2015 Release 5 Notes for Websense Cloud Email Protection Solutions

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

2015 Release 5 of our cloud email protection product includes the following product updates and corrections.

What's new in 2015 Release 5?

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

Outbound mail connectivity testing

The mail connectivity test available has been extended to provide testing for outbound mail. The test requires sender and recipient information to perform checks on whether mail is being routed correctly.

To perform an outbound mail test:

1. Go to **Email** > **Messages > Toolbox**.
2. Select the **Outbound Mail Test** tab.
3. Enter a sender address. This must be for a domain registered and checked with your cloud service account.
4. Enter a recipient address.
5. Click **Run Test**.

Running the test does the following:

- Checks the outbound route connectivity to the recipient domain
- Generates a message from the cloud email service to your selected recipient domain using TLS

Administrator password expiration limit warning

A warning that a password expiration limit of 90 days or fewer is recommended now appears in the following cases:

- When you go to **Account > Contacts**, and click **Edit** under Account Management
- When you edit a contact's login details, and select a value greater than 90 days from the **Expire password** drop-down list.

This recommendation is for both security best practice and PCI compliance purposes.

Links to data security and privacy information

A new Privacy & Security option has been added to the Help menu in the Cloud TRITON Manager. The documents accessible from this menu item include:

- the Websense Privacy Policy
- an Information Security statement for Websense cloud services
- information about ISO27001 certification

Resolved issues in this release

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

- URL sandboxing was not working correctly for customers who also have TRITON AP-WEB with Web Cloud module.
- The Account Summary report was showing a total count of 0 for all rows rather than the actual number.
- Bulk spam messages could be released from the message details page in an end-user message report.
- New messages have been added to the message log list to cover situations where whitelist entries have been ignored, either because the address is spoofed, or because the sender cannot be validated.
- The Check SMTP Connectivity option for secure transport rules was causing untrusted connection notifications for a specific cloud service cluster.
- The **Account > Privacy Protection** page, which is specific to TRITON AP-WEB, was visible to email customers.