Release Notes for Forcepoint TRITON AP-DATA v8.3.0

Updated: 24-Jan-2017

Applies To:	Forcepoint TRITON AP-DATA v8.3.0

Use the Release Notes to find information about what's new and improved in Forcepoint™ TRITON® AP-DATA v8.3.0:

New in TRITON AP-DATA

Updated: 24-Jan-2017

Applies To:	Forcepoint TRITON AP-DATA v8.3.0

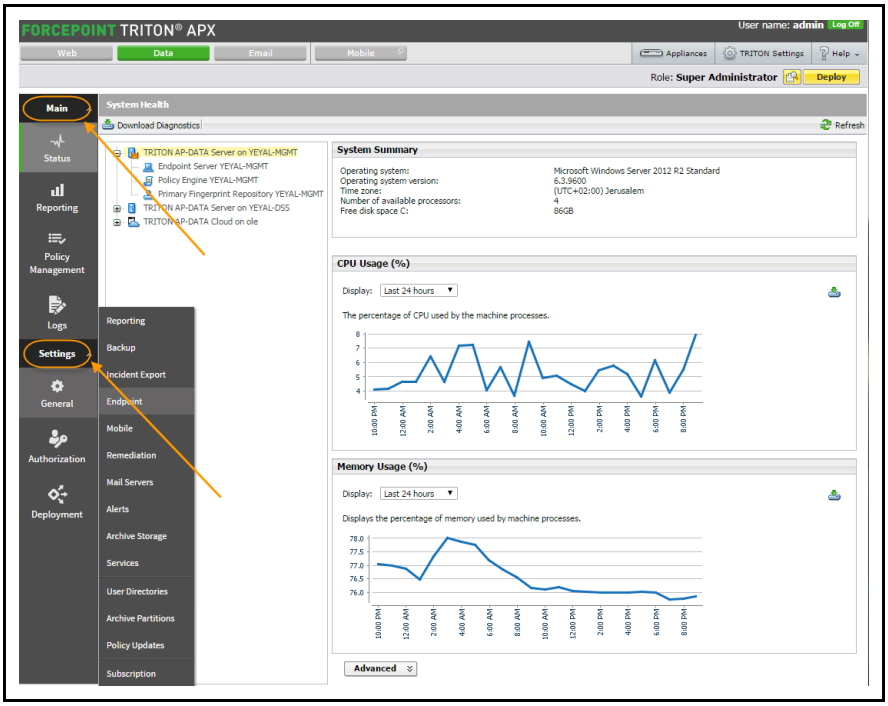
Version 8.3 of Forcepoint TRITON AP-DATA is a major release that offers several new features, including:

TRITON AP-DATA

Fresh look

The TRITON Manager has been redesigned to provide faster access to the menus and options you require. Instead of having 2 tabs, Main and Settings, all options are now on one page.

The paths are the same. The functions are the same. But instead of clicking the **Settings** tab and then selecting **General > Endpoint**, for example, you simply select **General > Endpoint** in the **Settings** section of the left navigation panel.



The Web and Email modules of the TRITON Manager have been updated with the new look as well.

Cloud content inspection

TRITON AP-DATA Cloud App Security is a new DLP product license. It includes a new DLP module that provides data-in-motion content inspection for files uploaded into and stored within enterprise cloud collaboration services, such as Microsoft Office 365. The license also includes data discovery capabilities for supported enterprise cloud applications.

By applying established DLP policies to data stored in enterprise cloud applications, the module is able to audit and prevent the storage of sensitive data that could expose your organization to data loss and compliance infringements. To enable existing DLP data in motion policy rules for enterprise cloud applications, you need only enable the Cloud Services channel on a DLP policy's Destination tab.

TRITON AP-DATA Cloud App Security can be installed in a private data center (on-premises) or in a public cloud platform. In the version 8.3 release Microsoft's Azure cloud platform is supported.

Version 8.3 supports data in motion DLP policy enforcement for Microsoft OneDrive for Business. This release can apply DLP policies based on file upload and public sharing operations.

The TRITON AP-DATA Cloud App Security license also provides discovery functionality for Box, SharePoint Online, and Exchange Online. Discovery is carried out using an on-premises deployed data discovery crawler.

The new TRITON AP-DATA Cloud App Security module is managed in the TRITON Manager like all TRITON AP-DATA modules. Several new elements have been added to the user interface:

- *System module*
- *Action plan*
- *Destination channel*
- *Report filters*
- *System health*

For detailed instructions on installing and configuring TRITON AP-DATA Cloud App Security, refer to the TRITON AP-DATA Installation Guide.

