2016 Release 1 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 16-February-2016

2016 Release 1 of our cloud email protection product includes the following product updates and corrections.

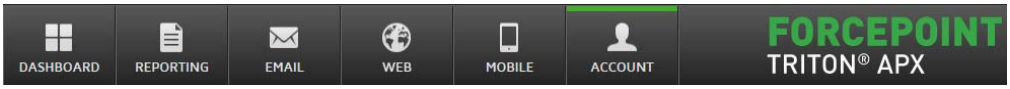
What's new in 2016 Release 1?

TRITON AP-EMAIL with Email Cloud Module | 16-February-2016

Look and feel enhancements

To support the transition from Raytheon | Websense to Forcepoint LLC, the cloud portal has a new look and feel. The colors and logos throughout the portal, including

the logon screen and the portal toolbar, have been updated to reflect the Forcepoint brand.



In addition, if you use phishing block pages, end users will see that the Websense logo has been replaced by the Forcepoint logo. However, if you have previously changed the default logo or customized your notification pages, your changes remain in effect and end users will not see any change.

These changes do not affect product features and functionality.

Over time, you may notice the branding extended to other areas of the portal, like the Help system, as well as to external content, like the Knowledge Base.

Report Catalog and Report Builder package

This release offers a new email reporting package. The package includes an expanded and tailorable Report Catalog and a powerful Report Builder. When enabled for your account, the Report Catalog/Report Builder package supplements the existing reporting features.

> **Note**
> The Report Catalog/Report Builder package is available to all TRITON AP-EMAIL with Email Cloud Module subscribers, but is **not enabled by default**. Please contact Technical Support to have the feature enabled.

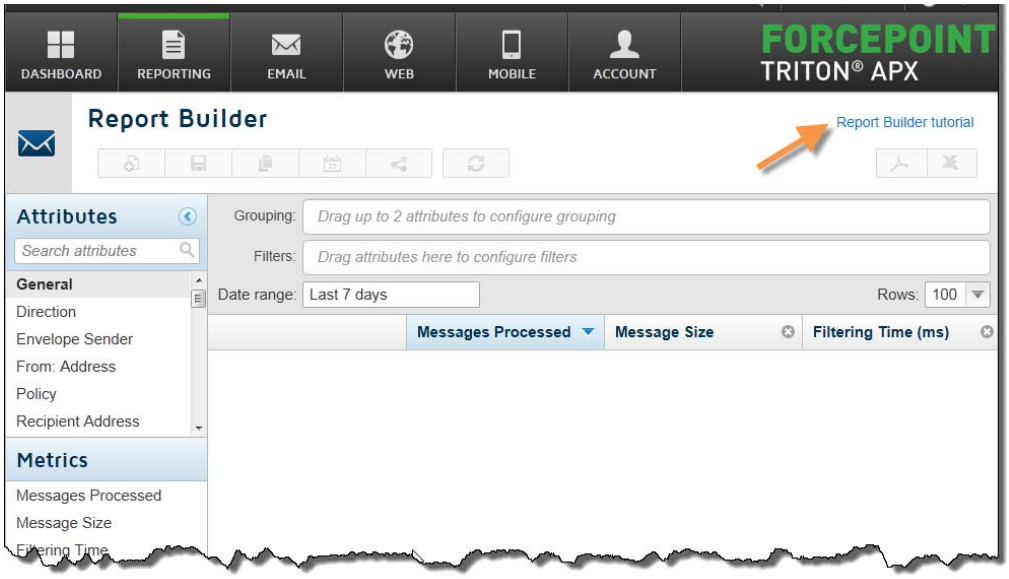
When the Report Catalog/Report Builder package is enabled:

- If you subscribe to only email services, a new sub-menu labeled **Report Center** is added to the **Reporting** menu. In addition, a new sub-menu labeled **Legacy Email Reports** is added to offer the features of the standard reporting package. These reports are still available to you unchanged.

- If you subscribe to cloud web services, as well as email services, the email features of the Report Catalog/Report Builder package are added to the existing **Report Center** menu. In addition, the existing sub-menu labeled **Email Reports** is renamed **Legacy Email Reports** to reflect the re-classification of the original email reports. These reports are still available to you unchanged.

> **Note**
> The new cloud email Report Catalog/Report Builder package cannot create all of the report types that the standard reporting package offers. Additional features will be added to the Report Catalog/Report Builder package in the future.

If you have never used the Report Builder, the Report Builder window includes a link to a helpful 5-minute video tutorial.



For complete information about the email Report Catalog/Report Builder features and their use, see Release Notes for TRITON AP-EMAIL Cloud Reporting.

Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 16-February-2016

- The **Largest Messages** report (located on **Reporting > Email Reports > Volume**) did not offer a date range beyond 2 days. Manually specifying a larger range resulted in an error. Flexible date ranges are now supported.
- When managing Personal Email Subscriptions with the Bulk Upload feature, the CSV upload would sometimes fail, reporting an internal error.
- Email messages deleted in the spam queue could be released via the Personal Email Subscription (formerly End User Message Report). For clarity, messages that have been deleted from the spam queue are now labeled “Deleted” in the Personal Email Subscription report.
- In rare cases, after a domain was added or moved, the route check failed when the connection was TLS.

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

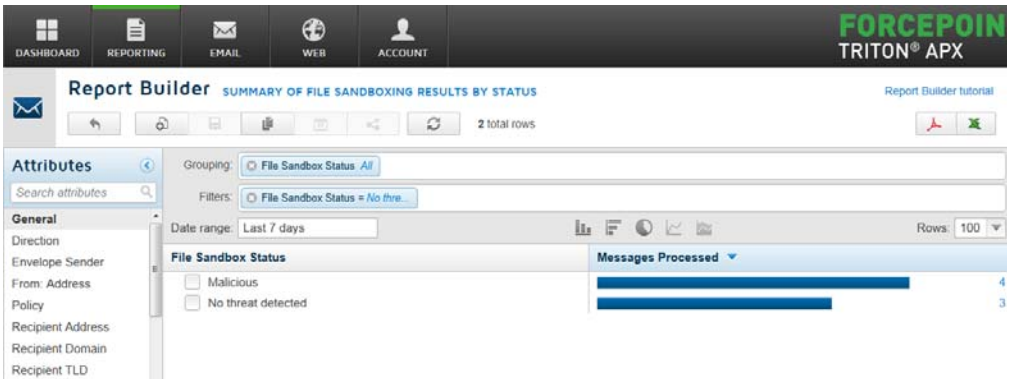
The Report Catalog includes 2 predefined File Sandbox reports:

- *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:

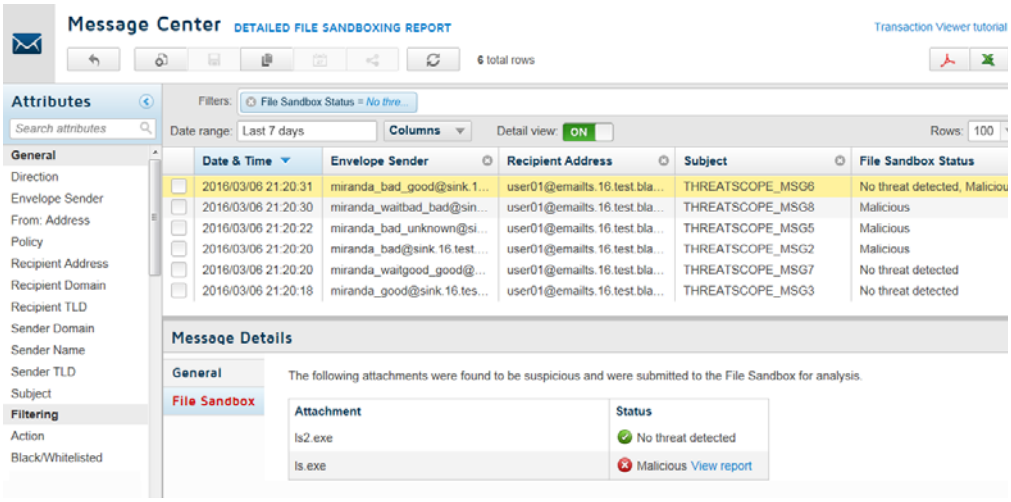
- **Malicious** indicates that sandbox analysis detected potentially damaging, malicious behavior.

