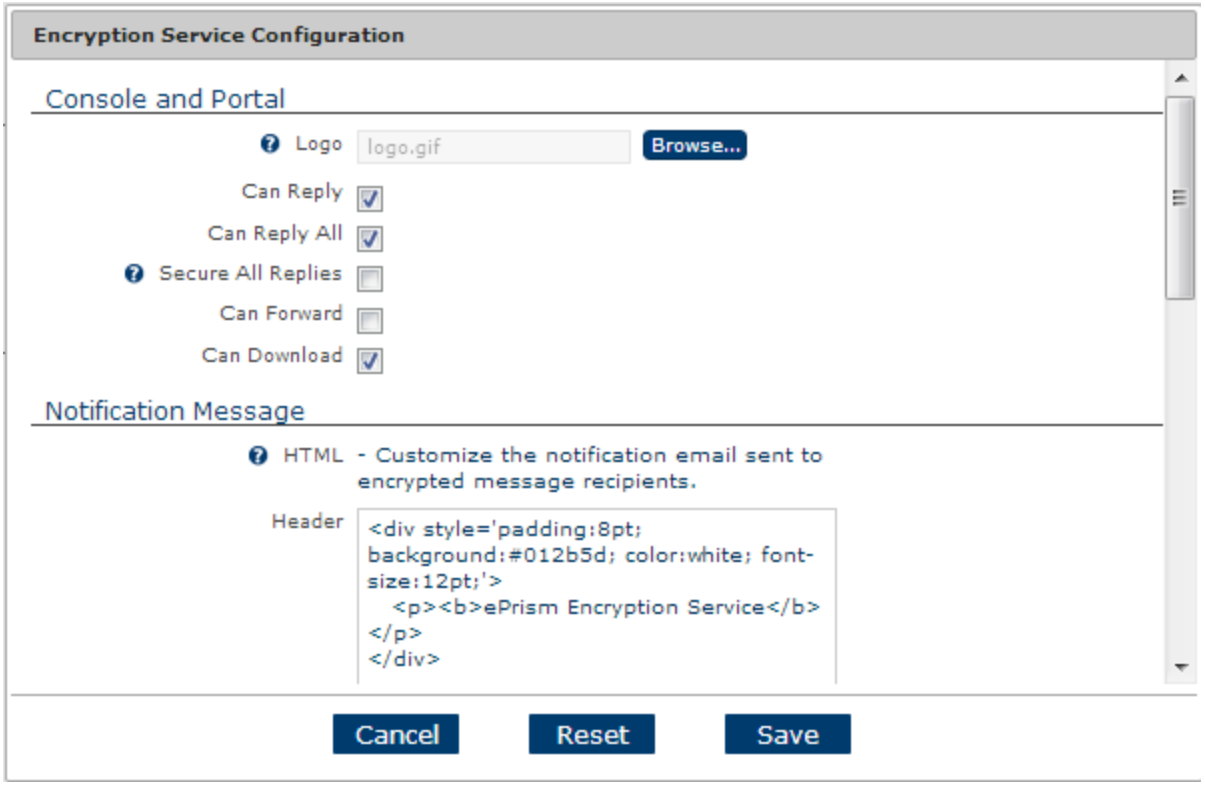

Figure 32. Configure Encryption Service

3. Select the logo.
   - This logo appears on the Encryption portal login and message list pages.
   - It can also appear in the notification message (see below).
4. Select which actions the user will be able to take on encrypted messages.
5. If you want all replies to remain on the encryption server as well, select **Secure All Replies**.
6. You can customize the message that is sent to users to notify them that an encrypted message is available. 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='ePrism Encryption Service'>

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.

Never Encrypt	Transport Layer Security (TLS) is never attempted during the session.
Always Encrypt (any certificate)	The ePrism appliance accepts any certificate from the gateway.
Always Encrypt (valid certificate)	The ePrism appliance accepts any valid, non-expired, certificate that has the proper form and syntax.
Always Encrypt (trusted certificate)	The ePrism appliance 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.

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

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.

