

Messaging Security Suite



800-782-3762
www.edgewave.com

Red Condor is now EdgeWave

EdgeWave acquired Red Condor in 2010 to add comprehensive Messaging Security to the already existing web security solutions offering.

© 2001 - 2011 EdgeWave. All rights reserved. The EdgeWave logo is a trademark of EdgeWave Inc. All other trademarks and registered trademarks are hereby acknowledged.

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

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

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

PDFAQHigh08.2.0.001

Contents

Personal Dashboard	1
What is the Personal Dashboard?.....	1
How do I get to the Personal Dashboard?.....	1
How do I release a message from the Personal Dashboard?.....	1
How do I delete messages listed in the Personal Dashboard?.....	1
How can I access my email when the mail server is down?.....	2
The Spam Digest	3
What is the Spam Digest?.....	3
What do I do with the Spam Digest?.....	3
How do I view a message listed in the Spam Digest?.....	3
How do I release a message from the Spam Digest?.....	4
How do I delete messages listed in the Spam Digest?.....	4
I don't want to see the Spam Digest. What do I do?.....	4
How do I change the frequency that I receive the Spam Digest?.....	4
Are there any other Spam Digest options?.....	4
Quarantined Messages	5
What are quarantined messages?.....	5
How can I find a message?.....	5
Can I change the quarantined message display?.....	5
What username and password do I use to access my quarantined messages?.....	6
Filtering Options	7
How does filtering work?.....	7
Do I need to worry about viruses?.....	7
What are my filtering options?.....	7
What are Administrator settings?.....	7
How do I view or change my filtering options?.....	8
What is "phishing"?.....	8
What is a bot?.....	8
What are subject tags?.....	8
How do I configure a subject tag?.....	9
How do I select which foreign characters to filter or tag?.....	9
Why are attachments risky?.....	9
How do I select which attachments to block, filter, or mark up?.....	9

Whitelists and Blacklists	10
What are "Friends" (Whitelist) and why do I need to tell you about them?.....	10
How do you add someone to the Friends whitelist?.....	10
What are "Enemies" (Blacklist)?.....	10
How do you add someone to the Enemies blacklist?.....	10
Can I view my Friends and Enemies lists?.....	11
How do I remove someone from my Friends or Enemies list?.....	11
How Messaging Security Works	12
How do you identify spam?.....	12
Is somebody reading my mail?.....	12
Will the filtering delay my mail?.....	12
Can I run the filtering software on my computer?.....	13
Problems?	14
What if my password doesn't work?.....	14
Some spam still gets through to my mailbox. What do I do?.....	14
I mistakenly released a spam message. What happens now?.....	14
Why am I getting returned mail as "Undeliverable" or "NDR"?.....	14

Personal Dashboard

What is the Personal Dashboard?

The Personal Dashboard is your control panel for managing your email filtering settings. It allows you to view and release quarantined messages, create and change your Personal Dashboard password, customize your digest options, configure your mail filtering preferences, manage your whitelist and blacklist, and view your account status.

How do I get to the Personal Dashboard?

Click the **My Account** link in the upper right corner of the Spam Digest to open the Personal Dashboard Login screen. If needed, enter your username and password to enter the Personal Dashboard.



Note: The Personal Dashboard opens to the version (low- or high-bandwidth) that you used the last time you logged in. To switch, click the link at the bottom of the login page.



Tip! Bookmark the login page in your browser for easy access.

How do I release a message from the Personal Dashboard?

You can release one or more messages from the quarantine to be delivered to your email inbox. Click the Messages tab, then select the messages to release and click **Release**. The messages are sent to your email inbox.

How do I delete messages listed in the Personal Dashboard?

You do not need to delete messages from your quarantine. All messages are automatically deleted after 35 days. You can, however, manually delete messages from your quarantine. Click the Messages tab, then select the messages to delete and click **Delete**. The messages are deleted.

How can I access my email when the mail server is down?

Email Continuity provides access to your email inbox when your regular email server is down. If your organization has licensed this feature AND your system administrator has enabled it, you can use the Messages tab of the Personal Dashboard to manage all of your incoming messages.