- **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.



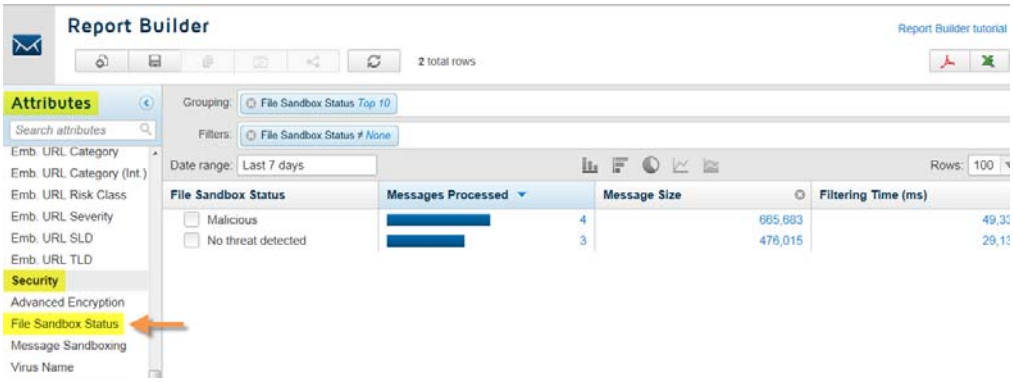
Note

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

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.

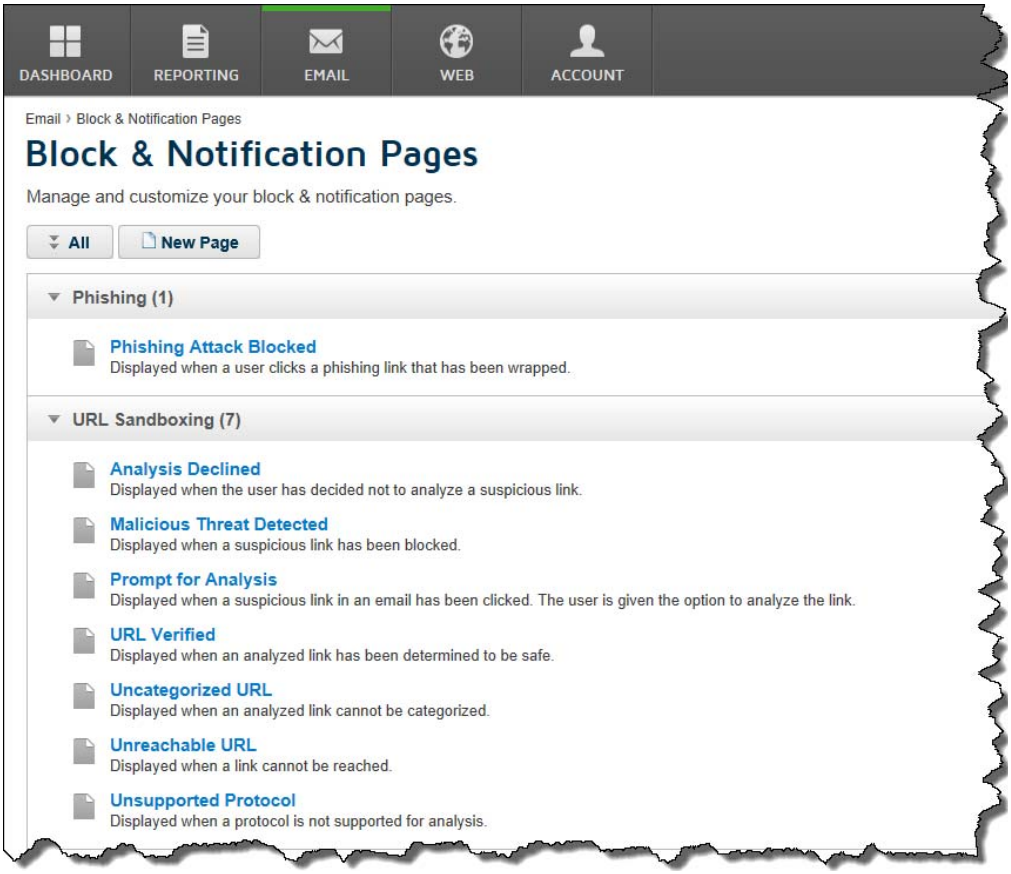
What's new in 2016 Release 3?

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.

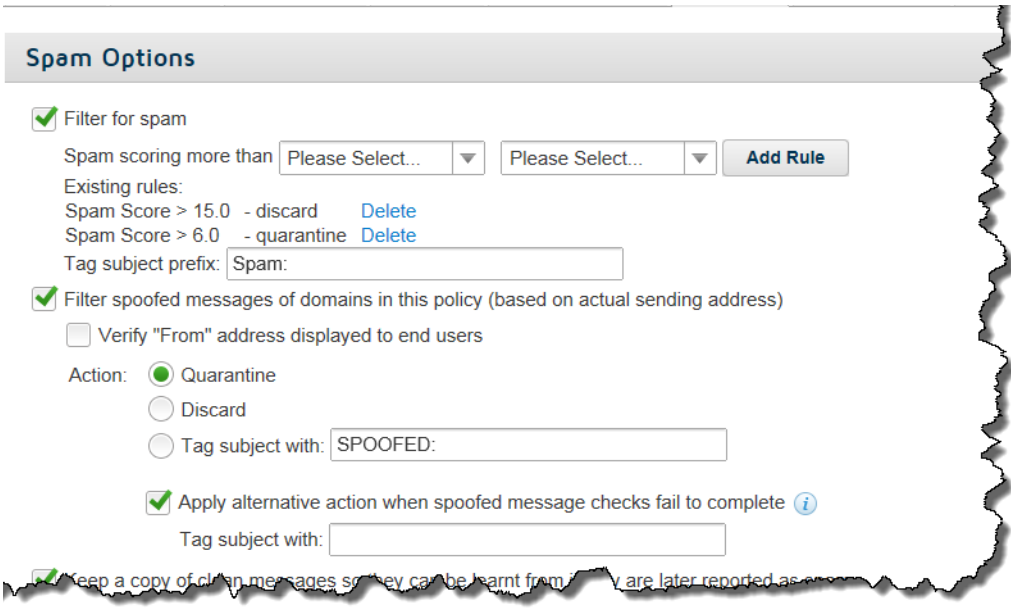
Additional spoofed message options

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**.

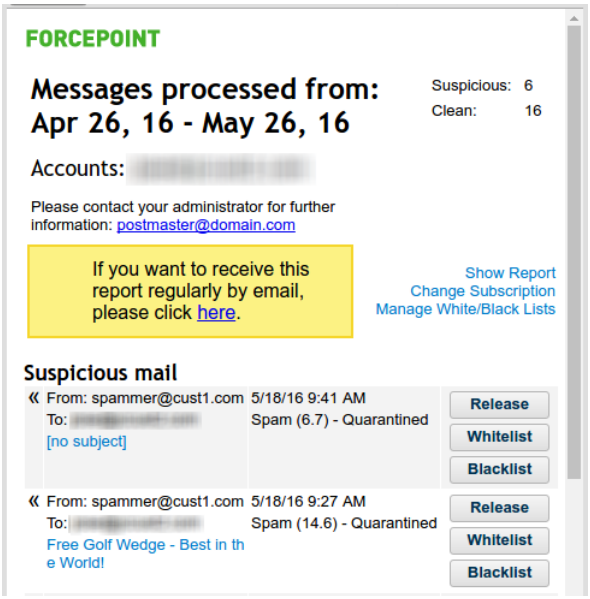


Available disposition options are determined by the disposition option selected for confirmed spoofed messages.

