

2016 Release 3 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 28-July-2016

2016 Release 3 of our cloud email protection product includes the following product updates and corrections.

- *What's new in 2016 Release 3?*
 - *Customizable block and notification pages*
 - *Additional spoofed message options*
 - *Personal Email Subscription report on mobile devices*
 - *Outbound routing to Microsoft Office 365 and Google Apps email services*
- *Resolved issues in this release*

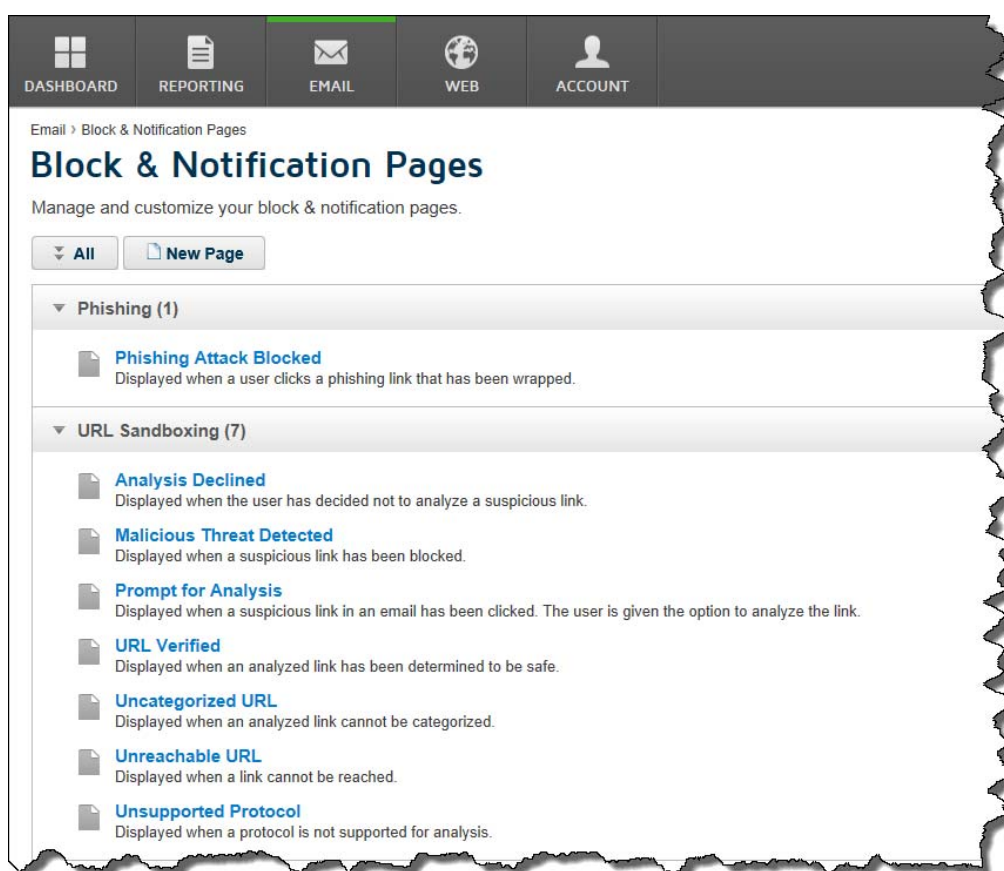
What's new in 2016 Release 3?

TRITON AP-EMAIL with Email Cloud Module | 28-July-2016

Customizable block and notification pages

In the Cloud TRITON Manager, phishing block pages and the new customizable URL sandboxing notification pages are configured by going to **Email > Policy Management > Block & Notification Pages**.

The new URL sandboxing notifications consist of a collection of 7 **customizable** notification pages.



Block and notification page customization can enhance the value and trustworthiness of TRITON AP-EMAIL protection services. Notification and block pages can be branded with your organization's assets (such as a logo), helpdesk contact information, tailored descriptions of security actions and policy, and more.

For detailed information about the customization options and procedures, see **Configure Block & Notification pages** in Cloud TRITON Manager Help.

