

ePrism Email Security

Welcome to EdgeWave ePrism Email Security!

This short guide is designed to get you up and running with your fully hosted Email Security Suite. It can also be used as a quick reference guide for commissioning and changing the most frequently used features of this man-aged service.

If you have questions beyond what is covered in this document, please refer to the [Administration Guide](#) or visit the EdgeWave Customer Support Portal.

Step 1. 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.

Step 2. Creating an Account and Logging in to the Portal

The customer portal offers an easy-to-use, convenient user interface for your Messaging Security Suite subscription. Here you can provision services, set up users, and add additional services.

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



- D. Fill out the new account form with all information that is required
(Remember when filling out the form to select **Try Data Protection** and **Try Archiving** as shown below):

Try Data Protection		<input checked="" type="checkbox"/>
Try Archiving		<input checked="" type="checkbox"/>
Try Outlook Archive Client		<input type="checkbox"/>
Try an Email Security Package		<input type="radio"/>

- E. Click Save.
- F. Once saved, select your account under "2 Configure Services" to configure your subscription services.



Step 3a. Setting up a Domain

EdgeWave's fully hosted inbound email filtering lowers your network's bandwidth requirements by eliminating spam, and protects your email users, your company, and network from outside threats such as spam, viruses, malware.

1. From the Add New dropdown at the top of your screen select Domain as show in the figure (right)
2. Enter Domain Name in the Add Domain field. (i.e.: mail.company.com)
3. Enter the Mail Gateway information
4. Choose the Mailbox Discovery method (Optional)
5. Click Add



Step 3b. Applying Filtering Settings for Your Added Domain

Next screen that appears you will need to setup your new domain options. There are a few important items on this page to fill in to get your Inbound Mail set up.

- A. Make sure you are comfortable with the filter settings as shown in hte figure (below)

Blocked Messages	Permanently discard	▼
Virus	Block	▼
Phishing	Quarantine	▼
Adult	Block	▼
Spam	Quarantine	▼
Bot	Quarantine	▼
Junk	Markup	▼

- B. Confirm that 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 after required IP addresses have been entered and a test email has been sent)

- C. Change your domain's DNS MX record to match the four custom MX records which are displayed in the Status Tab and look similar to these examples below(Note: Items in red will be your mx record):

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

ePrism Email Security

Step 3c. Adding Mailboxes to your Domain

- A. From the Add New dropdown select Mailbox
- B. Choose the Domain Name that you want these mailboxes to populate within.
- C. Be sure to use a separate line for each mailbox.
- D. After all desired mailboxes have been entered simply click Add.

Add Mailboxes

Domain Name

Add Mailboxes

Step 3d. Set spooling settings

The default setting for spooling is 2 hours this can be set to a maximum of 160 hours. There is no limit for the number of messages or size of mail messages during this period.

▼ Routing and Session Management

Limit message size

Block messages exceeding megabytes

Spool messages for up to hours

Send copy of every delivered message to

Keep a copy of messages delivered to the Mail Gateway

Domains required to use TLS: +

Anti Spoof Protection

Enable global protection

Enable smart protection

Step 3e. Cut over inbound filtering

The last step in setting inbound filtering is to change existing records to the new records. The new mx records can be found in the status link at the top of your domain settings page for ePrism. It is VERY important that all previous steps are completed BEFORE changing the MX records to avoid interruptions in mail service. Assuming ePrism is able to successfully deliver mail to your gateway there will be no interruption in mail delivery during the change. The graphic below is an example of mx records that will be changed found under the status link as mentioned above.

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

ePrism Email Security

Step 4a. Setting Up Outbound Email Filtering

Outbound email filtering ensures you are not sending sensitive data, or distributing viruses and malware unknowingly via email to your network. This service also ensures you will not end up on black lists because of Botnet activity or spam messages.

First add an Outbound IP

1. Click on the Outbound IP link from the Add New dropdown menu.
2. Enter the IP address of the sending mail server in the IP Address Range field in CIDR format (i.e. 123.45.67.89/32).
3. From here you can now setup your filtering settings for Outbound mail.

Step 4b. Setting Up Data Loss Protection (DLP)

In addition to Outbound email Filtering, DLP or Data Loss Protection, scans all outbound attachments in your email for potentially sensitive data to protect your company and comply with health care or financial regulations. DLP Categories are able to scan over 250 different categories of attachments.

Data Loss Protection is configured on the Outbound IP settings tab. Simply set the dispositions for Adult, Spam, Social Security or Credit Card as seen in Figure 4.1

Blocked Messages	System quarantine ▼
Virus	Block ▼
Phishing	Quarantine ▼
Adult	Block ▼
Spam	Quarantine ▼

Step 4c. Setting Up Encryption and Special Routing

When you need to send sensitive information via email it remains vulnerable to third party interception. With EdgeWave's encryption service, you ensure that only the recipient can view the sensitive email. You can also set your DLP service to automatically trigger encryption of emails containing specific content.

Before the encryption service can be used a Special Route must be selected in your Special Routing section of the Outbound IP Settings page. These choices can be found within the Outbound IP filter options as shown in the figure below:

Social Security	Block ▼
Credit Card	Allow
Compliance - Health	Markup
Compliance - Finance	Quarantine
Profanity	Block
	Special Routing
	Attach Encrypted
	Quarantine ▼

ePrism Email Security

Step 4d. Cutting over outbound filtering

In order to cut over outbound filtering configuration for an outbound send connector will need to be configured with smart-host routing pointing to the FQDN found under the status link of the outbound settings page. This FQDN is unique to your outbound IP and any traffic sent to this address will have the outbound settings applied.

Outbound Host

Set your SmartHost entry in your outbound mail server to the following hostname to enable outbound filtering:

172-27-46-250.selab.rcimx.net

The hostname listed here can only be used if EdgeWave is managing your outbound DNS records. Go to the Appliance Dashboard to configure this setting.

Step 5. Getting Started with Archiving

Government and Industry regulations very often require companies to keep email for a number of years, in case of legal or auditing issues. EdgeWave's Archiving service makes it easy for you to archive your email for a number of years. In addition, our easy search function enables you to quickly find any email, even if you sent it 7 years ago.

To get Archiving set up, simply follow the Archiving Deployment Sheet your Sales Rep sent you. EdgeWave will take care of the rest. The EdgeWave team will contact you as soon as we receive the completed deployment sheet.

Where to go for more Information

- a. End User & Administrator resources: <http://www.edgewave.com/support/eprism/documentation/>
- b. Product Information: <http://www.edgewave.com/products/email-security/>

Adding Services to Your Subscription

If you see a service that interests you but haven't subscribed to yet, please contact your Sales Rep at (855) 881-2004.