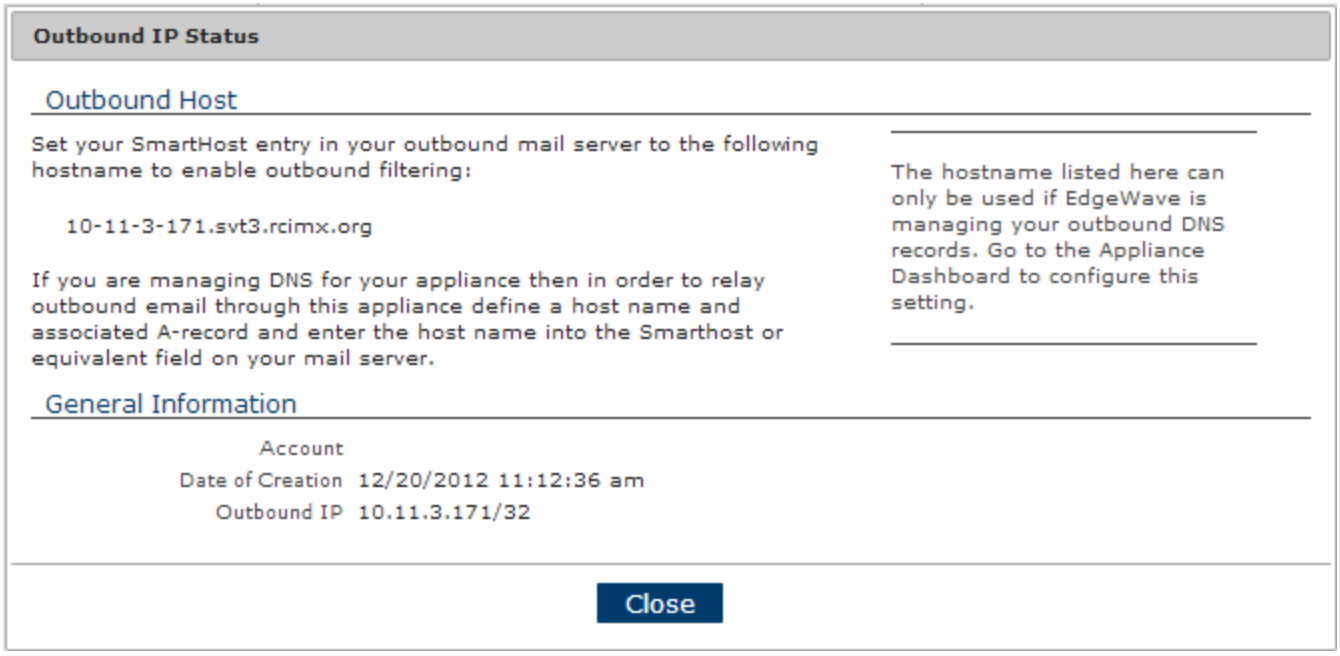

Figure 33. Outbound IP Status

CHAPTER 7 Mailboxes

Mailboxes are user email accounts managed by the Email Security system. 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 EdgeWave 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.
   - Use a comma to list multiple aliases. Aliases can be alternate domains.
3. Click **Add**.

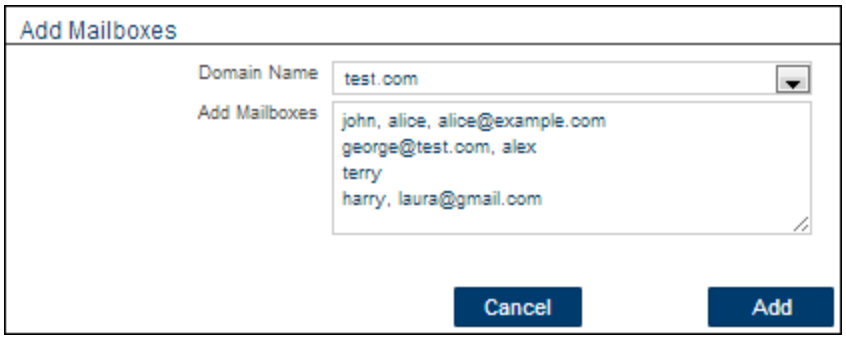

Figure 34. Mailboxes

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}

General Settings

Figure 35. 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.
Password	The password can be changed here if Authentication is set to Internal.

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 option is overridden (from the domain setting) for this mailbox.