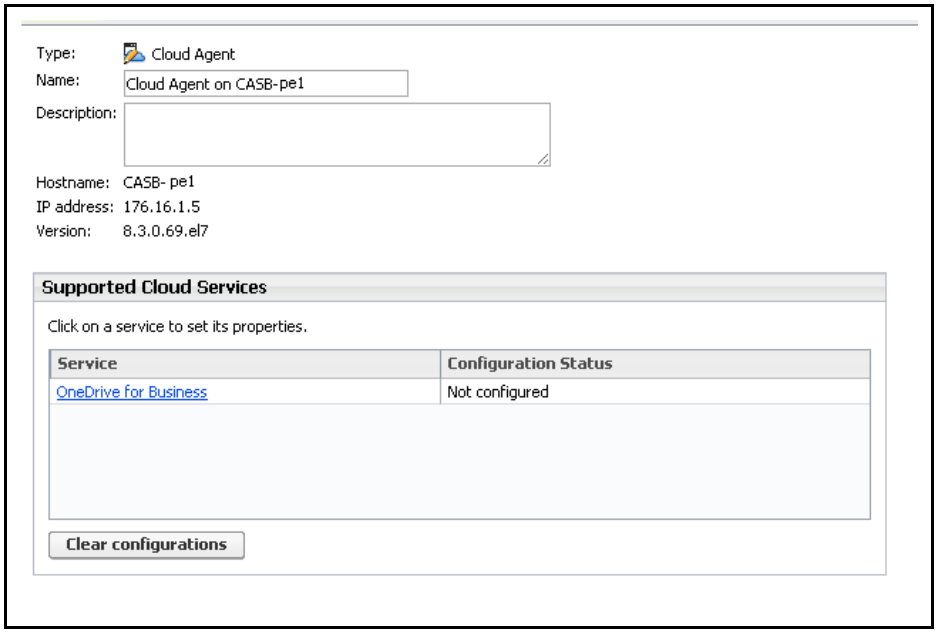
System module

After installing TRITON AP-DATA Cloud App Security and registering it with the management server, a new module is added to the **Settings > Deployment > System Modules** page. The module includes a policy engine and a fingerprint repository.

Because you can have more than one module in the system, there may be more than one module displayed.

When you click a module name, you see a name and description for the module, as well as a list of available cloud services and their configuration status.

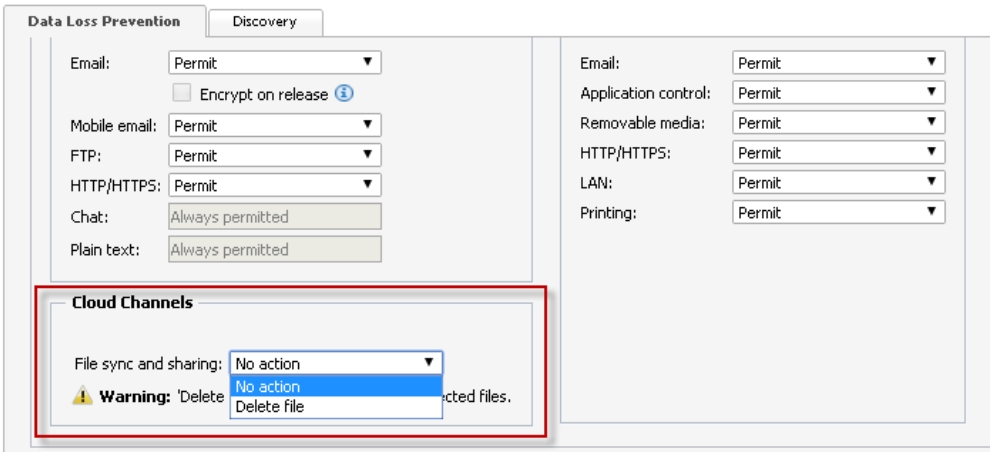
You must configure a service in order to register it with the TRITON management server. This is required the first time you set up the TRITON AP-DATA Cloud App Security module.



Action plan

There is a new section on the **Add Action Plan** screen for configuring the action to take when there is a policy violation on cloud channels. To get to this screen, select **Main > Policy Management > Resources > Action Plan > New.**

For the Cloud channel, **File sync and sharing**, you can select **Permit** or **Delete file**. Other Cloud channels and actions will be added in the future.