- 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.

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?

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

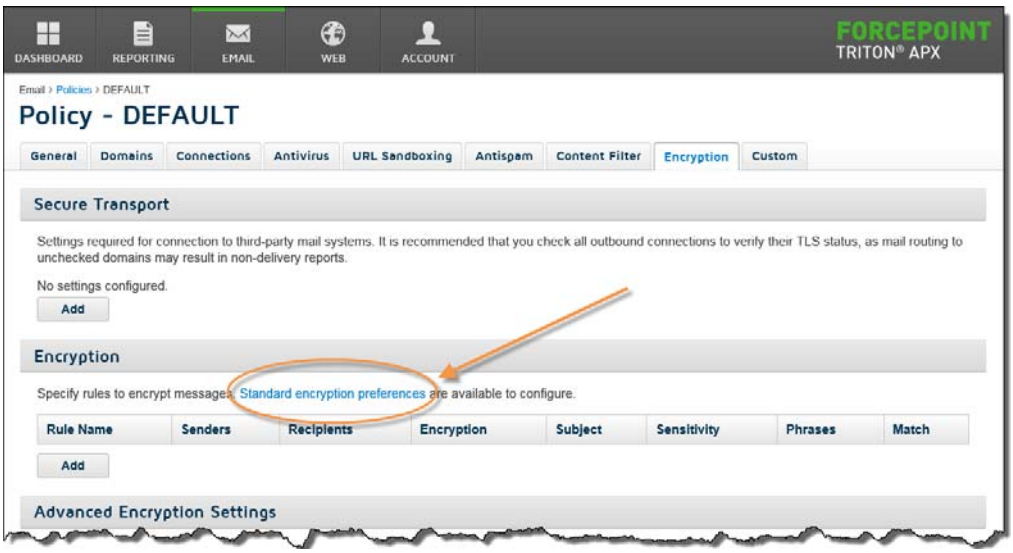
When administrators connect to the Cloud TRITON Manager for the first time to activate their account, a new wizard takes them through the initial steps of:

- 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

2016 Release 5 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 18-November-2016

2016 Release 5 of TRITON AP-EMAIL with Email Cloud Module includes the following product updates and corrections.

What's new in 2016 Release 5?

TRITON AP-EMAIL with Email Cloud Module | 18-November-2016

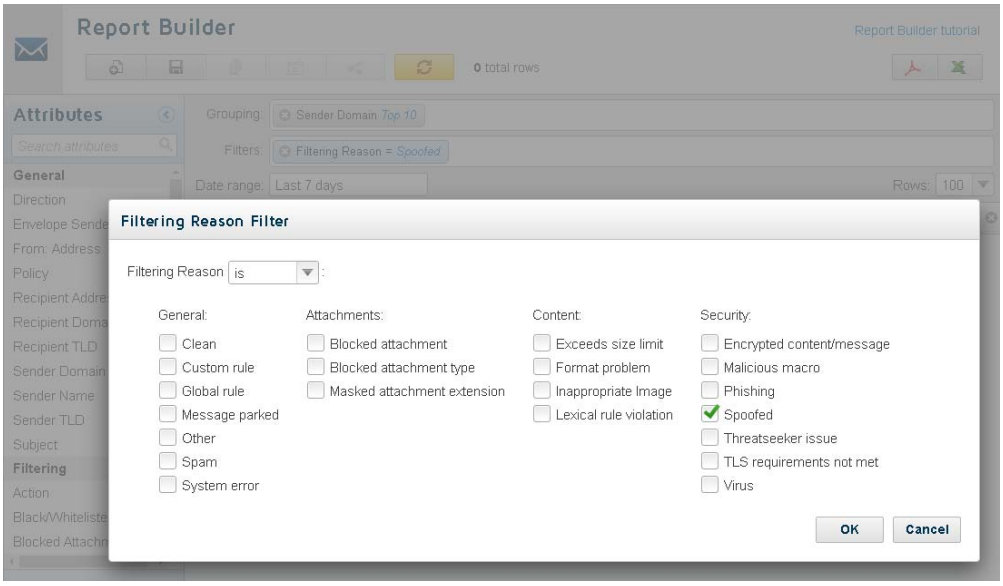
Increased efficiency for scheduled report jobs

In order to increase resiliency for accounts that have many or very large scheduled report jobs, changes have been made to:

- Increase the job timeout period to allow jobs that take more than 15 minutes to complete
- Distribute the start time when multiple jobs are scheduled
- Increase the frequency with which the scheduler runs to every 5 minutes

'Spoofed' Filtering Reason in Report Builder reports on spoofed messages

When the "Filter spoofed messages" option is enabled (an Antispam option), use the Report Builder to create a report of spoofed messages. In the Report Builder, select the desired Grouping options and then add **Filtering Reason** as the Filters selection. In the **Filtering Reason Filter** dialog box, select **Spoofed** and then update the report.



Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 18-November-2016

- The Transaction Viewer Tutorial video, available from each of the detail view reports in the cloud portal, has been updated. It now includes information about using the Transaction Viewer, Incident Manager, and Message Details reports. Click the Video Tutorial link from any of the 3 detail view reports to launch the video.
- The Personal Email Subscription report did not display properly when viewed in Microsoft Outlook.
- End users could not save changes to their Personal Email Subscription settings when the Subscription Settings page was accessed via the Change Subscription button in their Personal Email Subscription report.

2016 Release 6 Notes for Cloud Email Protection Solutions

TRITON® AP-EMAIL with Email Cloud Module | 13-December-2016

2016 Release 6 of TRITON AP-EMAIL with Email Cloud Module includes the following product updates and corrections.

What's new in 2016 Release 6?

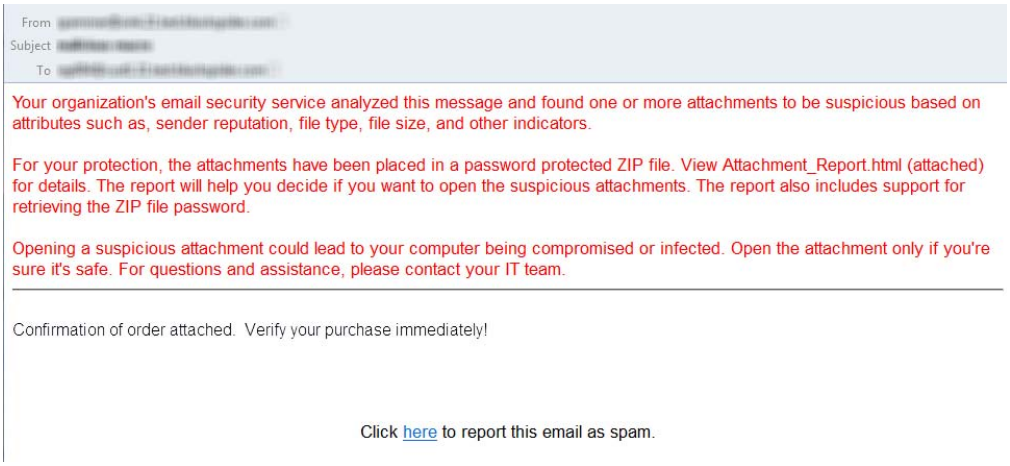
TRITON AP-EMAIL with Email Cloud Module | 13-December-2016