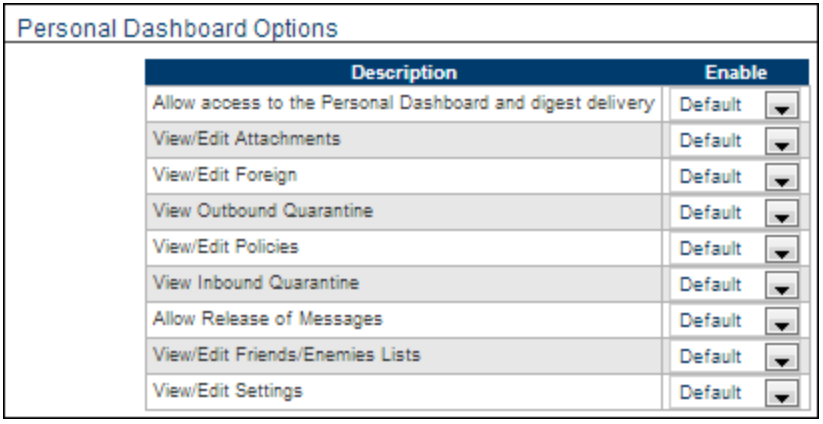

Figure 36. Personal dashboard options for an individual mailbox

Option	Description
Allow access to the Personal Dashboard and digest delivery	Allows this mailbox user to access the Personal Dashboard and receive the spam digest. If this option is disabled, the remaining Personal Dashboard options are no longer available.

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 have been quarantined.
View/Edit Policies	Users can view the mailbox policies.
View Inbound Quarantine	Users can view incoming messages that have been quarantined.
Allow Release of Messages	Enables releasing of messages. If this is disabled, the Release icon/button does not appear on the Personal Dashboard.
View/Edit Friends/Enemies Lists	Users can view and change their own friends and enemies lists. If disabled, the system lists apply.
View/Edit Settings	Users can view and change their own Personal Dashboard settings. If disabled, the default settings apply.

Outbound Mail Options

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

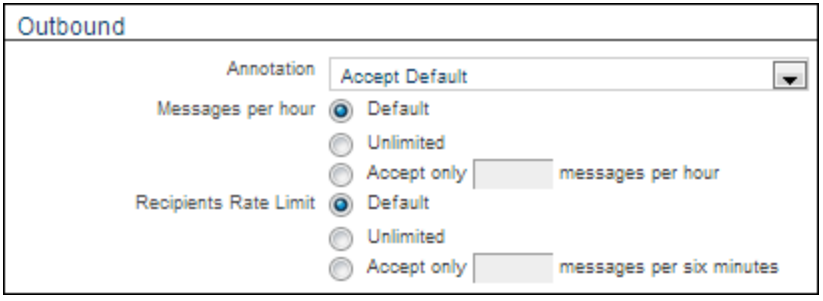

Figure 37. Outbound mail settings for an individual mailbox

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 Setting 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 Setting Rate Limits), Unlimited to remove the limit, or specify the number of messages per 6 minutes for this mailbox.

Mailbox Aliases

The Email Security alias handling feature 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 by the EdgeWave filter 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.

Creating 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.schom@yourdomain.com, but also have aliases of joe@yourdomain.com, joes@yourdomain.com, or jschmo@yourdomain.com.

The value of having awareness of aliases within the EdgeWave servers is that EdgeWave can create a single quarantine view that aggregates all quarantine for the aliases and their associated primary mailbox. This is preferable than having a user have a separate quarantine and daily digest for the primary and alias account.

Note: Aliases in individual overrides of outbound rate limits are not supported.

To create a mailbox alias:

Manage >> Mailboxes >> {Mailbox}

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

Autodiscovering Aliases

If you are using a Mailbox Disovery 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 Email Security LDAP feature 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

Changing Filter Policies and Digest Settings

To change the policies for an individual mailbox:

Manage >> Mailboxes >> more

1. In the Mailboxes list, click the **Personal Dashboard** link next to the name of the mailbox you want to change.

   The Personal Dashboard for the mailbox is displayed. This is where filter policies, whitelists and blacklists, and digest settings can be modified.

2. To modify the digest and time zone settings for this mailbox, click the **Settings** tab (high bandwidth) or the **Digest** tab (low bandwidth).

3. To specify how messages are filtered on the high bandwidth Personal Dashboard, click the **Policies** tab. On the low bandwidth Personal Dashboard these settings are on the **Policies**, **Foreign**, **Attachments**, **Friends**, and **Enemies** tabs.

Unprotecting a Mailbox

Unprotected mailboxes do not have their mail filtered through the Email Security system. 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 EdgeWave 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**.

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**.

CHAPTER 8 Verifiers

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.