When Email Continuity is active, an additional button, Inbox, appears on the Messages tab.



Note: Depending on the settings applied by your email administrator, Email Continuity may or may not be available to all users.

The Spam Digest

What is the Spam Digest?

The Spam Digest has two main functions. It provides:

- A list of your quarantined email identified as spam, junk, or containing a virus or other dangerous content since the last digest.
- An entryway to your personal dashboard where you can manage your account and customize your digest. You can review quarantined messages and release them if needed.



Tip! Click the **my account** link near the top right of the Spam Digest to open the login screen of the Personal Dashboard in your browser. Then bookmark this page in your browser for easy access.

What do I do with the Spam Digest?

You don't have to do anything! The messages listed in the Spam Digest have already been filtered.

The Spam Digest summarizes the filtering activities for your account since the last digest. You may choose to review the list of messages for any valid messages that were mistakenly filtered out.

The Spam Digest requires no user action to delete the spam/junk mail listed in the summary. They are deleted automatically after 35 days. Alternatively, you can log into the Personal Dashboard, select one or more email messages, and delete them manually.



Note: You only receive a spam digest if you have received messages that have been blocked or quarantined during the latest digest period.

How do I view a message listed in the Spam Digest?

If you have permission, click the **View** link to the left of the message in the list you want to view. Depending on system administrator settings, you may need to log in. Your message is highlighted in the Messages page of your Personal Dashboard. You can view the message in the bottom panel of the Messages page.

How do I release a message from the Spam Digest?

Click the **Release** link to the left of the message in the list. The message will be immediately sent to your email inbox.

How do I delete messages listed in the Spam Digest?

There is nothing to do. The spam messages listed in the Spam Digest have already been filtered. These messages will automatically delete after 35 days. Each digest you receive lists only the new filtered mail, while the older filtered mail is not shown.

If you want to delete messages before the 35 days, you can do this in the Personal Dashboard. See [Personal Dashboard](#) for details.

I don't want to see the Spam Digest. What do I do?

Click the **Unsubscribe** link in the bottom left corner of the Spam Digest. It will no longer be delivered to your email inbox.

How do I change the frequency that I receive the Spam Digest?

The digest delivery frequency can be set to daily, weekly, monthly, or never. By default, the Spam Digest is sent out daily. You can change the frequency in either of two ways:

- From the Spam Digest, click the **Change Report Frequency** link.
- From the Personal Dashboard, click the **Settings** tab.

Are there any other Spam Digest options?

From the Personal Dashboard, you can also select:

- Whether to receive the report in HTML, text, or multipart format
- Which types of messages to include in the digest by content
- The sort order of the message list
- Your time zone

Quarantined Messages

What are quarantined messages?

Quarantined messages are the messages that the system has kept and not delivered to your inbox. The Spam Digest posts a summary of the quarantined messages for your account for the previous day. Quarantined messages are archived for 35 days online.

You can view your quarantined messages on the Personal Dashboard. You can also set the sorting order of the messages.

How can I find a message?

You can search for any text string in any field displayed in the Messages tab. Just enter the text in the search box. The quarantine list filters automatically. For instance, if you are looking for an email from your cousin Dan (dan@example.com), you can enter Dan in the search box. Any messages from dan@example.com will display, as will messages that have the words dance, dandruff, or danger in the subject line.



Note: Search does not examine the contents of the message. Therefore, you cannot search for text in the message body.

Can I change the quarantined message display?

Yes, you can select the attributes of the quarantined email list. The configurable list can display one or more of the following columns:

- Category: the type of message (such as spam or virus)
- Cause: the reason the message was caught by the filter
- Date: the date and time the message was received
- Sender: SMTP envelope address of the sender
- From: the display email address of the sender
- To: the message recipient's email address
- Country: the character set used in the message
- Size: the size of the email in bytes

- **Filter:** the filter rule that caused the message to be quarantined
- **Zone:** the severity of the potential email threat
- **Subject:** the subject line of the message

To configure your quarantine display:

1. Hover your mouse over one of the column headings to display the downward triangle icon on the right.
2. Click **Columns**.
3. Select the check box of any column to display. Deselect any column to hide.