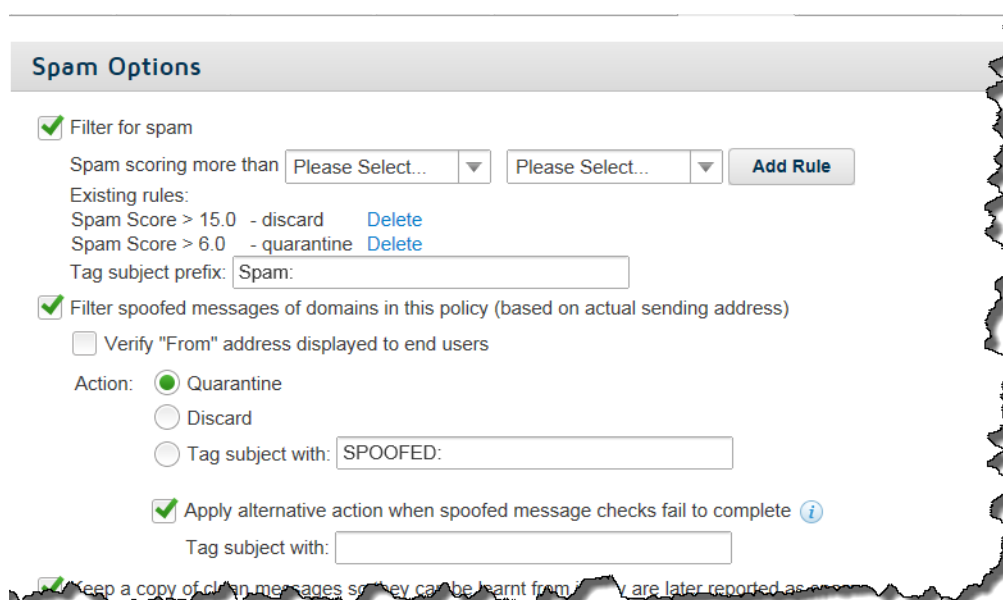
Additional spoofed message options

Detecting spoofed email messages is an essential part of controlling undesirable and potentially dangerous messages in email traffic.

Administrators have new disposition options when spoofed message analysis does not complete as expected and therefore cannot confirm the spoofed message status. This can happen when there is a DNS timeout, or when an error prevents the SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail) validation checks from completing. By default, when this happens the message is considered spoofed and the spoofed message action is applied.

Now administrators can specify an alternate action when spoofed message checks fail to complete and the spoofed message status cannot be determined.

In the Cloud TRITON Manager, go to **Email > Policies > Antispam**.



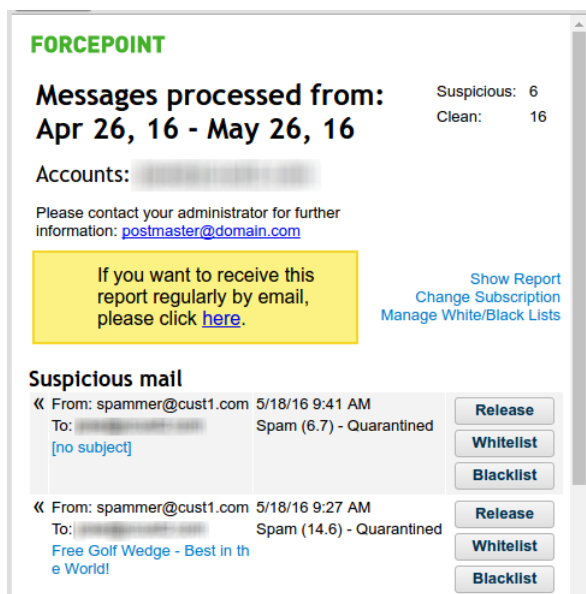
The screenshot shows the 'Spam Options' configuration page. It includes several sections: 'Filter for spam' with dropdowns for 'Spam scoring more than' and 'Please Select...', an 'Add Rule' button, and a list of 'Existing rules' (Spam Score > 15.0 - discard, Spam Score > 6.0 - quarantine) with 'Delete' links. Below this is a 'Tag subject prefix' field set to 'Spam:'. The 'Filter spoofed messages of domains in this policy (based on actual sending address)' section has a 'Verify "From" address displayed to end users' checkbox. The 'Action' section has radio buttons for 'Quarantine' (selected), 'Discard', and 'Tag subject with: SPOOFED:'. The 'Apply alternative action when spoofed message checks fail to complete' checkbox is checked, with an information icon. Below it is a 'Tag subject with:' field. At the bottom, there is a checkbox for 'Keep a copy of clean messages so they can be learnt from' and a partially visible checkbox for 'are later reported as'.

Available disposition options are determined by the disposition option selected for confirmed spoofed messages.

- When the Action is **Quarantine** or **Tag Subject with**, and **Apply alternative action when spoofed message checks fail to complete** is selected, the available option is **Tag Subject with**.
- When the Action is **Discard**, and **Apply alternative action when spoofed message checks fail to complete** is selected, the available options are **Quarantine** or **Tag Subject with**.

Personal Email Subscription report on mobile devices

On some mobile devices, the Personal Email Subscription report was difficult to read and interact with. The report now delivers a much-improved user experience.



Outbound routing to Microsoft Office 365 and Google Apps email services

If you are using Microsoft Office 365 or Google Apps for email, TRITON AP-EMAIL provides the ability to easily configure and validate your outbound route from these two providers into the TRITON AP-EMAIL cloud service.

In the past this feature was available upon request. Beginning with 2016 Release 3, this feature is available to all customers. Access this feature in the Cloud TRITON Manager by going to **Email > Policies > *policy_name* > Add Outbound Route**.

Your existing configuration is not affected by the introduction of this feature.

Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 28-July-2016

- Scheduled reports would sometimes run on a day that did not match the configured start date.
- When a Personal Email Subscription report containing Hebrew was saved, the text became garbled.
- In the Message Details feature of the Report Center, when a **Spam Score** was included as a filter, sometimes the report would not run, or could not be saved, opened, or renamed.
- In configurations with more than 1 dictionary (to support lexical rules), when the dictionaries were **Attached** to one-another, causing each to include the other's contents in their dictionary, an internal error occurred and the administrator was returned to the logon screen.
- Entries in the **Inbound Mail Servers** list could not be reordered using drag-and-drop.

