

2016 Release 4 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 29-September-2016

2016 Release 4 of our cloud email protection product includes the following product updates and corrections.

- *What's new in 2016 Release 4?*
 - *Additional file type recognized*
 - *First logon wizard for new accounts*
 - *Option to hide MIME details in encrypted message retrieval*
- *Resolved issues in this release*

What's new in 2016 Release 4?

TRITON AP-EMAIL with Email Cloud Module | 29-September-2016

Additional file type recognized

On the **Email > Policies > *policy_name* > Inbound/Outbound Attachment Blocking** page, you can quarantine messages containing attachments matching file types that you specify.

An additional file type is recognized.

File Type Category	File Type	Extension
Compressed and Encoded Formats	RAR5	.rar5

First logon wizard for new accounts

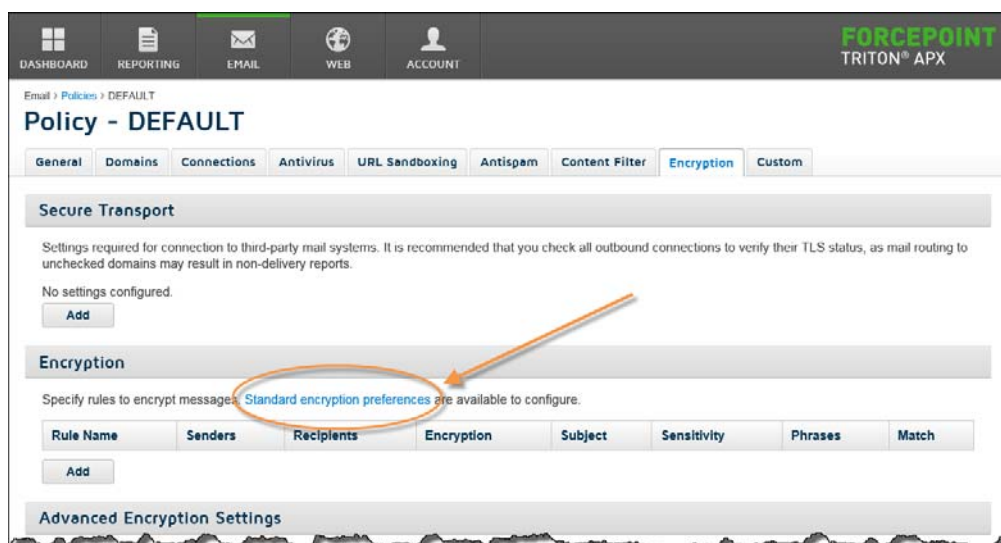
When administrators connect to the Cloud TRITON Manager for the first time to activate their account, a new wizard takes them through the initial steps of:

- Accepting the license agreement for each Forcepoint™ cloud product that they have purchased
- Selecting a primary and backup cloud data center for storing their reporting data
- Providing an administrator email address and password recovery question for use in recovering a lost administrator password

Option to hide MIME details in encrypted message retrieval

Administrators can choose to include (default) or exclude the MIME details when a parked, standard encryption message is retrieved and delivered to the recipient (end user). The setting applies to all policies.

To configure the option, in the Cloud TRITON Manager go to **Email > Policies > any_policy**, select the **Encryption** tab, and then select **Standard encryption preferences**.



Move the slider to the desired setting and click **Save**. The setting applies to all policies.

Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 29-September-2016

- When the Google Apps option was enabled, DNS lookups on Google Apps mail servers could fail in a way that unnecessarily kept outgoing messages from being sent.
- TRITON AP-EMAIL with Email Hybrid Module and the Email Encryption Module could get the message “SMTP 571 - Relaying denied. Encryption not enabled.” This happened when the advanced encryption settings section of the customer policy was missing.
- The Help documentation that describes “Editing an annotation” has been corrected to indicate that the annotation text size limit is 4KB, not 64KB.
- Occasionally a TLS connection test would report failure when, in fact, the test passed.
- A quarantined message that was released could sometimes take several hours to be delivered.
- Translated text is updated for end-user blacklist and whitelist configuration pages. Languages include: French, Italian, German, Spanish, Portuguese (EU), Portuguese (Brazilian), Dutch, Swedish, Greek, Czech, Slovak, Romanian, Polish