EdgeWave supports two levels of verifiers:

- **Account-level**: For mailbox discovery and authentication for ePrism 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 eight pre-defined verifiers:

- **LDAP**: Lightweight Directory Access Protocol.
- **VRFY**: SMTP command for verifying an email address.
- **RCPT TO**: SMTP command for verifying an email address.
- **Communigate CLI**: Command Line Interface (CLI) for server communications.
- **POP - Authentication Only**: POP3 protocol for dashboard login authentication.
- **Database**: SQL based database servers containing email addresses for all valid mailboxes, and optionally, passwords. EdgeWave supports both MySQL and PostgreSQL databases.
- **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.

Adding a Verifier

Add New >> Verifier

1. Select the account.
2. Enter a descriptive name for the verifier.
3. Enter the verifier information (see below).
4. If you want to test the connection, enter the information for validation. See Testing the Verifier Connection for details.
5. Click **Add**.

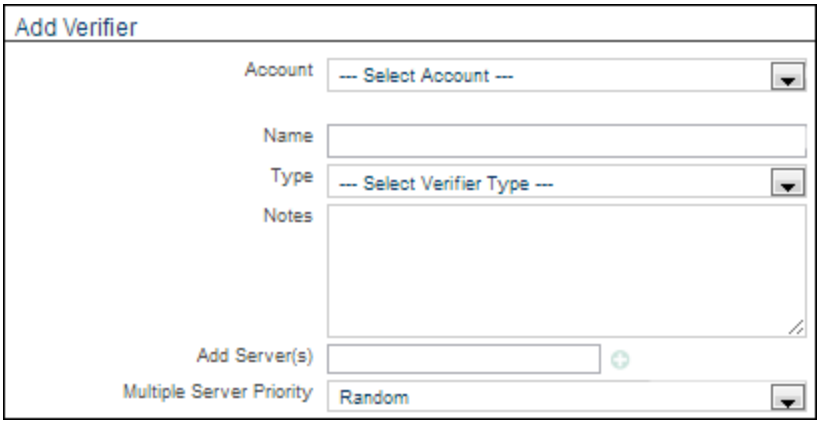

Figure 38. Adding a Verifier

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: • 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. • If the system is on an appliance and licensed for Vx, at least one address must be external. Optional: Select the **SSL** checkbox to use Secure Socket Layer encryption for traffic between EdgeWave and the verification server. Repeat as needed for multiple verification servers.
Multiple Server Priority	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 needed.
Verifier-specific settings	Depending on the verifier type, select additional options as applicable.

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.

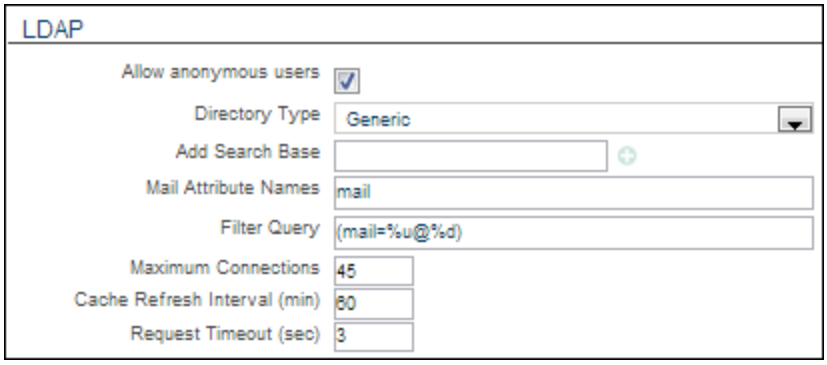

Figure 39. LDAP Verifier

- Optional: Select the **Allow Anonymous Users** checkbox to bind anonymously to the LDAP directory.
- If the **Allow Anonymous Users** checkbox is not selected:
  - In the **Bind Name** text box, enter the ID of the user permitted to search the LDAP directory.
  - In the **Bind Password** text box, enter the password of the user permitted to search the LDAP directory.
- In the **Directory Type** list, select the type of directory. Options are Active Directory, Generic, Zimbra, and Domino.
- In the **Add Search Base** text box, enter the location in the directory from which the LDAP search begins.
- In the **Mail Attributes Names** text box, enter the names of the attributes that contain the email address of the user.
- In the **Filter Query** text box, enter the query to use to locate the user in the directory by email address. %d = domain, %u - user.
- In the **Maximum Connections** text box, enter the maximum number of simultaneous connections between the EdgeWave directory and the LDAP directory.