Limited availability: Secure suspicious attachments

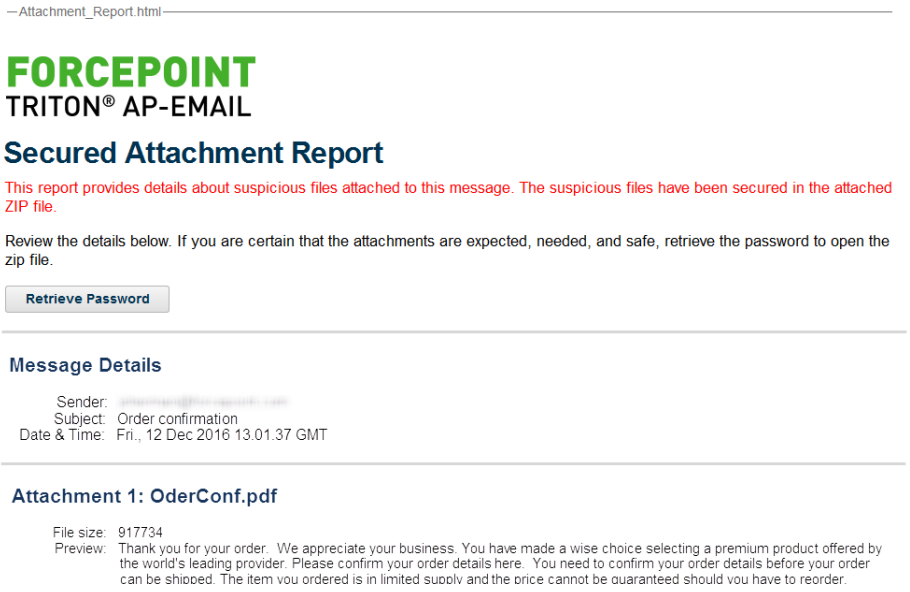
For cyber criminals, attaching malicious files to emails continues to be a very effective attack strategy. TRITON AP-EMAIL performs rigorous analysis of attachments, including sending suspicious files to a sandbox for observation and analysis (optional feature). However, even when a file passes analysis, some attributes of the attachment can continue to make it suspicious. These attributes include sender and domain reputation, attachment file type, attachment size, and the spam score of the message, among others.

Email administrators now have the option to secure suspicious attachments in a password protected zip file that is delivered to the recipient along with a report that includes the message details, a preview of the attachment content, and a link that the recipient can use to retrieve the zip file password. The email is also annotated with a

customizable message. Below is a sample of a message delivered with a secured attachment.

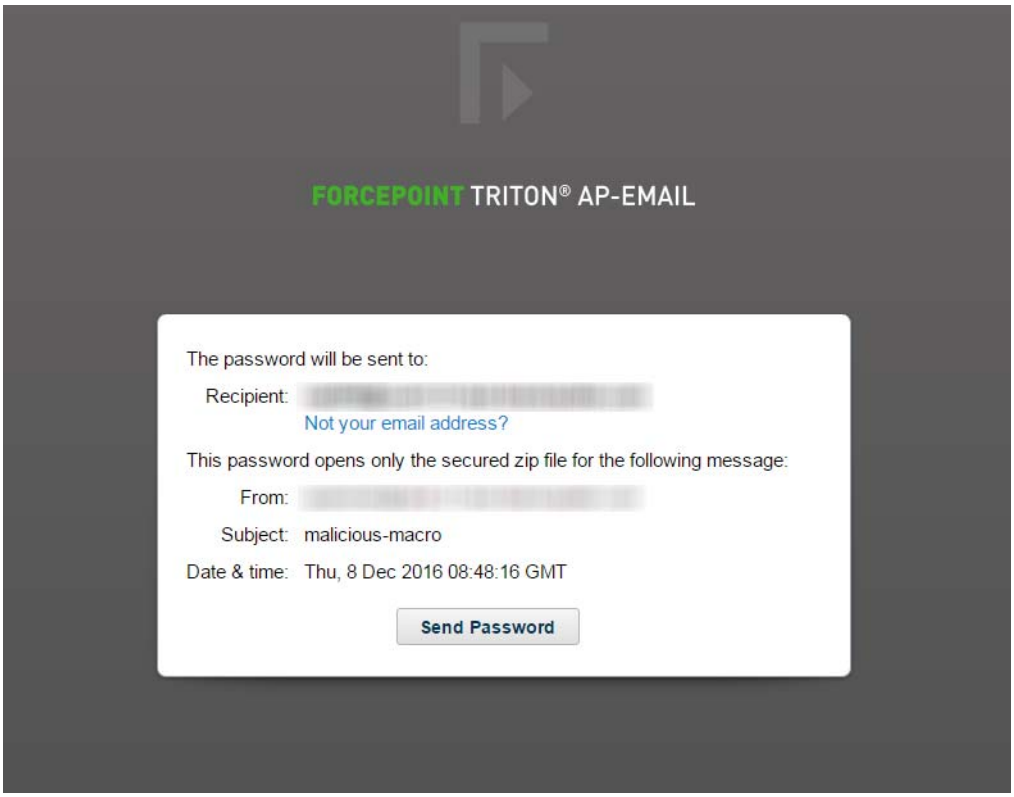


Here is a sample Secured Attachment Report.



By securing the attachment in this way, the recipient and organization have the time and information needed to take a fully considered action.

Should the recipient choose to retrieve the zip file password by clicking the **Retrieve Password** link, they are taken to a Forcepoint TRITON AP-EMAIL portal to confirm their request. Once confirmed, a separate email is sent containing the password.



Only the original recipient can receive the password. If a message with secured file attachments is forwarded, recipients of the forwarded message must ask the original recipient for the password.

Should you choose to enable the feature and secure suspicious file attachments, it's very important that you prepare your users to receive them and take appropriate action. Users should know that:

1. Their email security service analyzes email attachments for malicious content. When found, the attachment is not delivered.
2. The email security service also looks for suspicious file attachments. An attachment can be suspicious for several reasons including the reputation of the sender or sending domain, attachment file type, attachment size, the spam score of the message, and other attributes.
3. When a suspicious attachment is found:
   - The attachment is placed in a password protected zip file and delivered, along with the original message, to the intended recipients.
   - A **Secured Attachment Report** is also attached to the original message. The report includes the message details, a preview of the attachment content, and support for retrieving the password for the secured zip file.

4. Recipients should carefully examine the Secured Attachment Report to help determine if the attachment is safe.
5. Opening a suspicious attachment could lead to the computer being compromised or infected. Recipients should open the attachment only if they're sure that it's safe. If in doubt, contact the IT team for assistance.
6. If a user receives a forwarded copy of a message with the secured zip file, they need to ask to original recipient for the password. Only the original recipients can retrieve the password.

The **Secure suspicious attachments** feature is enabled at the policy level (per policy).

To enable the feature:

1. In the portal go to **Email > Policies >** ***policy_name*** and select the Content Filter tab.
2. In the Inbound Content Filter section, enable **Secure suspicious attachments**.
3. Click the adjacent **Customize settings** link to review and customize the message that is inserted into the original message.
4. You can also add sender addresses or domains to exclude from the secure attachment rule.
5. Save your changes.

Resolved issues in this release

TRITON AP-EMAIL with Email Cloud Module | 13-December-2016

- When an end-user used the **Report as spam** feature to report a message as spam, some URLs were constructed in such a way that the TRITON AP-EMAIL service could not process the URL.
- Customizing the **Subject line prefix** value (default string) of a notification email (Email > Policy Management > Notification Email > *selected_policy*), did not change the string that was inserted into the Subject line of a quarantined message. The default value was still inserted.
- When processing a very large CSV file for bulk upload of personal email subscriptions (Email > Personal Email Subscriptions > Bulk Upload), the process sometimes failed due to a timeout error.
- The service response to SPF (Sender Policy Framework) error messages has been changed to reduce "unknown" results and improve interpretation of whether or not an email message is spoofed.
- Defang parsing of HTML email messages containing embedded fonts or media has been improved, allowing such messages to be delivered, rather than being quarantined.

Release Notes for TRITON AP-EMAIL Cloud Reporting

Updated: 11-February-2016

Applies to:	TRITON AP-EMAIL with Email Cloud Module: Report Catalog and Report Builder

Use these Release Notes to learn about the features of the new Report Catalog and Report Builder package for TRITON AP-EMAIL with Email Cloud Module. When enabled for your account, Report Catalog and Report Builder supplement the standard email reporting package.

Note

The email Report Catalog/Report Builder package is not enabled by default. Contact Technical Support to have this feature enabled.