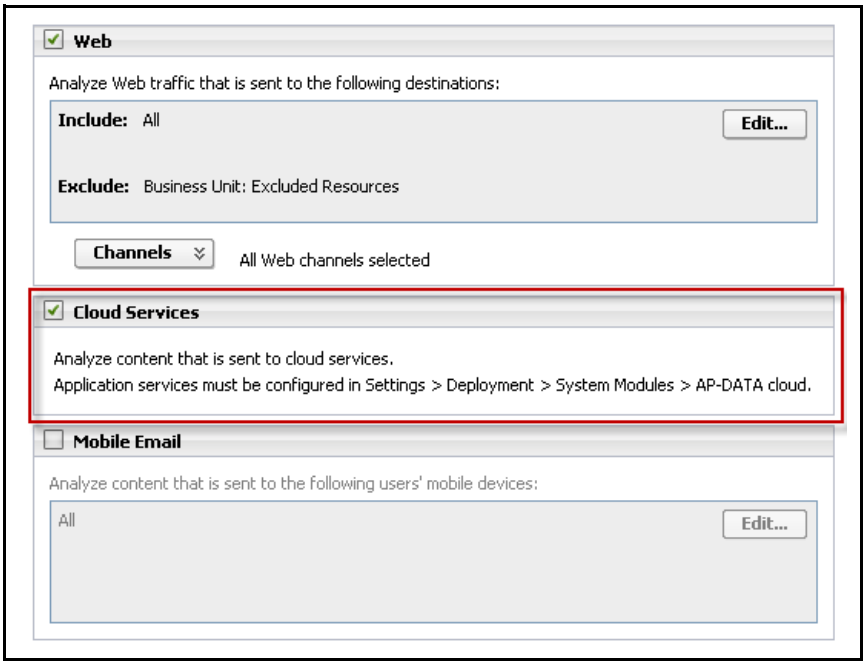


Destination channel

Cloud services are now offered as destination channels in DLP policies.

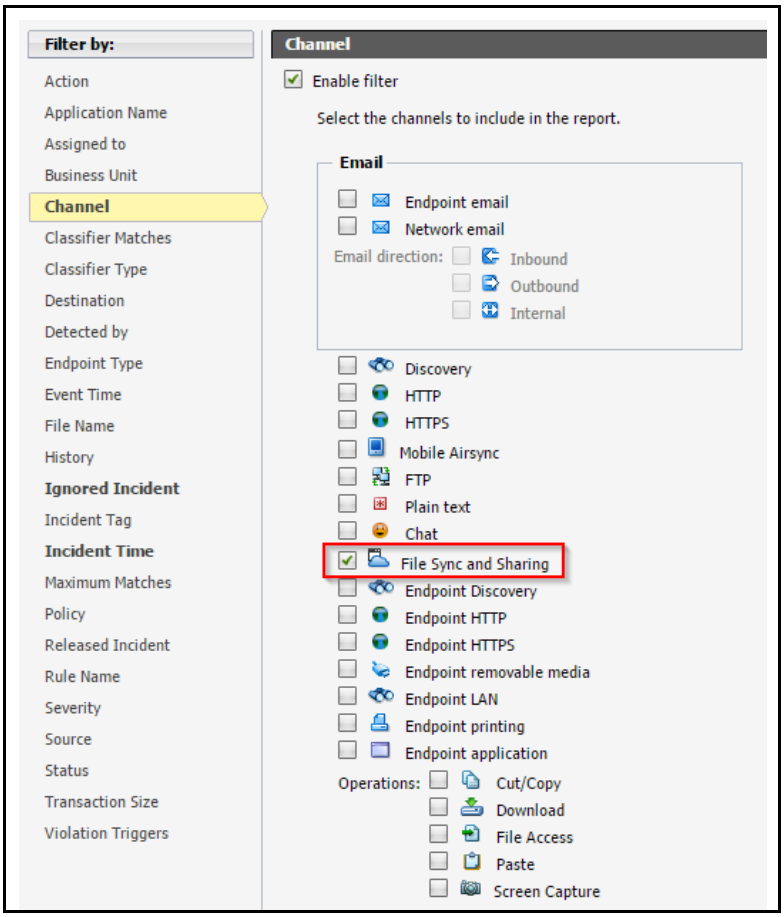
There is a new Cloud Services section on a policy's Destination page. Select this option if you want content that is sent to OneDrive for Business to be analyzed by the system.

This channel is disabled by default.