- In the **Cache Refresh Interval (min)** text box, enter the minimum number of minutes between queries by the EdgeWave 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.
- In the **Request Timeout (sec)** text box, enter the maximum number of seconds to wait for a response from the directory server before the connection times out.

VRFY Verifier

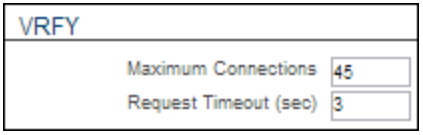

Figure 40. VRFY Verifier

- In the **Maximum Connections** text box, enter the maximum number of simultaneous connections allowed between the EdgeWave server and the mail server.
- In the **Request Timeout (sec)** text box, enter the maximum number of seconds to wait for a response from the mail server before the connection times out.

RCPT TO Verifier

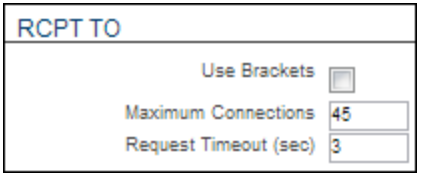

Figure 41. RCPT TO Verifier

- Optional: Select the **Use Brackets** checkbox to indicate that the mail server requires brackets (<>) to surround the email address.
- In the **Maximum Connections** text box, enter the maximum number of simultaneous connections between the EdgeWave server and the mail server.
- In the **Request Timeout (sec)** text box, enter the maximum number of seconds to wait for a response from the mail server before the connection times out.

Communigate CLI Verifier

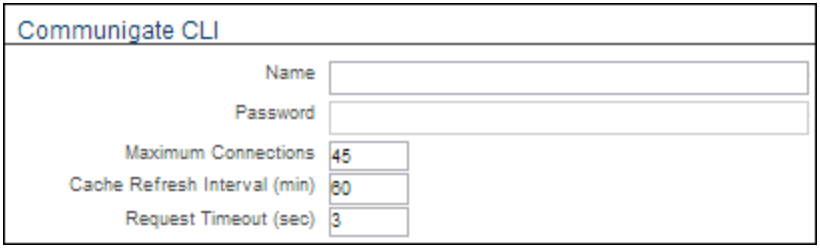

Figure 42. Communigate CLI Verifier

- In the **Name** text box, enter the name of the account that will communicate with the Communigate server.
- In the **Password** text box, enter the password of the account that will communicate with the Communigate server.
- In the **Maximum Connections** text box, enter the maximum number of simultaneous connections between the EdgeWave server and the Communigate server.
- In the **Cache Refresh Interval** text box, enter the minimum number of minutes between queries by the EdgeWave server to the Communigate server to update its local cache of the user list. The actual time will vary between 0.5 and 1.5 times the interval.
- In the **Request Timeout** text box, enter the maximum number of seconds to wait for a response from the Communigate server before the connection times out.

POP - Authentication Only Verifier

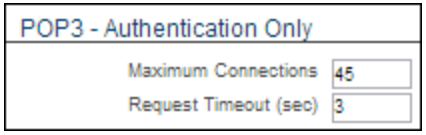

Figure 43. POP Verifier

- In the **Maximum Connections** text box, enter the maximum number of simultaneous connections between the EdgeWave server and the POP server.
- In the **Request Timeout (sec)** text box, enter the maximum number of seconds to wait for a response from the POP server before the connection times out.

