



Release Notes for Version 8.0

Document issue:	1.3
Date of creation:	3/28/11
Date of last revision:	4/13/2011 9:09:00 AM
Classification:	Commercial in confidence –
Distribution: <input checked="" type="checkbox"/> Electronic <input type="checkbox"/> Hardcopy only	Restricted to: Internal and current customers only

Summary:

This document covers a major Release 8.0 providing new features, enhancements and bug fixes.

PROPRIETARY INFORMATION

Not to be reproduced or made available to third parties without prior consent from Red Condor and not to be used in any unauthorized way



Table of Contents

1# Overview	3#
2# New Features	3#
2.1# Email Data Compliance.....	3#
2.2# Support for multiple IP addresses	3#
3# Feature Enhancements	4#
3.1# Additional Enhancements.....	4#
3.1.1# XML API Changes.....	4#
4# Fixed Bugs	5#
4.1# 1355 Report Subscription Service is not Time Zone aware.....	5#
4.2# 6092 Pipe () character inhibiting inbound message processing	5#
4.3# 6263 Dashboard HTTP session is not maintained when there are multiple A records.	5#
4.4# 7894 "Release Wizard" in Personal Dashboard does not always get displayed.....	5#
4.5# 7956 Display of alerts on Appliance dashboard does not always get displayed.....	5#
4.6# 8094 Loopback text is incorrect.....	5#
4.7# 8123 Outbound spooler duration is not honored	5#
4.8# 8129 Spooling when primary gateway is unroutable and random gateway distribution is used	5#
4.9# 8195 Help link does not work on Preferences>Branding page.....	5#

1 Overview

Release 8.0 is a major release that includes several new features, some enhancements and bug fixes. In addition the system has been rebranded as EdgeWave.

2 New Features

Below is a list of new features that have been added to our messaging security solution.

2.1 Email Data Compliance

Provides new content analysis that uses proprietary logic and lexicons to protect private or regulated content from leaving the premises via your outbound email stream. Policies support compliance regarding:

- Exposure of personal health care information
- Capture of financial information
- Credit Card Matching
- Social Security number matching
- Profanity

Administrator's now can control any messages that contain such regulated content and choose to allow, mark up, quarantine or block such transmissions. Full attachment scanning is also provided for each outgoing message. Easy to configure using simple drop down treatments for each new category: health, finance and profanity takes all the guesswork out of your email compliance efforts.

This feature requires an additional license and it's configurable through your current Admin Dashboard. These feature can be enabled for both hosted and appliance customers.

2.2 Support for multiple IP addresses

New ability to set up multiple IP addresses on the MAG appliance Ethernet interface(s). The appliance can be configured to send and receive mail on multiple IPs through the appliance dashboard via the Network Tab. An IP can be set to receive inbound and outbound or outbound only. All other application settings apply to all the IPs configured.

This feature will be available at no additional cost for all appliance customers.

3 Feature Enhancements

Below is a list of feature enhancements that have been added to our messaging security solution.

3.1 Additional Enhancements

- a. Administrators can now view message attachments in the Advanced, Recent Activity, Quarantine and Delivered Messages reports.
- b. The Domain mailbox list can now be downloaded from the Administrator dashboard Domain Mailboxes page.
- c. Spam determined to come from a Bot is now separated out in a different category named Bot. Users can dispose of this type of mail differently from regular spam.
- d. System Administrators can now configure brand defaults for Domain and Outbound IP settings.
- e. Weak ciphers configuration is now independent of the use of HTTPS in the Appliance dashboard.
- f. Support for authentication continuity has been added. Through the use of new Static and Composite Verifiers dashboard authentication can continue to function even when one Verifier is not accessible. The Composite Verifier contains both a dynamic Verifier such as LDAP and a Static Verifier, which is a locally stored user and password list. When the LDAP Verifier is not available the Static Verifier is checked instead.
- g. Automatic mailbox deletion now includes both active and unprotected mailboxes.
- h. When the Domain Authentication setting is Internal the Administrator can set user passwords.
- i. DNS/Mx Record is now used to resolve the destination server for all out going messages. Prior to this release outbound messages to local domains always went to the defined mail gateway without the use of Mx record look up.

3.1.1 XML API Changes

- a. Domain and Outbound IP settings have been split. There is now an <Outbound> element for configuring Outbound IPs.
- b. The addition of default settings for Domains and Outbound IPs.
- c. Additional Domain, Outbound & Mailbox attributes to support the new features.

4 Fixed Bugs

- 4.1 **1355** Report Subscription Service is not Time Zone aware
- 4.2 **6092** Pipe (|) character inhibiting inbound message processing
- 4.3 **6263** Dashboard HTTP session is not maintained when there are multiple A records
- 4.4 **7894** “Release Wizard” in Personal Dashboard does not always get displayed
- 4.5 **7956** Display of alerts on Appliance dashboard does not always get displayed
- 4.6 **8094** Loopback text is incorrect
- 4.7 **8123** Outbound spooler duration is not honored
- 4.8 **8129** Spooling when primary gateway is unroutable and random gateway distribution is used
- 4.9 **8195** Help link does not work on Preferences>Branding page