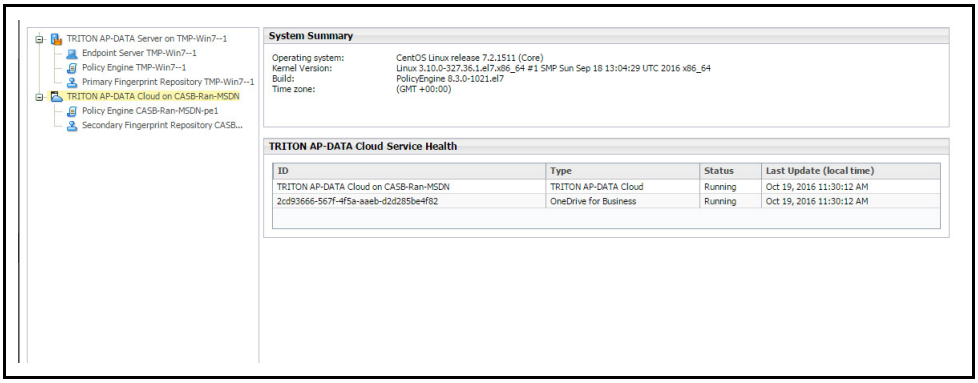
Report filters

You can now filter reports by cloud service channels. For v8.3, this includes file sync and sharing. Select this box to include file sync or sharing incidents in your report, such as those involving external file sharing.



System health

A new System Health page is available for TRITON AP-DATA Cloud App Security modules. It shows information about the cloud agent itself, such as operating system and kernel version, as well as the status of the cloud agent and cloud service (running, pending deployment, etc.)



As with other modules, System Health displays information about system resources for the policy engine and fingerprint repository that are part of the agent, such as CPU and memory usage.

Incident Risk Ranking enhancements

In TRITON AP-DATA v8.2.5, Forcepoint added an advanced security analytics capability called incident risk ranking. It uses statistical data modeling and behavioral baselines to automatically identify and rank groups of high-risk incidents.

A new DLP component, the analytics engine, consumes incidents generated by DLP policies across all core TRITON AP-DATA components and reports on those with the highest data loss or data theft risk score. You can use this information to identify the highest risks to your organization so that you can take remediation action and prevent future risks.

No additional license is required to benefit from this new analytics capability.

This feature includes an **Incident Risk Ranking – Top Cases** report that shows up to 20 cases with the highest risk scores during the selected time period, along with details for those cases. Cases are groups of related incidents that, combined, indicate a risk to your organization—for example, incidents of data being sent to suspicious destinations or those occurring outside normal office hours.

Enhancements in v8.3 include:

- *New My Cases report*
- *More information on the case card*

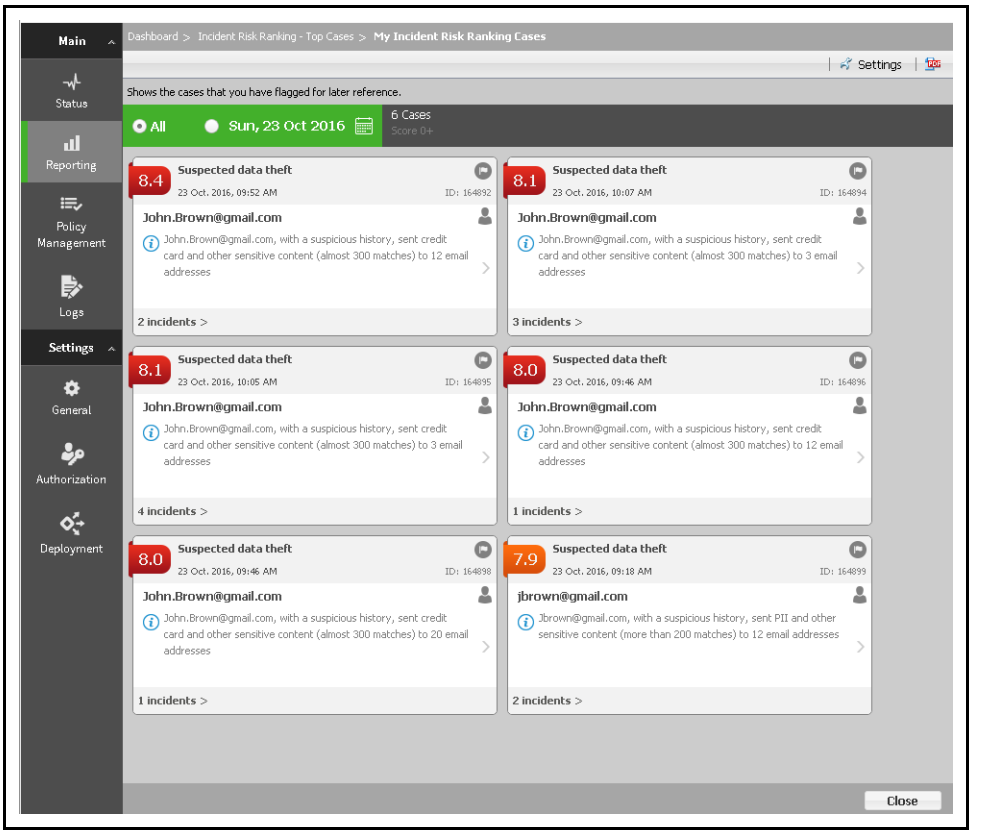
New My Cases report

Starting v8.3, you can add cases from the **Incident Risk Ranking – Top Cases** report to a personal case list known as ***My Cases***. A flag ( ) has been added to the case cards for this purpose.

Use My Cases as a temporal workbench for tracking cases that you're working on or for storing cases for future inspection. This report can show all cases that you have

flagged or only those from a specific date.

You can have up to 200 cases in your My Cases list.



You must have a role with **Summary reports** permissions to view any of the Incident Risk Ranking reports.

More information on the case card

In v8.3, the case card has been redesigned to provide more details.

Information about the incident source and reasons for the incident are now on the front of the case card. For example:

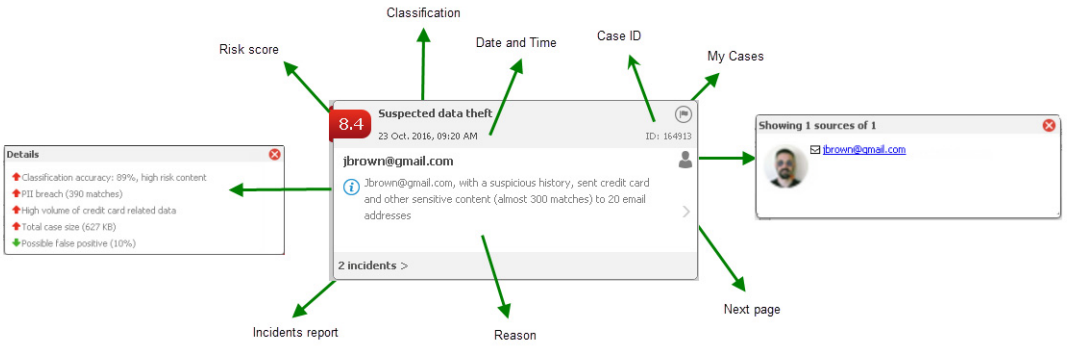
```
jbrown@gmail.com sent credit card and other sensitive
content (almost 300 matches) to 3 common email addresses.
```

Click the person icon ( ) to view the LDAP role and picture of the source if available.

To view case details, click the ( ) icon on the card. This provides the case summary that was previously on the front of the case card.

To add a case to or remove it from your *My Cases* list, click the flag ( ) icon.

The other elements on the card are the same as in previous versions. For example, to view incident details, click the number of incidents link. This leads you to the TRITON AP-DATA incidents report where you can drill down into incident specifics, including forensics.

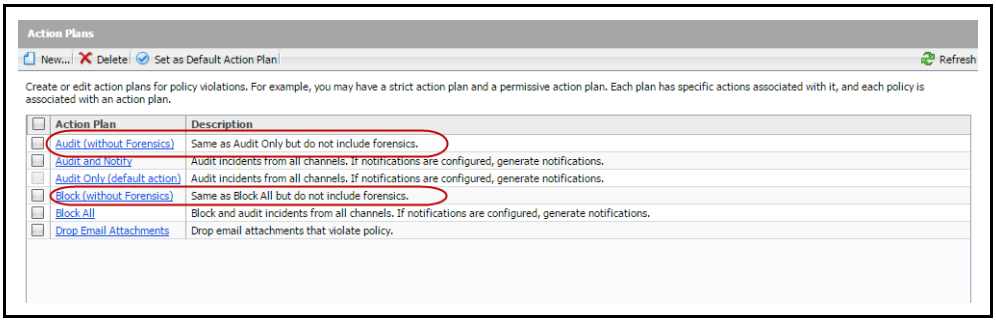


Audit and block without forensics

Two new action plans have been added to TRITON AP-DATA in v8.3:

- Audit Without Forensics
- Block Without Forensics

These actions are the same as Audit Only and Block All, except they do not capture forensic data so they decrease storage requirements. These action plans are ideal for regulations that require that user data will not be stored, such as PCI.



