

2015 Release 1 Notes for Websense Cloud Email Protection Solutions

TRITON AP-EMAIL with Email Cloud Module |13-Jan-2015

To address the wide-scale adoption of cloud and mobile technologies, along with a rapid growth in distributed workforces, Websense, Inc., is excited to launch a new, industry-leading security suite – [Websense® TRITON® APX 8.0](#). This new modular platform provides **advanced threat and data theft protection** for organizations that wish to embrace new technologies and working practices. TRITON APX provides protection across the entire kill-chain, reveals actionable intelligence, and enables real-time feedback to educate and motivate end users to avoid risky behavior. This product release is the culmination of eighteen months of business transformation and innovation. As a result, Websense customers are now able to maximize the unparalleled protection and ROI of Websense TRITON APX solutions well into the future.

The 2015 Release 1 product release adopts a new product naming and grouping of the familiar Websense TRITON product line.

Original Name	New Name
Websense Cloud Email Security	Websense TRITON AP-EMAIL with Email Cloud Module

Previous product functionality remains intact. The user interface has the same look and feel, and the core product continues to provide the strong protections you've come to rely on.

In addition to new names, our cloud email protection solution offers new features and includes product corrections. Refer to the information provided in these Release Notes for additional product information:

- ◆ *What's new in 2015 Release 1?*
 - *Antispoofing improvements*
 - *Bulk spam messages cannot be released via EUMRs*
 - *Improved EUMR processing in different timezones*
- ◆ *Resolved issues in this release*

What's new in 2015 Release 1?

Antispoofing improvements

The Spoofed Messages options on the Antispam tab now include a **Verify “From” address displayed to end users** check box. Select this to check if both the address the message recipient sees in the From: field and the envelope sender address match domains defined in your policies.

If you select this option, one of the following happens:

- ◆ If the envelope sender address does not match one of your policies but the From: address does match, the cloud service performs message authenticity checks on the From: address.
- ◆ If the envelope sender address matches one of your policies, the cloud service performs message authenticity checks on the envelope sender only.

If this option is not selected, the From: address is ignored and authenticity checks are performed only on the envelope sender if it matches one of your policies.

This option is disabled by default. If you have other organizations authorized to send messages on your behalf, you should ensure that your SPF records include the IP addresses of those organizations before enabling the option, otherwise those messages will be detected as spoofed.

Note that this feature is unrelated to the existing **Apply whitelist matching on spoofed email addresses** option, which is unchanged.

Bulk spam messages cannot be released via EUMRs

The “Release” option in the End-User Message Report has been removed for messages that were quarantined as bulk spam. Only administrators can release bulk spam messages via the cloud portal.

Improved EUMR processing in different timezones

The processing of EUMRs in different timezones has been improved in this release. When adding a new recipient on the Subscriptions tab, the Timezone drop-down list now includes locations rather than just offsets to GMT. The cloud service ensures that any alterations for the listed locations (for example, to daylight savings time) are set automatically.

If you imported subscriptions in bulk using a CSV file, you need to download and edit your current subscriptions so that they use location-based timezones rather than

offsets. To assist with this, you can download a list of all the supported timezones in CSV format from the Bulk Upload tab.

Resolved issues in this release

- ◆ HTML code in a message was being corrupted during processing.
- ◆ The logs for some quarantined messages were unavailable for review.
- ◆ Some parked attachments could not be retrieved due to incorrect decoding of the content.
- ◆ If there are no results, the Quarantine Audit Trail now displays “No matching records found” rather than “Page cannot be displayed”.
- ◆ Portal tables were missing dividing lines in Internet Explorer 8.
- ◆ The unique pass phrase answer can now be changed on the **My Account** page.

Technical Support

Websense provides technical information about Websense products online 24 hours a day, including:

- ◆ latest release information
- ◆ searchable Knowledge Base
- ◆ show-me tutorials
- ◆ product documents
- ◆ tips
- ◆ in-depth technical papers

Access support on the website at:

www.websense.com/content/support.aspx

If you need additional help, please fill out the online support form at:

www.websense.com/content/contactSupport.aspx

Note your case number.

Third-Party Software Notice

Websense, Inc., provides software solutions that integrate with your existing environment. In the complex environments that are common in today's marketplace, this involves interacting with a variety of third-party software products. In some cases, Websense, Inc. makes an effort to simplify the acquisition of this third-party software. However, you must obtain any upgrades and enhancements to those products directly from the third-party vendor.

If you have questions, contact Websense Technical Support for additional information.

©1996–2015, Websense, Inc. All rights reserved.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.