What username and password do I use to access my quarantined messages?

Depending on the configuration set by your system administrator, you may be able to sign up on the Personal Dashboard and set your password.

1. Click the Personal Dashboard link in the second paragraph of the Spam Digest to open the Personal Dashboard Login screen.
2. Click **Signup**.
3. Enter your email address and create a password.

If this does not work, contact your system administrator.

Filtering Options

How does filtering work?

The system flags messages that have suspicious content and sorts them into one of the danger zones based on the potential harm they could cause you or to your computer. In increasing danger, mail is classified into the following zones:

- **Green Zone:** Junk mail, including unsolicited advertising
- **Yellow Zone:** Suspicious mail, including blank, foreign, and with attachments
- **Red Zone:** Potentially dangerous, including spam, virus, and adult

Do I need to worry about viruses?

The system filters all email through two separate anti-virus programs. If your email has a virus, we will catch it.

What are my filtering options?

Depending on how aggressively you want to filter your email, you can configure each of the filtering categories to block the messages (delete them immediately), quarantine the messages for review, forward the messages to your mailbox with a tag in the subject line, or allow the messages to pass directly to your mailbox without a tag.



Note: You cannot modify a filtering option your administrator has set to block.

What are Administrator settings?

The Administrator settings icon on the Policies tab denotes a filtering option that has been configured by your system administrator. These settings cannot be removed, but they can be modified if permitted.

How do I view or change my filtering options?

Log in to the Personal Dashboard and select the Policies tab. This tab displays your current settings. You can change a setting for most filtering categories by selecting a different option from the drop-down list to the right of the message type.

Change foreign and attachments settings by right-clicking the item and selecting an option from the pop-up window. You can add a file extension to the Attachments list by typing in the extension in the text entry box, selecting the filtering option from the drop-down list, and clicking the plus sign button.



Note: You cannot modify a filtering option your administrator has set to block.

What is "phishing"?

Phishing messages fraudulently attempt to lure the user into giving up personal information such as credit card numbers, passwords, and social security numbers. They appear to originate from banks, department stores, online merchants, and other trusted sources.

What is a bot?

A bot is an autonomous piece of software used by criminal hackers to infect computers, which then come under the command of the hacker. A network of these hijacked PCs is called a botnet, and it is often used to send spam. EdgeWave Email Security defends against bot infections on both the inbound and outbound mail streams.

What are subject tags?

Subject tags are short bits of text (up to 50 characters) prepended to the subject line of an email message to alert you that a message has been flagged as suspicious. You can use the tags to set up filtering rules in your mail client.



Note: We recommend ending the subject tag with a colon. When sorting on the subject line, most mail programs ignore the text before a colon and sort on the content of the rest of the subject line.

How do I configure a subject tag?

Log in to the Personal Dashboard and select the Policies tab. For each filtering option that you want to tag, select Markup from the drop-down list. A new text box appears to the right of the drop-down list. Type your text entry into the box.

How do I select which foreign characters to filter or tag?

Log in to the Personal Dashboard and select the Policies tab. In the Foreign section, right-click the character set and select an option from the pop-up window.

Why are attachments risky?

Some attachments can contain potentially harmful programs, such as viruses, spyware, and keyboard loggers that can cause loss of data and/or personal information. We recommend that you never open an attachment from senders you do not know, or those from senders you DO know, but from whom you were not expecting a file.

How do I select which attachments to block, filter, or mark up?

Log in to the Personal Dashboard and select the Policies tab. In the Attachments area, right-click the attachment type and select an option from the pop-up window.

You can add a new attachment type by entering the file extension in the leftmost text box, selecting the action from the drop-down list, and clicking the green plus icon. For marked up attachments, you can enter the subject tag in the rightmost text box.

Whitelists and Blacklists

What are "Friends" (Whitelist) and why do I need to tell you about them?

The Friends whitelist contains email addresses and domains of those individuals and organizations that you trust. Only add an entry to the Friends whitelist if the sender sends you spam that you actually want to receive. For example, you may be on a large mailing list that would be flagged as a bulk mailing.