Updated third-party support

This release of TRITON AP-DATA adds support for the following:

- IBM Domino v9 discovery
- Microsoft SQL Server 2016 fingerprinting and discovery

SQL Server 2016 is now also a supported reporting and incident database for the TRITON management server.

End of life for FCI agent

Starting with v8.3, TRITON AP-DATA no longer supports the Microsoft FCI agent, new or existing. As a result, FCI configuration options are no longer available in the TRITON Manager.

New and enhanced policies/classifiers

In v8.3, there are many new and improved policies, rules, and classifiers.

New

- Rules for the policies “Software Source Code”, “ITAR”, “Export Administration Regulations (EAR)”, “Smart Power Grids / SCADA”, “Data Sent During Unusual Hours”, “Suspected Mail to Self”, and “Software Source Code for Discovery” that identify Python source code.
- “Wide” and “Narrow” rules for the policy “Password Files” for detection of SAM files.
- Rules to the policy “Password Files” to identify .htpasswd files (Apache HTTP Servers' password files).
- Rule to the policy “Confidential Warning” to detect a dictionary phrase in a header or a footer.
- Rules to the policy “Israel PII” to identify 8- or 7-digits Israeli Identity Number, replacing other related rules in the policy.
- Three new classifiers: “Python Source Code (Wide)”, “Python Source Code (Default)”, and “Python Source Code Extensions”.
- Four new classifiers: “Security Accounts Manager (SAM) Files - Textual (Wide)“, “Security Accounts Manager (SAM) Files - Textual (Default)”, “Security Accounts Manager (SAM) Files - Textual (Narrow)”, and “Security Accounts Manager (SAM) Files (Registry)”.
- Seven new classifiers: “.htpasswd file that uses the crypt hash function (Wide)”, “.htpasswd file that uses the crypt hash function (Default)”, “.htpasswd file that uses the crypt hash function (Narrow)”, “Security Accounts Manager (SAM) Files - Textual (Wide)”, “Security Accounts Manager (SAM) Files - Textual (Default)”, “Security Accounts Manager (SAM) Files - Textual (Narrow)”, and “.htpasswd File Name”.
- One new file-type classifier, “Outlook Restricted-Permission Message”.
- One new script classifier, “Dictionary Phrase in Header/Footer”.
- Replaced the pattern classifier, “PIN with proximity”, with the new script classifier, “PIN with proximity”, that masks the PIN.
- Replaced 4 Israeli Identity Number-related classifiers, “Israeli ID (Narrow)”, “Israeli ID: 7 or 8 digits with proximity”, “Israeli ID (Default + 7 or 8 digits)”,

and “Israeli ID with proximity” with 7 new classifiers: “Israeli Identity Number Near Term”, “Israeli Identity Number - 8-Digits (Default)”, “Israeli Identity Number - 8-Digits (Wide)”, “Israeli Identity Number (8-Digits) Near Term”, “Israeli Identity Number - 7-Digits (Default)”, “Israeli Identity Number - 7-Digits (Wide)”, and “Israeli Identity Number (7-Digits) Near Term”.

Enhanced

- Accuracy of the quick policies, “Malaysia PII”, “France PII”, “Australia PII”, “Canada PII”, “Ireland PII”, and “US PII”, by changing some rules to be enabled only on the Wide sensitivity.
- Raised the threshold of the rules “South Korea PII: Korea Phones” and “Japan PII: Telephone Numbers” to 10.
- Accuracy of the “Various Archive Formats” and “Various Spreadsheet Formats” file-type classifier.
- Accuracy of the rules, “Password Files: SAM Files (Default)” and “Counter Malicious: Password files”, by adding coverage of textual SAM password files.
- Accuracy of magnetic track-related classifiers.
- Changed the classifier, “PCI Audit: CCN with CVV”, to mask the CVV and the magnetic track-related classifiers to mask the magnetic tracks.
- Changed rules in the following data-in-motion policies to use the default action plan “Audit Without Forensics”: “Credit Card Magnetic Strips”, “EU finance”, “FCRA”, “FFIEC”, “IT asset information”, “Michigan Privacy Act SB 309”, “PCI”, “PCI Audit”, “Peoples Republic of China Finance”, “Suspected Malicious Dissemination”, and “Wisconsin SB 164”.
- Changed rules in the following discovery policies to use the default action plan “Audit Without Forensics”: “General Sensitive Information for Discovery”, “PCI for discovery”, “PCI Audit for discovery”, “Peoples Republic of China Finance for Discovery”, and “Suspected Malicious Dissemination for Discovery”.
- Renamed both the classifier, “Text in Header/Footer”, and related rule, “Text in Header/Footer”, to “Key Phrase in Header/Footer”.
- Renamed the Data privacy policy category “European Union” to “European Union (GDPR)” to support compliance with EU-wide data privacy regulations.
- Changed names and descriptions of entities relating to Kennitala (Icelandic ID numbers) to indicate that they only catch Kennitala of individuals.
- Updated the names and descriptions of several file types, file-type classifiers, and rules to remove references to Office files’ specific yearly versions.
- Accuracy of the Israeli Identity Number-related rules.

