


ePrism Messaging Security Suite



Welcome to EdgeWave Messaging Security!

This short guide is intended to help administrators setup and test the EdgeWave Messaging Security Suite for evaluation purposes. A more detailed step-by-step guide is also available upon request.

 = EdgeWave Advantage

 = Evaluation Goal


Before You Get Started

Make sure you have access to the DNS MX records for your domain(s) in order to change them when you are ready to cut over to the EdgeWave service. If you prefer, you can also try the EdgeWave Security Suite in-series with your current email filtering provider. Contact your EdgeWave Representative if you have any questions regarding this setup. If at any time during the Evaluation period you wish to bypass or remove the EdgeWave Security Suite, simply change your MX Records back to your previous provider.

Creating an Account and Logging into the Customer Portal

EdgeWave offers messaging security customers access to a user portal with an easy-to-use, web-based UI with a single integrated console:

- All of EdgeWave's email security services are **Fully Hosted Solutions**, significantly reducing the time and resources you need to spend on email security administration.

 *Because you have chosen a SaaS solution and a fully hosted service, your email security services are always up to date and managed for you. This means you are free to focus on other crucial IT issues.*

- **Centralized Management from a Web-Based UI** enables all administrative tasks to be performed efficiently and easily.

 *Provision your email security services from one, easy-to-use portal. The user interface makes it easy to provision email accounts, set up Domains, and run reports. Your email security suite will be up and running in no time.*

Setting up a User Account and Logging into the User Interface

1. Navigate your web browser to <https://portal.edgewave.com>
2. Register as a New Customer, log in to the Portal, and accept Terms and Conditions
3. Create an account by clicking on "1 Add Accounts".



4. Fill out new account form. (**Bold** fields are required).
5. Click Save.
6. Once saved, select your account in "2 Configure Services" to configure your subscription services.



The Base For Email Security - Email Filtering



About Email Filtering

EdgeWave's email filter (EMF) service is much more than a simple Spam Filter. It includes both inbound and outbound filtering services that utilize the latest in multi-layer protection, including our superb Zero Minute Defense technology.

- **Inbound Filter:** EdgeWave's inbound email security filters spam, viruses, and other malware through a filter stack of 13 filters. One of the filters is EdgeWave's "**Zero Minute Defense**" – a human team of analysts, who constantly write custom rules for our clients to make sure you are protected against the latest email threats. This **Multi Layer Protection** ensures you are always protected in the best possible way with the lowest possible number of False Negatives or False Positives. EdgeWave's email filters sit in front of your corporate networks and offer **Perimeter Defense**. They filter emails BEFORE they reach your servers and computers.



You get the best possible, thorough protection against inbound email threats. Human review teams ensure the fastest possible reaction to any new threat. EdgeWave's Perimeter Defense significantly reduces the bandwidth needed by your servers, because all spam and threats get eliminated before they reach your network.

- **Outbound Filter:** EdgeWave's outbound filters ensure that no sensitive data or profanity, as defined by **HIPAA/Financial Regulatory Requirements** and your **Acceptable Use Policy** gets sent from your network. This is valuable compliance protection, and ensures the reputation and security of your company. Outbound filters also successfully detect **Botnet Activity**. Additional outbound protection is offered through EdgeWave's **DLP** service, which additionally scans outbound email attachments. (For more information on DLP, please refer to the appropriate section in this guide.)



Protect your company, your customers, and your reputation effectively with EdgeWave's Outbound email filter. In addition to regulatory compliance, our outbound filters also ensure you will not be black listed because of Botnet activity from your network.

Setting up Inbound Email Filtering

1. Set up domain

- Click on **Add Domain** link.
- Enter Domain Name in the **Add Domain** field. (i.e: mail.yourcompany.com)
- Choose **Mailbox Discovery** method
- Enter Mail Gateway
- Click Save

2. Configure services – There are 4 items to configure to activate inbound service. In order:

- Make sure your filter settings comply with your email usage policy. (Settings can be changed later by going back to the Settings tab)
- Confirm there is an entry in the Mail Gateways field and it is accepting connections from the EdgeWave IP address range (208.80.200.0/21) (This can be tested by going to the Status tab.)
- Ensure all mailboxes are listed (Mailboxes tab) and/or a Mailbox Discovery method is set up and tested (Settings tab)
- Change domain's DNS MX record to match the 4 custom MX record which are displayed in the Status tab.

Setting up Outbound Email Filtering

1. Set up outbound IP

- Click on **Add Outbound IP** link.
- Enter IP address range in the **IP Address Range** field in CIDR format (i.e 123.45.67.89/32).