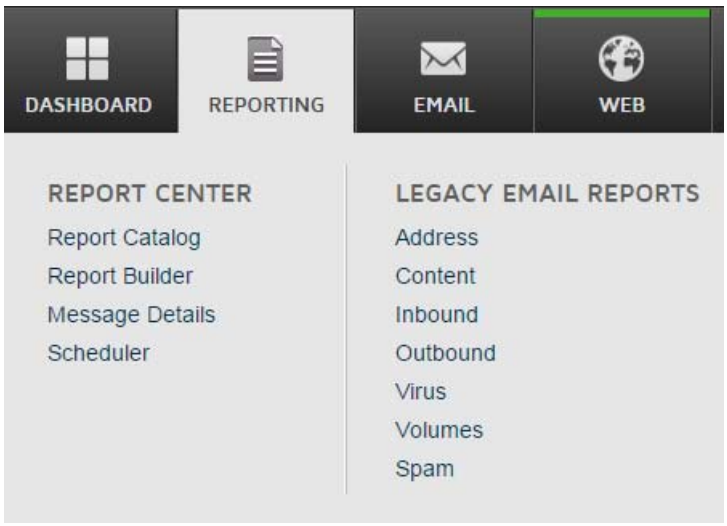
The Report Catalog contains a number of predefined reports that cover common scenarios, available in bar chart, trend chart, and tabular formats. You can copy any

predefined report to apply your own filters to create a custom report, and share your reports with other administrators.

The Report Builder offers an enhanced model for creating multi-level, flexible reports that allow you to analyze information from different perspectives and gain insight into your organization's email message trends. If a high-level summary shows areas of potential concern, you can drill down to find more details.

When the email Report Catalog/Report Builder package is enabled:

- If you subscribe to only email services, a new sub-menu labeled **Report Center** is added to the **Reporting** menu. In addition, a new sub-menu labeled **Legacy Email Reports** is added to offer the features of the standard reporting package. These reports are still available to you unchanged.



- If you subscribe to cloud web services, as well as email services, the email features of the Report Catalog/Report Builder package are added to the existing **Report Center** menu. In addition, the existing sub-menu labeled **Email Reports** is renamed **Legacy Email Reports** to reflect the re-classification of the original email reports. These reports are still available to you unchanged.

> **Note**
> The new cloud email Report Catalog/Report Builder package cannot create all of the report types that the standard email reporting package offers.
>
> Additional features will be added to the Report Catalog/Report Builder package in the future.

Contents of these release notes include:

Supported browsers

The reporting package is supported on the following browsers:

- Internet Explorer 9 and later
- Google Chrome version 32 and later
- Mozilla Firefox version 26 and later

Other browsers may produce unexpected results.

Accessing the reporting package

1. Access the Cloud TRITON Manager at https://admin.websense.net/portal, and log on using your standard credentials.
2. Select **Reporting** from the toolbar.

3. Under Report Center, select either Report Catalog, Report Builder, or Scheduler.

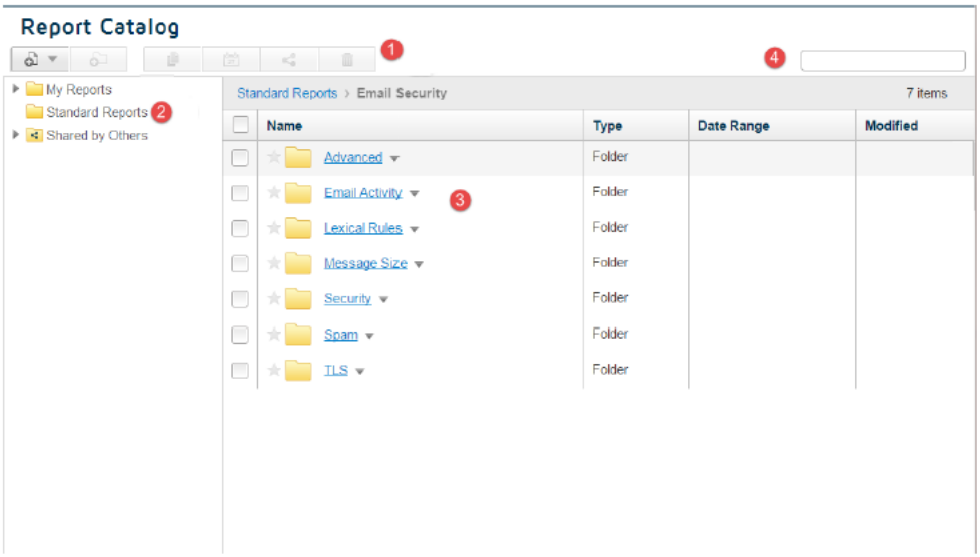
Using the Report Catalog

This section contains instructions for navigating around the Report Catalog, accessing and running reports, creating custom reports, and sharing reports and folders.

- *Navigating the Report Catalog*
- *Managing reports*
- *Managing folders*

Navigating the Report Catalog

To access the Report Catalog, click **Reporting** at the top of the page and select Report Catalog. The Report Catalog includes the following elements:



1. The **Toolbar** contains buttons for returning to the previous page, creating new reports and folders, copying, sharing, and deleting items.
2. The **folder list**, in the left-hand pane, contains 3 top-level folders:
   - The Favorites folder enables you to easily locate your most frequently-used reports. You can mark a report or report folder as a favorite in the following ways:
     - Click the star to the left of the report or folder name in the Report Catalog. The star turns yellow when selected.
     - Click the star to the right of the report name in the Report Builder or Transaction View. You do not need to save your changes.

     To remove a report from Favorites, click the star again to turn it gray.

     When viewing the Favorites folder, note that you are essentially viewing a list of shortcuts to the reports. Choose **View in folder** from a favorite report's drop-down menu to see the report in its original folder.
   - My Reports contains all of the reports and folders that you create.
   - Standard Reports contains the predefined reports provided in TRITON AP-EMAIL. (If you have both cloud email and web protection, select the Email Security sub-folder.) These are divided into the following folders:
     - Advanced
     - Email Activity
     - Lexical Rules
     - Message Size
     - Security

- Spam
- TLS

For more information, see *Predefined reports*.

- Shared by Others contains items that have been shared for use by all administrators in your account. Each folder has the user name of another administrator, and contains the reports shared by that administrator.

If a folder contains one or more sub-folders, click the arrow to see those sub-folders in the left-hand page. Click a folder name to see its contents in the right-hand pane.

3. The table in the right-hand pane displays the contents of the folder you select in the folder list. This can be one or more-sub-folders, or a list of reports. To see a description of a particular report, hover the mouse over the report name.

   From this pane, you can perform actions on one or more reports and folders, such as copying, renaming, and deleting folders, or editing, running, or sharing a report. The actions available to you depend on the permissions configured – for example, you cannot delete reports in the Standard Reports folder.

4. The **Search** field enables you to search for specific words or phrases in report titles. Search results list the report name, its location, and if applicable, the report owner and the last time it was edited. You can manage a report directly from the search results list – for example you can run it, or if you have suitable permissions, share or delete it.

Managing reports

Running a report

To run a report:

1. In the left-hand pane, navigate through the folder structure and select the sub-folder containing the report you want. The reports appear in the table on the right of the screen.
2. Click the report you want to run. Alternatively, click the down arrow next to the report, and select **Run** from the menu.
3. The results are displayed in the Report Builder. See *Viewing report results* and *Viewing detailed reports* for more information.

Creating a new report

To create a new report:

1. In the toolbar, click the **New Report** button, and select whether you want to create a grouped or transaction report.

   Selecting a grouped report opens the Report Builder. Selecting a transaction report opens Transaction View.

2. Define attributes (for a grouped report), filters, and date ranges for your report as described in *Creating a report*.
3. To save your new report to the Report Catalog, click the **Save** button in the toolbar.
4. Enter a name and optionally a description for the report. The name can be a maximum of 200 characters, and the description a maximum of 400 characters.
5. Select the folder to store the report in. By default this is the My Reports folder; if you have created sub-folders, you can use the **Folder** drop-down to choose one of those.
6. Click **Save Report**.