TRITON AP-ENDPOINT DLP

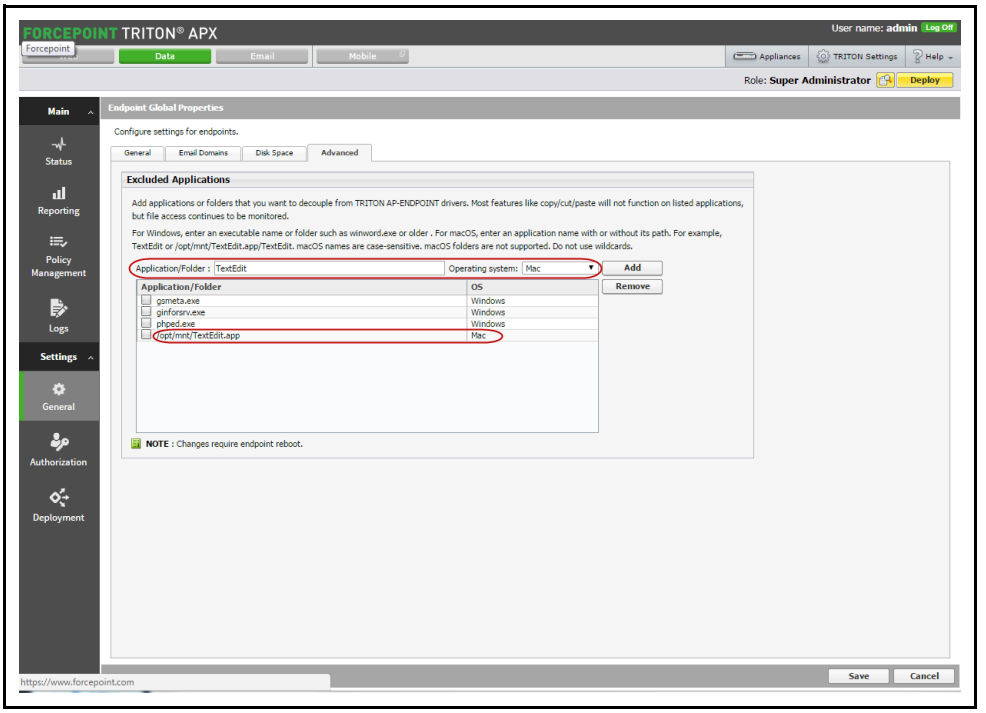
Endpoint application exclusion for macOS

Until now, the system allowed you to exclude Windows-based endpoint applications from TRITON AP-ENDPOINT drivers when necessary—for example, when they are experiencing compatibility problems with the endpoint software.

Starting with v8.3, you can also exclude macOS-based applications when needed.

To do so, select **Settings > General > Endpoint** and then select the **Advanced** tab. Enter the name, operating system, and file path as prompted.

Most features like copy/cut/paste will not function on listed applications, but file access continues to be monitored.



User confirmation dialog

The dialog box used to get confirmation from end users when they perform a disallowed endpoint operation has been redesigned.

The new design enables trusted users to make an informed decision on whether they should **Allow** or **Block** the transfer of data that triggered a DLP policy rule. Users must provide a justification if they decide to authorize the transaction. Possible reasons include:

