2016 Release 2 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 5-May-2016

2016 Release 2 of our cloud email protection product includes the following product updates and corrections.

What's new in 2016 Release 2?

TRITON AP-EMAIL with Email Cloud Module | 5-May-2016

Elliptic Curve Diffie Hellman ciphers for Perfect Forward Secrecy

Support is added for Mail Transfer Agents (MTA) that use Elliptic Curve Diffie Hellman (DH) ciphers for Perfect Forward Secrecy (PFS).

Important

MTA's that advertise Diffie Hellman ciphers must have, at minimum, 768bit DH keys. Keys that do not meet the minimum requirement will experience TLS handshake failures when the TRITON AP-EMAIL service attempts to connect; messages will bounce.

System administrators should check their MTA configuration as soon as possible, and upgrade the cipher key, if needed.

File Sandbox reporting

For **Email Sandbox Module** subscribers, 2 predefined File Sandbox reports are available in the **Report Catalog**. In addition, File Sandbox reports can be constructed in the **Report Builder**, which is designed to allow you to easily create and save custom reports for personal or shared use.

Note

File Sandbox reports are available only in the Report Center package (Report Catalog/Report Builder). If the package is not enabled for your account, contact Forcepoint Technical Support to have it enabled.

As with other Report Catalog/Report Builder reports, File Sandbox reports can be:

- Scheduled for periodic creation and sent to a specified recipient list
- Exported to a PDF or CSV file

What is File Sandboxing?

Accessing File Sandbox reports in the Report Catalog

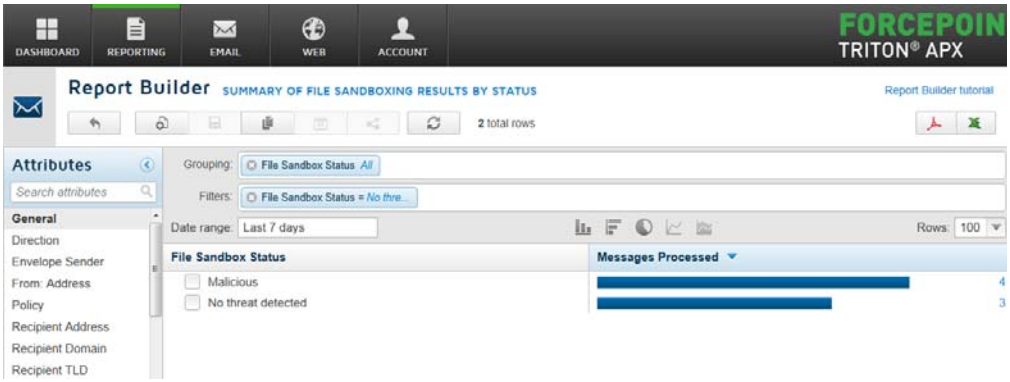
The Report Catalog includes 2 predefined File Sandbox reports:

- *Report 1: Summary of File Sandboxing Results by Status*
- *Report 2: Detailed File Sandboxing Report*

> **Note**
> A feature of all predefined reports is that they can be customized and then saved in your **My Reports** folder.

Report 1: Summary of File Sandboxing Results by Status

Summary of File Sandboxing Results by Status generates a report by result status of all File Sandboxing analysis performed in the last 7 days.



There are 3 possible status values:

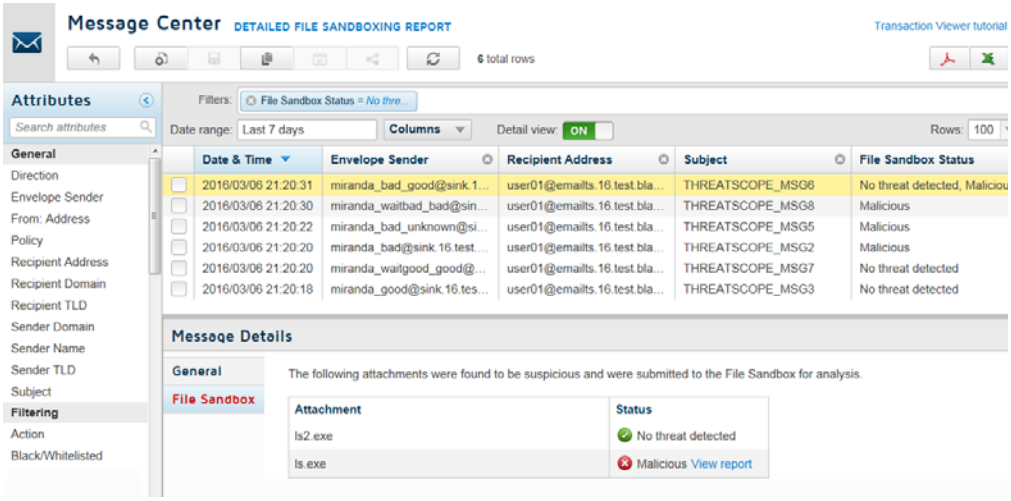
- **Malicious** indicates that sandbox analysis detected potentially damaging, malicious behavior.
- **No threat detected** indicates that sandbox analysis did not detect any malicious behavior.
- **Pending analysis** indicates that a file has been submitted to the sandbox and is queued for analysis.