Copying a report

To copy a report:

1. Navigate through the Report Catalog to find the report you wish to copy. This can be a standard report, one created by you, or a report shared by someone else.
2. Click the down arrow next to the report you want, and select **Copy** from the menu.

Note

To copy multiple reports, mark the check box to the left of each report, then click the **Copy** button in the toolbar.

3. If you are copying a standard or shared report, select the folder where you want to store the copied report. By default this is the My Reports folder; if you have created sub-folders, you can use the **Folder** drop-down to choose one of those.

   If you are copying one of your own reports, it is automatically saved to the same folder as the original. You can move it to a different location later if required; see *Moving items between folders*.
4. Click **Copy**.

   The report is saved to the selected location. If you are copying a report that you own, "Copy" is appended to the report name. You can now rename the report by clicking its down arrow and selecting **Rename** from the menu. You can also edit it as required.

Editing a report

To edit an existing report:

1. Navigate through the Report Catalog to find the report you wish to edit. This can be a standard report, one created by you, or a report shared by someone else.
2. Click the down arrow next to the report you want, and select **Edit before running** from the menu.

   This opens the Report Builder or Transaction View, depending on whether you are editing a grouped or a transaction report.

3. Edit the attributes, filters, and date range of the report as required, then click the **Update Report** button in the toolbar.
4. If you are editing a report that you created, or a shared report for which you have editing permissions, you can save your changes by clicking the **Save** button in the toolbar. The report is saved with the same name and in the same location, overwriting the previous version.

   If you are editing a standard report, or a shared report for which you do not have editing permissions, click the **Save As** button in the toolbar to save the edited report to one of your folders.

Sharing a report

To share a report:

1. In My Reports, click the down arrow next to the report you want, and select **Sharing** from the menu. Alternatively, mark the check box(es) next to one or more reports, and click the **Share** button in the toolbar.

   Note

   You can also share a report after running it in the Report Builder.

2. In the popup window, select one of these options:
   - **Not shared** means you are the only person who can access the report. Select it if you want to remove sharing from a report.
   - **View only** allows others to run the report, but not save any changes to it.
   - **Allow editing** enables others to both run and save changes to the report.
3. Click **OK**.

   The report now has the sharing icon next to it in the report list. Hover the mouse over the icon to see the sharing permissions allocated to the report.

Deleting a report

To delete a report:

1. In My Reports, click the down arrow next to the report you want to delete, and select **Delete** from the menu. Alternatively, mark the check box(es) next to one or more reports, and click the **Delete** button in the toolbar.
2. In the popup window, click **Delete** to confirm.

Managing folders

Creating a new folder

You can create new folders only within the My Reports folder, up to a maximum of 4 levels of sub-folders. Folder names can have a maximum of 200 characters.

To create a new folder:

1. Navigate to the location in My Reports where you wish to place the new folder.
2. Click the Add Folder button in the toolbar.
3. Enter the new folder name, then click **Add**.

You can rename the folder later, if required, by clicking its down arrow and selecting **Rename** from the menu.

Copying a folder

When you copy a folder, you also copy all of the contents in that folder, including sub-folders and their contents.

To copy a folder:

1. Navigate through the Report Catalog to find the folder you wish to copy. This can be a folder containing standard reports, one created by you, or a folder shared by someone else.
2. Click the down arrow next to the folder you want, and select **Copy** from the menu.

Note

To copy multiple folders, mark the check box to the left of each folder, then click the **Copy** button in the toolbar.

3. If you are copying a standard or shared folder, select the location where you want to store the copied folder. By default this is the My Reports folder; if you have created further sub-folders, you can use the **Folder** drop-down to choose one of those.

   If you are copying one of your own folders, it is automatically saved to the same location as the original.
4. Click **Copy**.

   The folder is saved to the selected location. If you are copying a folder that you own, “Copy” is appended to the folder name. You can now rename the folder by clicking its down arrow and selecting **Rename** from the menu. You can also edit the reports in the folder as required.

Moving items between folders

If you have several folders under My Reports, you can easily move reports and folders around using drag-and-drop:

1. Select the item(s) that you want to move.
2. Drag the item(s) to the destination folder, in either the left-hand or right-hand pane. Note that a “Move items” popup appears as you start the drag: this turns green when hovering over a valid location, or red when over a folder where you cannot drop the report – for example, in Standard Reports.
3. A success message appears once you have moved the item(s) to a valid location.

Note

Moving a report to a folder that has different sharing permissions does not change the sharing permission assigned to the report.

Sharing a folder

When you share a folder, you also share the reports in that folder with the same permissions. You can then edit the sharing permissions for individual reports within the folder; see *Sharing a report*.

To share a folder:

1. Navigate through My Reports until the folder you want to share is shown in the right-hand pane.
2. Click the down arrow next to the folder, and select **Sharing** from the menu. Alternatively, mark the check box(es) next to one or more folders, and click the **Share** button in the toolbar.
3. In the popup window, select one of these options:
   - **Not shared** means you are the only person who can access the folder. Select it if you want to remove sharing from a folder.
   - **View only** allows others to run the reports in this folder, but not save any changes to them.
   - **Allow editing** enables others to both run and save changes to the reports in this folder.
4. Click **OK**.

   The folder now has the sharing icon next to it in the list. Hover the mouse over the icon to see the sharing permissions allocated to the folder.

Deleting a folder

Deleting a folder also deletes all reports and sub-folders contained within it,

To delete a folder:

1. Navigate through My Reports until the folder you want to share is shown in the right-hand pane.
2. Click the down arrow next to the folder you want to delete, and select **Delete** from the menu. Alternatively, mark the check box(es) next to one or more folders, and click the **Delete** button in the toolbar.
3. In the popup window, click **Delete** to confirm.

Using the Report Builder

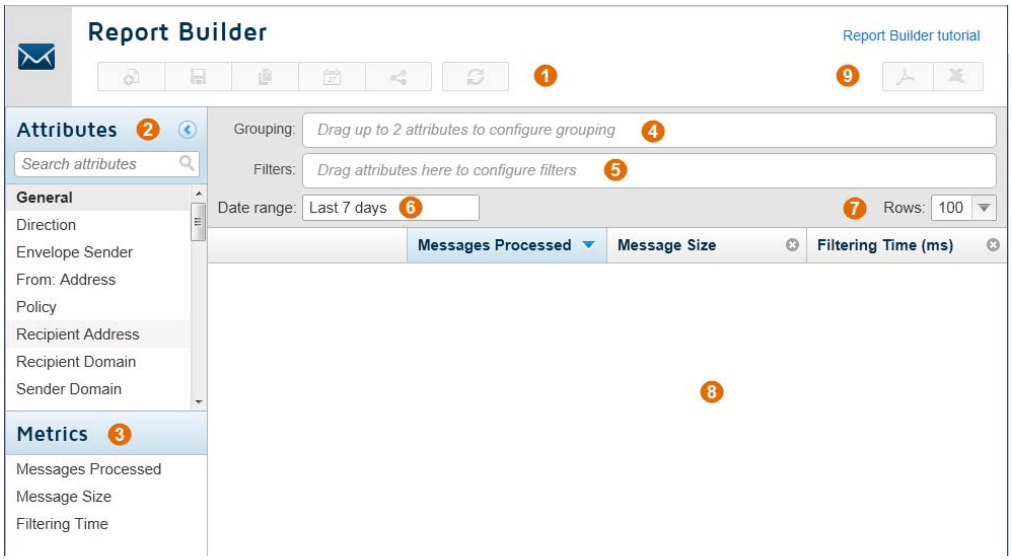
This section contains instructions for navigating around the Report Builder, creating reports, viewing the results, and drilling down to further details.

To access the Report Builder, go to **Reporting > Report Builder**. If you have both cloud web and email protection solutions, select **Email Security** from the popup that appears.