Database Verifier

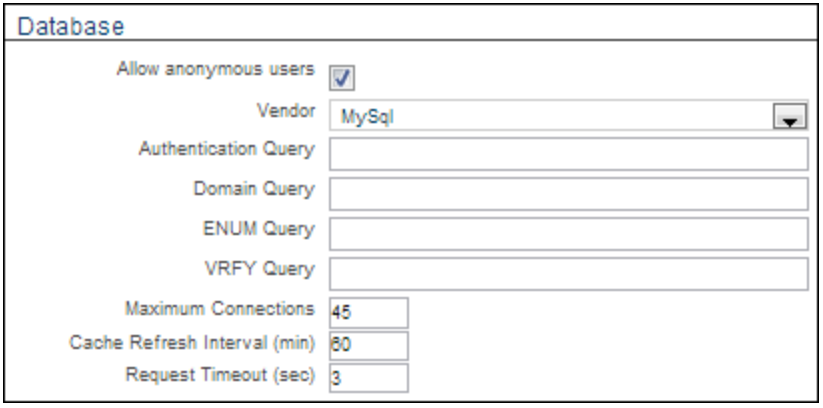

Figure 44. Database Verifier

- Optional: Select the **Allow Anonymous Users** checkbox to bind anonymously to the database server.
- If the **Allow Anonymous Users** checkbox is not selected:
  - In the **Name** text box, enter the name of the account that will communicate with the database server.
  - In the **Password** text box, enter the password of the account that will communicate with the database server.
- In the **Database Name** text box, enter the name of the database.
- From the **Vendor** drop-down list, select MySql or Postgres.
- In the **Authentication Query** text box, enter the SQL query to search the user password.
- In the **Domain Query** text box, enter the SQL query to retrieve the list of valid domains.
- In the **ENUM Query** text box, enter the SQL query to retrieve the list of valid recipients.
- In the **VRFY Query** text box, enter the SQL query to retrieve a specified mailbox.
- In the **Maximum Connections** text box, enter the maximum number of simultaneous connections between the EdgeWave server and the database server.

- In the **Cache Refresh Interval** text box, enter the minimum number of minutes between queries by the EdgeWave 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.
- In the **Request Timeout** text box, enter the maximum number of seconds to wait for a response from the database server before the connection times out.

Static Verifier

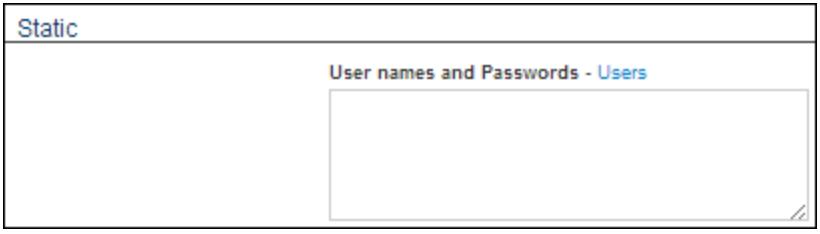

Figure 45. Static Verifier

- 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 2 or more verifiers. 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.

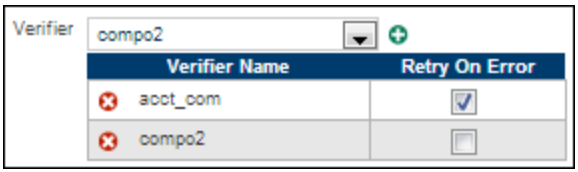

Figure 46. Composite Verifier

- 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.

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.

Figure 47. 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.

Custom verifiers created through the EdgeWave Provisioning API cannot be modified through the Administrator Dashboard unless the verifier type is changed from Custom to one of the pre-defined 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 system. 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.

CHAPTER 9 Content Filters

EdgeWave offers optional content filtering to 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. It 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.

To add a content filter:

Add New >> Content Filter

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

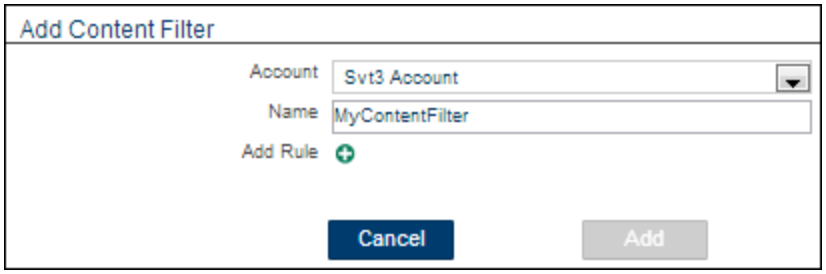

Figure 48. Adding a Content Filter

3. Add rules to define the content filter (see below).
4. 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.

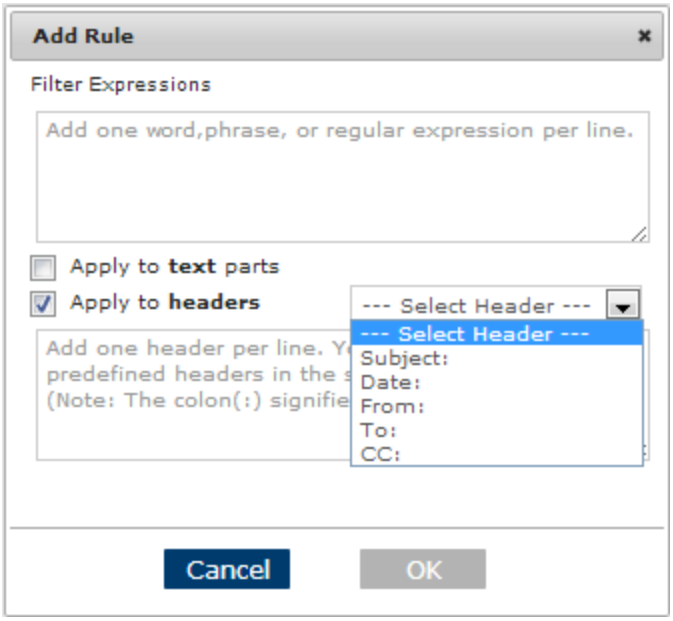

Figure 49. Defining Content Filter Rules

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.

5. 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 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**.

CHAPTER 10 Notifications

A notification is an email message that is sent when a specific event occurs. You can define which events trigger notifications, how often, and the message recipient. You can also receive notifications via text message using your wireless provider's email to SMS feature.

Notifications are set up through the Administrator Dashboard.

Adding a Notification

Add New >> Notification

1. Enter the Subject. This becomes the notification name, and will appear in the Subject field of the sent message.

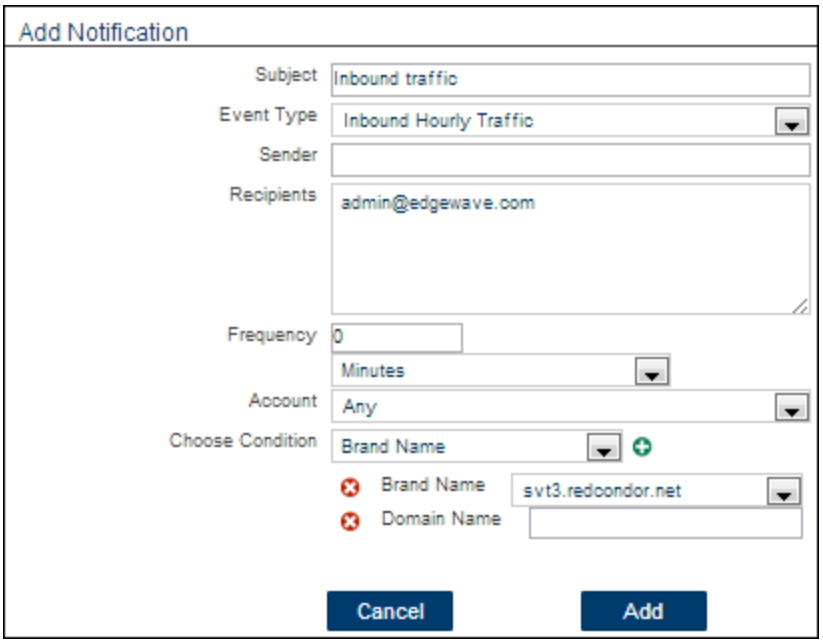

Figure 50. Adding a Notification

2. Select the event type that will trigger the notification message to be sent.

Note: The types of events available are dependent on the Admin role.

Event type	Description
Outbound Deferred Messages	Filtered messages waiting to be delivered to the mail gateway or the Internet.
Remote Server Offline	The system is unable to successfully connect to the destination mail gateway.
Inbound Hourly Traffic	The number of messages that enter the server for filtering from the Internet per hour.
Outbound Hourly Traffic	The number of messages that leave the server for the Internet or mail gateway per hour.

Event type	Description
Sender Rate Limit	This event occurs when the sender rate limit is exceeded.
Recipient Rate Limit	This event occurs when the recipient rate limit is exceeded.
Email Continuity Enabled	This event occurs when Email Continuity is automatically enabled.

3. Enter the sender email address. This address will appear in the From field of the sent message.
4. Enter the recipients to which the notification message will be sent, one per line. These can be regular email addresses, or text addresses. For text messaging, use the following formats (phone number is the recipient's mobile number).