How do you add someone to the Friends whitelist?

There are two ways to add someone to the Friends whitelist from the Personal Dashboard:

- If the mail has already been filtered and you want to release it, select the message you want to release from the Quarantine tab and click the Release icon. The message is released to your mailbox. You can opt to add the user to your Friends whitelist.
- If the mail has not yet been filtered and you are adding the address as a precaution, select the Policies tab. Scroll down to the Friends section and enter the email address, domain, IP address, IP address / mask, or country code.



Note: We strongly advise using the system for a month or more before adding anyone to your whitelist. Our extensive testing indicates that whitelists are more effective when they are used sparingly.

What are "Enemies" (Blacklist)?

If you have a legitimate sender that you do not want to receive further email from, you can add an entry (email address or domain) to the Enemies blacklist.

How do you add someone to the Enemies blacklist?

From the Personal Dashboard, select the Policies tab. Scroll down to the Enemies section and enter the email address, domain, IP address, IP address / mask, or country code.

Can I view my Friends and Enemies lists?

From the Personal Dashboard, select the Policies tab. Scroll down to the Friends or Enemies section. Your personal list displays. If your administrator has set up a domain Friends or Enemies list, you can click the hyperlink to view this list.

How do I remove someone from my Friends or Enemies list?

From the Personal Dashboard, select the Policies tab. Scroll down to the Friends or Enemies section. Your personal list displays. Select the name or names to delete, and click the Delete icon.

How Messaging Security Works

How do you identify spam?

The system investigates bulk email that is captured from numerous decoy mailboxes worldwide. When these mailboxes receive a suspected message, we classify the content.

We use the following filtering techniques:

- Signature filtering for virus detection
- Real time blacklists
- Message rate throttling
- Reputation scores
- Message finger print analysis
- Graphic image analysis
- Verifying recipient account name
- String based text rules
- Pattern rules
- Human review

Is somebody reading my mail?

No. We filter mail through a series of rules-based programs to flag suspicious messages. The only time a person looks at a specific message is if it has been sent to a decoy account or a wrong address, or is flagged by a user and sent to us for analysis.

Will the filtering delay my mail?

The filtering process typically introduces a delay of less than one second.

Can I run the filtering software on my computer?

No, the system is a hosted gateway solution without client software. Users manage their account settings through a Web browser. This means there is no software on your computer to install, configure, or maintain.

Problems?

What if my password doesn't work?

If you forget your password, or your password does not work, click the Forgot Password link, enter your email address, and a new password will be emailed to you.



Note: Contact your system administrator if you receive an error message after trying to sign in or have your password sent to you.

Some spam still gets through to my mailbox. What do I do?

Our thousands of decoy mailboxes typically identify and block new spam campaigns within minutes. If you continue to receive spam, please forward samples as attachments to spam@edgewave.com so that we can improve the quality of this service.

I mistakenly released a spam message. What happens now?

Released messages are automatically sent to your email inbox. This does not, however, affect future spam filtering. Identical spam will still be quarantined in the future.

Why am I getting returned mail as "Undeliverable" or "NDR"?

Recently many users have received NDR (Non Delivery Receipt) or “bounceback” messages. Bounceback/NDR messages are standard messages that notify a sender of a failed delivery. This mechanism has now been hijacked by spammers.

How it works: Spammers are using email addresses of known valid users to broadcast large volumes of messages pretending to be from those valid email addresses. Then, when hundreds or even thousands of those messages reach invalid recipients, the receiving mail servers “bounce” the message back to the users whose email addresses had been used for the campaign. Some users have received several hundred of these bounced messages in a given day.

This condition affects mail servers throughout the Internet. You are not responsible for your email address being used in this manner. There is no action you can take to prevent this misuse from happening. If you continue to get this type of spam, please forward samples as attachments to spam@edgewave.com so that we can improve the quality of our service.

Corporate Office

15333 Avenue of Science, San Diego, CA 92128

Phone: 858-676-2277

Toll Free: 800-782-3762

Fax: 858-676-2299

Email: info@edgewave.com