Report 2: Detailed File Sandboxing Report

Detailed File Sandboxing Report generates a transaction report in the Message Center that includes messages with file attachments that were analyzed by the File Sandbox in the last 7 days. The report filters for Malicious, No threat detected, and Pending analysis. Data includes date/time, sender and recipient addresses, the message Subject line, and file sandbox analysis status (see example, below).

When Message Details are displayed for a transaction—whether in a predefined report or in one created in the Report Builder—, if the message included one or more attachments that were sent to the File Sandbox, the usual message attributes are placed in a tab labeled General, and File Sandboxing details are included in a tab labeled File

Sandbox (see example, below). If one or more of the files was found to be malicious, the File Sandbox tab is selected by default and the label is displayed in red. Contents of an archive file are listed individually. Files found to be malicious offer a link to the file sandbox report, which opens in a new window in your current browser session.



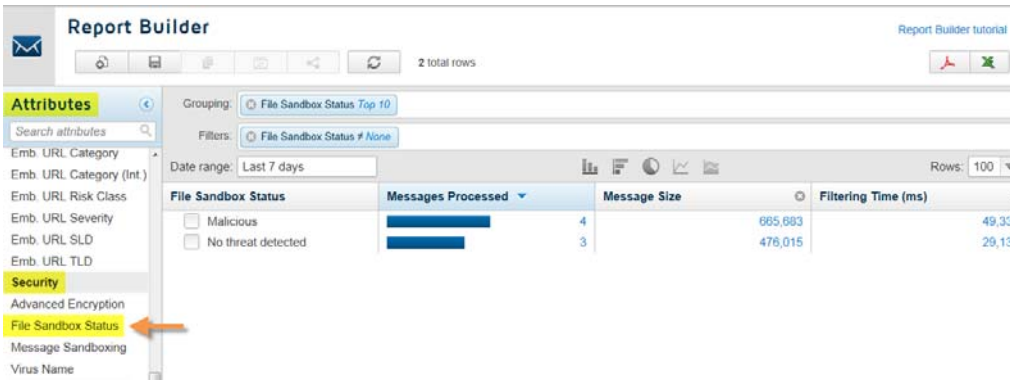
Note

The **Message Details** feature is common to predefined (Report Catalog) and custom (Report Builder) reports. See **Using Message Details** in Cloud TRITON Manager Help.

Building File Sandbox reports in the Report Builder

In the Report Builder, File Sandbox reports are constructed with the **File Sandbox Status** attribute.

In the Security section of the Attribute menu, drag and drop File Sandbox Status into the Grouping field. Note that a secondary grouping is not allowed when File Sandbox Status is the primary grouping. In the sample below, File Sandbox Status is also used to filter out messages where no file attachments were sent to the File Sandbox.



What is File Sandboxing?

When an email message is received that includes suspicious file attachments, the files are sent to a cloud-hosted sandbox for analysis. The sandbox activates the file, observes the behavior, and compiles a report. If the file is determined to be malicious, your configured policy determines whether the message is quarantined or an email alert is sent to the TRITON AP-EMAIL administrator, containing summary information and a link to the report. File sandboxing is available to Email Sandbox Module subscribers. For more details, see File sandboxing in Cloud TRITON Manager Help.

Additional file types recognized

Twenty one additional file types are now recognized, enhancing email security in two important ways:

- The additional file types offer more granular control when configuring attachment quarantine options. This is the **Quarantine messages containing files with these file types** option in the **Inbound/Outbound Content Filtering** sections of the **Content Filter tab**.
- Because these additional file types are recognized, TRITON AP-EMAIL can inspect the contents of these files to ensure compliance with your lexical analysis rules.

The additional recognized file types include:

File Type Category	File Type	Extension
Compressed and Encoded Formats	ICHITARO compressed	.jtdc
	B1 archive	.b1
	EDB	.edb
	Internet Calendaring and Scheduling (iCalendar)	.ics
	XZ archive	.xz
Database Formats	Borland Reflex 2	.r2d
Presentations	Apple iWork 2013 Keynote	
	MS Visio 2013	.vsdx
	MS Visio 2013 macro	.vsdm
	MS Visio 2013 stencil	.vssx
	MS Visio 2013 stencil macro	.vssm
	MS Visio 2013 template	.vstx
	MS Visio 2013 template macro	.vstm
Sound	Conifer Wavpack	.wv
	Sony Wave64	.w64
	Xiph Ogg Vorbis	.ogg

File Type Category	File Type	Extension
Spreadsheets	Apple iWork 2013 Numbers	
Video	ISO/IEC MPEG-4	
Word Processing	Apple iWork 2013 Pages PKCS #12 VCF file	 .p12, .pfx .vcf

Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 5-May-2016

- In reporting, when the virus report **Clicked Sandboxed URLs** was selected, no data was displayed for any time period, and the following message was displayed, “There is a possibility that the data is incomplete. Please try again later.”