- *Navigating the Report Builder*
- *Creating a report*
- *Viewing report results*
- *Viewing detailed reports*

Navigating the Report Builder

The Report Builder has the following elements:



1. The **Toolbar** contains buttons for returning to the previous page, starting a new report, and updating the current report.
2. The **Attributes** list contains the data types that you can use to create reports. and are divided into the following sections:

- General
- Filtering
- IP Address
- Message Content
- Security
- Time

Use the Search box at the top of the list to filter the Attribute list further. For more information, see *Report attributes*.

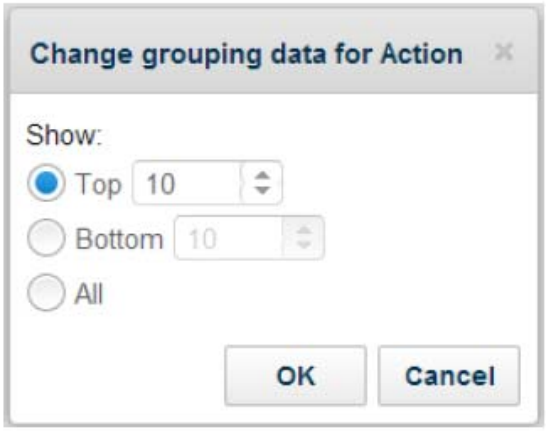
3. The **Metrics** list contains options that you can add as columns to the report. Drag metrics into and out of the report results area to add them to or remove them from the report. Further advanced metrics are available in the Message Details view.
4. The **Grouping** field can contain up to 2 attributes to define the data grouping that appears in the report. For example, if you drag the Policy attribute followed by the Recipient Address attribute into this field, this creates a summary report on messages by policy, and also displays the data broken down by recipient addresses within those policies. For more information on defining grouping data, see *Creating a report*.
5. The **Filters** field can contain attributes to filter the report results further. For example, you may wish to filter by specific senders, actions, or content types. For more information on defining filters, see *Creating a report*.
6. The **Date range** defines the time period covered by the report. This can be a standard period (between 1 hour and 8 months) or a specific date and time range.
7. The **display options** enable you to select how many rows appear in your report. Once a report has been generated, this section also includes options to page through longer reports, and to display the report results in different table and graph formats. For more information, see *Viewing report results*.
8. The **report results** appear when you click **Update Report**, and by default are in a table format. You can choose to display the results in different formats as described above, and to select report elements to drill down further. For more information, see *Viewing detailed reports*.
9. You can choose to export report results in PDF or CSV format.

Creating a report

To create a report:

1. Drag up to 2 attributes from the Attributes list to the Grouping field.
   - The Report Builder does not allow you to add more than 2 attributes, nor can you add the same attribute more than once.

- By default, the report shows the top 10 matches by number of hits. Click an attribute box in the Grouping field to change the grouping data to show a specified number of top results, a specified number of bottom results, or all results.



Note
Choosing to view all results may mean the report takes a long time to generate.

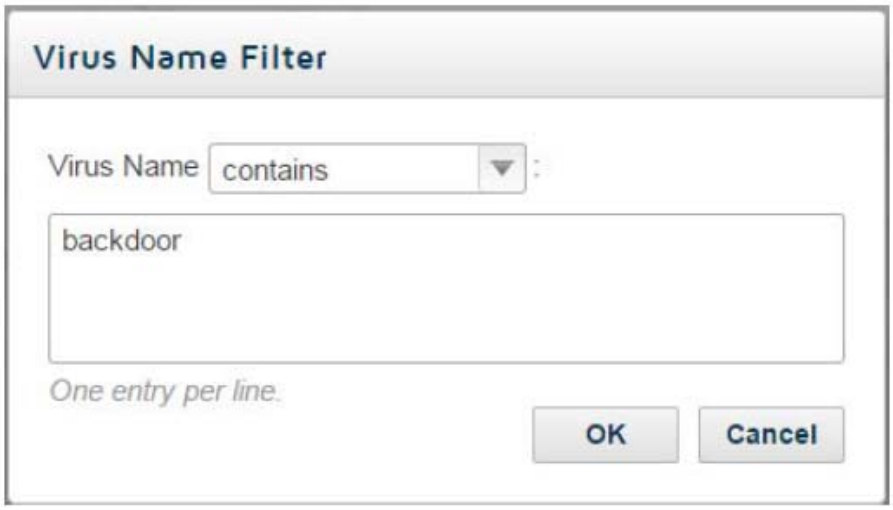
- To remove an attribute from the Grouping field, click the cross icon on the attribute box.

2. To add filters to the report, drag an attribute to the Filters field.
   a. On the popup that appears, use the drop-down list to define how the filter handles the values that you specify. The options available depend on the attribute that you have selected. For example, you may be able to include or exclude values, or state that search terms equal or do not equal your text.
   b. Enter or select the search term or value(s) that you wish to filter on. Depending on the filter, you can:
      - Select one or more check boxes
      - Start typing text that will autocomplete based on data in the system
      - Enter the exact text that you want to use

For filters where you are including or excluding values already stored in the system, start typing to see a list of potential matches:

Select the option you want from the list. You can add multiple values to the filter.

For filters where you enter free text, enter the terms you want on separate lines:



c. Click **OK** when done.

To edit a filter, click its attribute box. To remove an attribute from the Filters field, click the cross icon on the attribute box.

3. Click in the Date range field to define the report period.

- To specify a set period in hours, days, or months, select an option from the **Last** drop-down list.
- To specify a particular date range, select the **From** radio button and use the calendars to choose the required dates. Date ranges include the whole 24-hour period, unless you mark **Specify start and end time** to enable and edit the times for the report as well as the dates.

Click **Done** when you are finished.

4. Click the Update Report button to generate the report.

> **Note**
> The Update Report button turns yellow when you enter or change valid report content, signifying that you can generate a report with the selected criteria.

Viewing report results

Your report results are initially shown as a table, with a column for the grouping and filters you selected, and a column for each of the selected metrics. Use the arrows next to each first-level attribute to expand or collapse the second-level attribute content below it.

Use the options in the toolbar to define how you display and navigate through report results:

Select the number of rows to see on each page. The default is 100 rows; you can also select 50, 150, or 200 rows.

Use the arrow keys to page through longer reports, and quickly navigate to the first or last page.

View the report results as one of the following:

- column chart
- bar chart
- pie chart
- line chart
- area chart

Hover the mouse over an item in a chart to see more information, for example a percentage or a number of hits.

All of these charts are available for a single-level grouping report. For grouping reports with 2 attributes, only column and bar charts are available.

Each item in the report has a check box. Select one or more check boxes to open a popup window that enables you to:

- Drill down into more detailed information. See *Drilling into report items*.
- Show only the report items you have selected
- Filter out the report items you have selected
- View message details for the items you have selected. See *Message Details*.
- Cancel any selections you have made.

Viewing detailed reports

You can use grouping reports as a starting point for accessing more detailed information about web activity, either by drilling down into a particular aspect of a report, or using the Message Center to see further information about a report item.

Drilling into report items

To drill down into a report item:

1. Mark the check box next to each item you wish to drill down into.

   You can select multiple items and change your selections, even after the popup window appears.
2. In the popup window, select an available attribute from the Drill Into By the drop-down list. For example, if you have selected one or more categories from the grouping report, you may wish to see the users who have been accessing sites in those categories.
3. The new report loads. Note that as you have moved down a level in the report, the item(s) you selected in step 1 are now in the Filters field, while the Grouping field contains the other report attributes, including the one you selected in step 2.

   You can edit the content of the Grouping and Filters fields, and view the report in different formats, in exactly the same way as for the previous report.
4. To drill down a further level, repeat steps 1-3 above.

Message Details

The Message Details view is available for report items at all levels. To see the details for one or more report items:

1. Mark the check box next to each item you wish to view.

   You can select multiple items and change your selections, even after the popup window appears.
2. In the popup window, select **View Transactions**.

The Message Center loads, listing details for each message within the report item(s) you selected.