2. Configure services

- Make sure your filter settings comply with your email usage policy. (Settings tab)
- Redirect outbound mail from mail server on indicated outbound IP address to custom Outbound host entry (i.e. 123-45-67-89.rcimx.net)

Ensuring Email Continuity



About Continuity

EdgeWave's email Continuity service enables your company to send and receive email during planned or non-planned server outages through an easy-to-use web-based console. Continue business operations even when your servers are down due to a catastrophic event with EdgeWave's **MTA Agnostic** Continuity service. Implementation is as easy as checking a box in your Administrative dashboard.



Loss of email availability for just a day could cost your business a fortune. With EdgeWave's email Continuity service you ensure continued email operations, even if the unforeseeable happens.

Setting up Email Continuity

1. Continuity is designed to be activated when the Mail Gateway is not accepting connections.
2. Continuity is manually enabled on the Domains Settings page. Simply check the box to enable access.

Routing and Session Management

Block messages larger than megabytes.

Spool messages for up to hours.

Journaling

Send a copy of every delivered message to:

Enable Email Continuity (only use during downtime)

Keep a copy of messages delivered to the Mail Gateway

3. A separate authentication list can be set up for users to access their Personal Dashboard using temporary static passwords. Authentication can be set up using the Composite Verifier feature. Please refer to the Administration Guide for more details on this feature.

Protect Sensitive Data with DLP



About Data Loss Protection

EdgeWave's Data Loss Protection (DLP) service is an excellent tool for **Regulatory Compliance** with regulations such as HIPAA or SOX, and for enforcement of **Acceptable Use Policies**. The service is a great complement to Outbound Filtering. DLP scans outgoing attachments against healthcare, financial, or custom-built dictionaries to ensure confidential data stays safe and protected. The built-in **Encryption Trigger** is optional and can trigger the automatic encryption of sensitive data before it is being sent.



Be Government Compliant and enforce Acceptable Use Policies with technology that is transparent and easy to use. EdgeWave's Data Loss Protection service works hand-in-hand with the other email security services to offer excellent data loss protection of data in motion.

Setting up Data Loss Protection

Data Loss Protection is configured on the outbound IP Settings tab. Simply set the dispositions for the 3 additional categories for Compliance – Health, Compliance – Finance and Profanity.



Secure Email Delivery with Encryption



About Encryption

EdgeWave's Encryption service utilizes **Park and Pull** and **TLS** technology to ensure secure message delivery. This easy-to-use service delivers your encrypted messages to a secure portal, from which any email recipient can pick them up after proper authentication. Messages can automatically be sent encrypted after being identified as containing sensitive data by the service. Alternatively, senders can manually encrypt messages with the optional **Outlook Plugin**. There is no software download necessary for the recipient to receive an encrypted message.



EdgeWave's encryption service integrates seamlessly with the other email security services such as DLP and outgoing email filtering. It is easy to implement and use for both sender and recipient. Set the service to automatically encrypt messages containing confidential information, or manually encrypt messages as needed. The choice is yours. Park and Pull technology ensures you can send encrypted messages to anyone, because there is no need for additional software downloads.

Setting up Encryption

Before the encryption service can be used a Special Route must be defined on the Outbound IP Settings page. Go to Outbound IP and add your outbound IP address. Select the Route to Encryption Server option and then set the filter action to Special Routing for those filters you wish to have route mail to the encryption server.

Special Routing

Define the route to be used for the **Special Routing** message action.

Route to Secure Mail Delivery Enable read receipt

Custom:

Boundry Encryption

Route to:

Easy Access to Old Emails with Archiving



About Archiving

EdgeWave's Archiving service offers state-of-the-art technology that decreases the amount of archived data by as much as 80%. **Stubbing** significantly decreases and condenses archived data, and is a great way to archive data efficiently and fast to meet **Regulatory Requirements** with minimal impact to your company's resources. Archived data can be held indefinitely in case there is a **Legal Hold**, or for up to 7 years. The Archiving service offers easy **Searchability** and full **Outlook Integration** for easy access in **eDiscovery** situations.



Find old email communications fast and easily with EdgeWave's Archiving service. You need quick access to emails in the event of lawsuits, audits, or other eDiscovery situations. Outlook integration gives select users easy access to the archive without the need for additional software.

Getting Started with Archiving

To get Archiving set up, simply complete the "Archiving Deployment Sheet" your sales rep sent to you. EdgeWave will take care of the rest. The EdgeWave team will be in touch with you as soon as we receive the completed deployment sheet.

Evaluation of the Service / Reporting



EdgeWave's Messaging Security Suite Performance can be evaluated by running reports that return specific information...

1. Message Categories Summary



At a high level, the Messages Categories Summary provides a summary snapshot of your mail domain. In this report, Action (aka Message Disposition), or the action performed by the EdgeWave service such as Delivered, Marked Up, Quarantined, Blocked, or Discarded, is shown in columns, and the Category (OK, Spam, Junk, Adult, etc.) of the messages is shown in rows.