Carrier	Address format
Alltel	phonenumber@message.alltel.com
AT&T	phonenumber@txt.att.net
AT&T MMS	phonenumber@MMS.att.net
Cingular	phonenumber@cingularme.com
Metro PCS	phonenumber@MyMetroPcs.com
Nextel	phonenumber@messaging.nextel.com
Powertel	phonenumber@ptel.net
Sprint	phonenumber@messaging.sprintpcs.com
SunCom	phonenumber@tms.suncom
T-Mobile	phonenumber@tmomail.net
US Cellular	phonenumber@email.uscc.net
Verizon	phonenumber@vtext.com
Virgin Mobile	phonenumber@vmobl.com

5. Select how often notifications are to be sent for this event.
6. Select the account to be monitored.
7. Select the conditions that generate a notification. The available options vary depending on the type of event selected above. For each condition:
   - Select the condition and click ⊕.
   - Enter values if applicable.

   The possible conditions are as follows:

Condition	Description
Action	The action taken by the filter on a message (Accept, Markup, Quarantine & Block).
Category	The message category determined by the filter.
Count	The number of times the item measured must occur before the event is triggered.
Domain Name	Limit event generation to particular domains.
Enabled	The feature being monitored has been turned on.
Failure Count	The number of times the item measured must fail before the event is triggered.
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 the event is triggered.
Offline Duration	The minimum amount of time that connection attempts to a server must fail before an event is generated.
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

The following units of time can be used for the Duration condition:

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

The following units of size can be used for the Size condition:

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}

To edit the notification details:

1. Change the specifications as needed.
2. Click **Update**.

To delete the notification:

1. Click **Delete** .
2. To confirm, select the checkbox and click **Delete**.

CHAPTER 11 Reporting

EdgeWave supports account-level statistical information reports for inbound and outbound connections and messages for both hosted and ePrism appliance customers.

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.

Reports >> {Report Name}

1. Select the domain or outbound IP.
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.

For reports that return a list of messages:

- To see a preview of a message, click the **View** link next to the message.
- To release one or more messages to your mailbox, select the **All** checkbox or the checkboxes next to individual messages, and click **Release**.

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.

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. You can unsubscribe from a report at any time.

To subscribe to a report:

1. Run the report. See Running a Report for details.
2. Click **Subscribe**.
3. Rename the report and/or add email addresses to the CC: list (optional).
4. Select the report frequency.
5. Click **Save**.

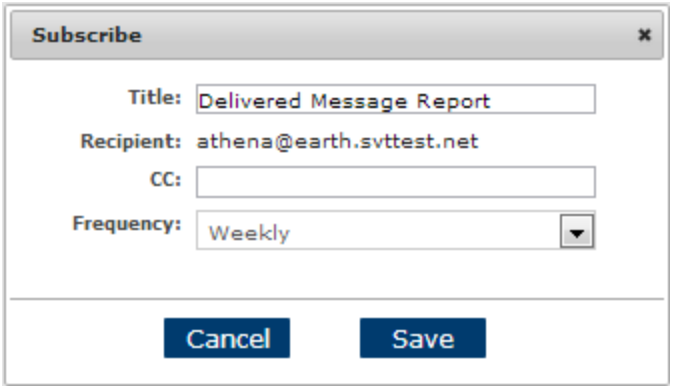

Figure 51. Subscribing to a report

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.
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.

Charts

Charts show data in graphical format and are available for many of the statistics within the system.

Reports >> 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.

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:
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.

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, 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 categories to include.
- Choose which actions to include.
- Choose which dispositions to include.
- Choose the layout (which columns to include).

Note: To include all categories, actions, or dispositions, leave the All checkbox selected. To choose which of these options to include, deselect the All checkbox and then select the options.

Delivered Message Report

This report allows the user to track legitimate messages. If you have enabled 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 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 message ID, 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).

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).

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, the current month to date, any of the previous three months, the current year to date, or either of the previous two 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. EdgeWave quarantines filtered email messages and makes them available through a link in the Spam Digest or a report.

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 and release from quarantine.

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, and/or subject, select the type of quarantine, 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 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).

APPENDIX A EdgeWave Message Headers

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

- **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.)

The following headers have been deprecated, but are still included in the message. They are now included in every message categorized by a filter:

- **X-REDCONDOR-FILTER**
- **X-REDCONDOR-PROFILE**
- **X-REDCONDOR-CAUSE**

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
SSN	category used for SSNFilter
VIRUS	category used for RuleType VIRUS and VirusFilter

APPENDIX B SMTP Session Return Codes

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>}

Corporate Office

2603 S. Washington St. STE 120, Naperville, Illinois 60565

Phone: (630) 759-9283 Email: sales@jikometrix.net