In the Message Center, you can:

- Edit the filters and date range for the messages you wish to see.
- Select the columns to display from the **Columns** drop-down. Click **Done** when you have made your selections.
- Click a column heading to make it the active column for sorting transactions. Click again to switch between ascending and descending order.
- Delete columns by clicking the X icon in a column heading. Note that you cannot delete the current active column.
- Drag metrics from the left-hand pane into the Filters field.
- Enable Detail View to see more detail for the selected message. The Message Details pane opens at the bottom of the page, and displays the timestamp, sender address, recipient address, direction, action, and filtering reason of the message.
- Export message details to PDF or CSV format. Either select one or more messages and then click **Export to PDF** or **Export to CSV** in the popup window that is displayed, or click the PDF or CSV icon in the top right to export all messages on the page.

Report attributes

Below is a list of available report attributes.

Name	Description	Filter values
Direction	The direction of the message: inbound or outbound.	Check boxes
Envelope Sender	Used by mail servers to check where the message originates and where to respond (for example, if there is an error or the message bounces). Often matches the From: address, but not always. For example, the message might come from a mailing list, or from an organization authenticated to send messages on your company's behalf.	Manual text
From: Address	The address the message recipient sees in the From: field of the message.	Manual text
Policy	The email policy used for filtering.	Autocompleted text
Recipient Address	The email address of a message recipient.	Manual text
Recipient Domain	The domain associated with a message recipient.	Manual text
Sender Name	The name of a message sender.	Manual text

Name	Description	Filter values
Sender Domain	The domain associated with a message sender.	Manual text
Subject	The text in the subject line of a message. There is also an option to filter by results with no subject.	Manual text
Action	The action applied to the message. Options are Accepted, Bounced, Bypassed processing, Discarded, Quarantined, Temporarily bounced.	Check boxes
Black/Whitelisted	Groups and filters messages by whether they are blacklisted, whitelisted, or neither.	Check boxes
Blocked Attachment Ext	Groups and filters messages by the extension of their blocked attachments (for example, EXE). There is also an option to include results with no blocked attachment extension.	Manual text
Filtering Reason	The result of filtering the message. Options are Blocked attachment, Blocked attachment type, Clean, Custom rule, Encrypted content/message, Exceeds size limit, Format problem, Global rule, Inappropriate image, Lexical rule violation, Malicious macro, Masked attachment extension, Message parked, Other, Phishing, Spam, System error, Threatseeker issue, TLS requirements not met, Virus.	Check boxes
Lexical Rule	The lexical rule applied to a message. There is also an option to include results with no lexical rules applied.	Manual text
Sender IP	The IP address of a message sender. There is also an option to include results with no sender IP address.	Manual text
Sender IP Country	The country from which the sender IP address originates.	Autocompleted text
Attachment File Type	A description of the type of file attached to a message - for example Microsoft Excel or Portable Network Graphic (PNG).	Autocompleted text
Attachment Filename	The name of a specific file attached to a message.	Manual text

Name	Description	Filter values
Attachment MIME Type	MIME type of a message attachment in the format content type/content subtype. For example, video/mpeg or text/csv.	Manual text
Content Type	The type of content detected within the message. Options are Archive, Audio, Encrypted, Executable, HTML, Image, None, Office Document, Signed, Video.	Check boxes
Emb. Domain	The domain of an embedded URL within a message.	Manual text
Emb. Full URL	The full URL embedded within a message.	Manual text
Emb. Host	The host name embedded within a message.	Manual text
Emb. URL Category	The category of a URL embedded within a message.	Autocompleted text
Emb. URL Risk Class	The risk class associated with a URL embedded within a message.	Check boxes
Emb. URL Severity	The severity level associated with a URL embedded within a message.	Check boxes
Advanced Encryption	The type of advanced encryption applied to the message. Options are Decrypted Inbound, Encrypted Outbound, or None. This attribute requires the Email Encryption module.	Check boxes
Message Sandboxing	The type of sandboxing applied to the message. Options are None, Phishing URL Sandboxed, URL Sandboxed. This attribute requires the Email Sandbox module.	Check boxes
Virus Name	The name of a virus detected in a message. There is also an option to include results with no virus name associated with them.	Manual text
Date	Enables you to group report entries by date. Note that this attribute is not available for filtering as the Date Range field performs this function.	N/A
Day of Week	Enables you to group and filter report entries by days of the week.	Check boxes
Hour	Enables you to group and filter report entries by hour.	24 hour selection
Month	Enables you to group and filter report entries by month.	Check boxes

Predefined reports

Below is a list of predefined reports.

Advanced reports

Report Name	Description
Message Analysis Delay	The time taken in rounded-up seconds to process and analyze messages.
Unprocessed Message Statistics	Details of messages discarded due to access control rules in the last 7 days.

Email Activity reports

Report Name	Description
Full Message Statistics	Total number of inbound and outbound email messages processed in the last 7 days.
Inbound Email Statistics	Total number of inbound messages in the last 7 days.
Outbound Email Statistics	Total number of outbound messages in the last 7 days.
Outbound Senders	Email addresses of users sending messages from your mail servers in the last 7 days.
Top Inbound Policies	Policies containing users receiving the most messages in the last 7 days.
Top Inbound Receiving Domains	Domains in your account receiving the most messages in the last 7 days.
Top Inbound Recipients	Most frequent recipients of inbound messages in the last 7 days.

Report Name	Description
Top Inbound Senders	Most frequent senders of inbound messages in the last 7 days.
Top Inbound Sending Domains	Domains sending the most inbound messages to your account in the last 7 days.
Top Inbound Sources	Most frequent source IP addresses of inbound messages in the last 7 days.
Top Outbound Policies	Policies containing users sending the most messages in the last 7 days.
Top Outbound Receiving Domains	Domains receiving the most messages from your account in the last 7 days.
Top Outbound Recipients	Most frequent recipients of outbound messages in the last 7 days.
Top Outbound Senders	Most frequent senders of outbound messages in the last 7 days.
Top Outbound Sending Domains	Domains in your account sending the most outbound messages in the last 7 days.
Top Recipients	Most frequent recipients of messages, both inbound and outbound, in the last 7 days.
Top Senders	Most frequent senders of messages, both inbound and outbound, in the last 7 days.

Lexical Rules reports

Report Name	Description
Most Matched Lexical Rules	The top 10 lexical rules matched in the last 7 days.
Top Recipients for Lexical Rule Blocks	Recipients of messages most frequently blocked by lexical rules in the last 7 days.
Top Senders for Lexical Rule Blocks	Senders of messages most frequently blocked by lexical rules in the last 7 days.

Message Size reports

Report Name	Description
Large Messages	Details of the largest messages processed through the service in the last 7 days.
Total Message Size	Total size of all messages processed for your account in the last 7 days.

Security reports

Report Name	Description
Emails Containing Viruses	Messages containing viruses detected in the last 7 days, using all techniques including Threatseeker.
Inbound Virus Percentage	Percentage of inbound messages containing viruses in the last 7 days.
Outbound Virus Percentage	Percentage of outbound messages containing viruses in the last 7 days.
Sandboxed URLs	Messages containing URLs that were sandboxed in the last 7 days.
Top Inbound Virus Sources	Most frequently-seen domains for inbound viruses in the last 7 days.
Top Virus Sources	Common source domains of viruses in the last 7 days.
Top Viruses	Top 20 most commonly-detected viruses in the last 7 days.

Spam reports

Report Name	Description
Inbound Commercial Bulk Email Statistics	Details of inbound messages detected as commercial bulk email in the last 7 days.
Inbound Spam Percentage	Percentage of inbound messages detected as spam in the last 7 days.
Inbound Spam Statistics	Details of inbound messages detected as spam in the last 7 days.

Report Name	Description
Outbound Spam Percentage	Percentage of outbound messages detected as spam in the last 7 days.
Outbound Spam Statistics	Details of outbound messages detected as spam in the last 7 days.

TLS reports

Report Name	Description
Mandatory TLS Delivery Failures	Details of messages in the last 7 days that could not be delivered because a TLS connection was not available.

Known issues

There are no current known issues.