Message Categories Summary

chbx.net
Server: Server:All
for November 2011

Category	Action				Total	Size	
	Accept	Markup	Quarantine	Block			
OK	184				184	41.2%	10MB
Digest	20				20	4.5%	453KB
Invalid Recipient					0	0.0%	0
Junk					0	0.0%	0
Sender	1				1	0.2%	40KB
Keyword					0	0.0%	0
Attachment		3			3	0.7%	145KB
Foreign					0	0.0%	0
RBL					0	0.0%	0
NDR					0	0.0%	0
Virus				15	15	3.4%	440KB
Phishing			2		2	0.4%	10KB
Adult					0	0.0%	0
Spam			72	150	222	49.7%	1,107KB
Bot					0	0.0%	0
Total	205	3	74	165	447		13MB
	45.9%	0.7%	16.6%	36.9%			

2. Virus Attack Detail



Administrators can run a Virus Attack Detail report that shows the date and time of the message, the virus name, source IP address, country of origin, and recipient. You can run reports spanning a user-selected period (from one day up to five weeks). The default report time span is one day. The screenshot below shows a sample Virus Attack Detail report.

Virus Attack Detail

chbx.net
Server: Server:All
for Oct 7, 2011 thru Nov 7, 2011

*(all dates in Pacific Standard Time)

Date/Time	Virus Name	Source IP	Country	Recipient
Oct 7 5:13AM	1800314	210.212.244.50	IN	
Oct 7 5:14AM	Email.Trojan-256	178.94.180.0	UA	
Oct 7 6:25AM	1806495	208.80.204.140	US	
Oct 7 8:42AM	Email.Trojan-256	119.156.18.242	PK	
Oct 8 6:58PM	Suspect.Bredozip-zippwd-6	208.80.204.140	US	
Oct 9 6:07PM	1649352	208.80.204.140	US	
Oct 9 7:49PM	1813845	208.80.204.140	US	
Oct 10 7:26AM	1813274	208.80.204.140	US	

3. Advanced Reports



Advanced Reports are highly customizable, providing all possible details relating to messaging for domains within up to an eight-day period. You can select a tabular or chart output, or both. In tabular format, you can sort the data by column. The screenshot below shows the options available for the report.

Advanced Report

chbx.net
Server: Server:All
for Nov 7, 2011

*(all dates in Pacific Standard Time)

All	Date/Time	From	Subject	Recipient	Category	Action	Detail	Delivery Details
								Disposition
	Nov 7 12:30AM	<digest@redcondor.com>	Spam Digest for Sunday, November 6, 2011	home@chbx.net	Digest	Accept		Delivered
View	Nov 7 12:30AM	<home+bnccaqsa7e9...@chbx.net>	Spam Digest for Sunday, November 6, 2011	alex@chbx.net	Digest	Accept		Delivered
<input type="checkbox"/> View	Nov 7 12:44AM	<sqwvvi@gmail.com>	Super Replicas - Luxury Watches, Bags, Jewelry	home@chbx.net	Spam	Quarantine	1801828	
View	Nov 7 1:01AM	<20111107090145e28...@bounces.amazon.com>	Amazon.com: One-Day Only--\$159.99 for the Garmin nüvi 14...	alex@chbx.net	OK	Accept		Delivered
<input type="checkbox"/> View	Nov 7 1:07AM	<0-ka@hydro.com>	Vacancy - apply online	alex@chbx.net	Spam	Block	1675039	
<input type="checkbox"/> View	Nov 7 1:35AM	<0-2ya.com@returns.groups.yahoo.com>	Career opportunity inside	alex@chbx.net	Spam	Block	1675039	
<input type="checkbox"/> View	Nov 7 2:21AM	<0-xhelgesenhilde...@hemil.no>	Job offer match, respond to apply	alex@chbx.net	Spam	Block	1675039	
<input type="checkbox"/> View	Nov 7 3:16AM	<0-ohen@cea.eop.gov>	Employment you've been searching!	alex@chbx.net	Spam	Block	1675039	
<input type="checkbox"/> View	Nov 7 3:33AM	<info.center@efips.gov>	Your Tax Payment ID 90349410 is failed.	alex@chbx.net	Spam	Block	audleybrass.co.uk	
View	Nov 7 3:52AM	<bounce-2058194_ht...@bounce.emailrestaurant.com>	Hey Early Bird - Catch this Holiday Deal! All Gift Cards ...	alex@chbx.net	OK	Accept		Delivered
View	Nov 7 4:20AM	<10051+10000+61956...@returns.sales.overstock.com>	LAST DAY 10% OFF	terrie@chbx.net	OK	Accept		Delivered