- Required for business purposes

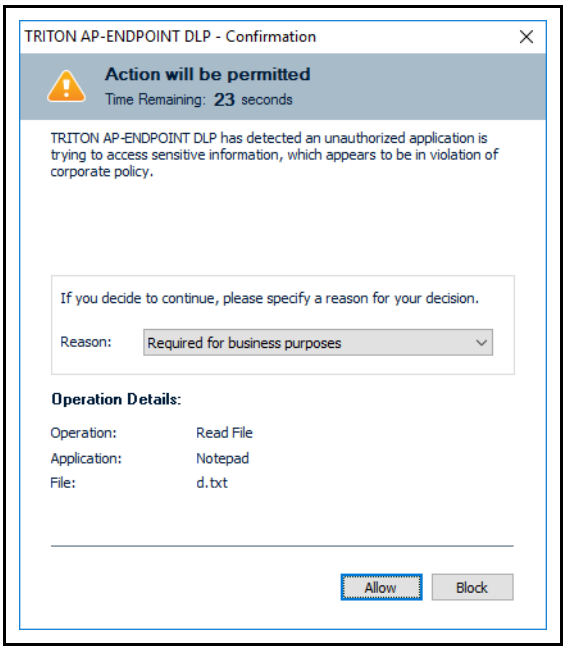
- Approved by my manager
- Personal data
- Not confidential

Users are given 30 seconds to respond, and they are shown the time that is remaining before the action is blocked. They are also given operation details to consider.

The confirmation dialog is shown when you select the **Confirm** action for one or more endpoint channels in your action plan in the TRITON Manager.

The Confirm action is only available on endpoints that are installed with Interactive mode. In Stealth mode, users are never prompted for action.

In v8.3, the Confirm action works for all endpoint channels except HTTP/HTTPS which is planned for a future release.



Bypass enforcement

In this version, bypass codes apply to specific endpoint hosts only, and the system validates the hostname before bypassing security. Administrators must select the affected endpoint client before generating the code.

Support for macOS 10.12 (Sierra)

TRITON AP-ENDPOINT DLP can now run on macOS operating system, v10.12 (Sierra). Mixed mode (combined DLP and web) is not yet supported on this platform.

IMPORTANT: This endpoint release does not support the macOS 10.12.1 or higher operating system update. If you are deploying Mac endpoints to macOS 10.12

systems, we strongly recommend turning off automatic OS updates until support for macOS 10.12.1 is announced by Forcepoint.

Ability to block posts in Chrome browsers

In this release, TRITON AP-ENDPOINT DLP is able to block posts that violate DLP policies in Chrome browsers. This block mode was removed in a previous release of the endpoint software due to content scanning performance limitations.

Requirements

Updated: 24-Jan-2017

Applies To:	Forcepoint TRITON AP-DATA v8.3.0

Operating system support

For the operating system requirements of TRITON AP-DATA modules, see the Deployment and Installation Center in the Forcepoint Technical Library, and click TRITON AP-DATA Requirements. There are no changes to operating system support in v8.3.

Starting with v8.2.5 however, the protector and mobile agent began running on CentOS 7.

Hardware requirements

See the Deployment and Installation Center in the Forcepoint Technical Library for TRITON AP-DATA hardware requirements. Click TRITON AP-DATA Requirements and then scroll below the operating system table. Requirements are listed for each TRITON AP-DATA module. There are no changes to hardware requirements in v8.3.

Backward compatibility

Where indicated below, TRITON AP-DATA v8.3.0 can support older supplemental servers, agents, and endpoints.

Supplemental servers

The TRITON management server v8.3.0 is fully compatible with Data Security supplemental servers v7.8.x and later.

Agents

The following agents are supported with the TRITON management server v8.3.0.

- Crawlers, protectors, and mobile agents running version 7.8.x or later
- Analytics engine v8.2.5

The FCI agent is no longer supported starting with v8.3.

Version 8.3 does not support older versions of TRITON AP-DATA Email Gateway for Office 365.

Endpoint

TRITON AP-DATA v8.3.0 can support older endpoint versions.

Version 7.8.x through 8.2.x endpoints are fully compatible with the v8.3.0 management server. They can accept new policies, classifiers, profiles, incidents, fingerprint updates, and status notifications. To take advantage of new features, however, they must be upgraded to v8.3.0. Version 8.3 does not support v7.7.x endpoints or earlier.

Version 8.3 endpoints can work with the following TRITON management servers and AP-DATA servers; however, endpoint features that were added after the manager release—such as support for screen captures on macOS—won't work. Version 8.3 endpoints will benefit from their updated operating system and browser support.

- v7.8.4
- v8.0
- v8.0.1
- v8.1
- v8.2
- v8.2.5

TRITON AP-WEB

The Web Content Gateway included in TRITON AP-WEB has an on-board DLP policy engine. It must be at v7.8.x or later to work with TRITON AP-DATA v8.3.0.

Note that TRITON AP-DATA Gateway v8.3 also includes a Web Content Gateway module. It is always at the same version as the management server. For more details, see Content Gateway appliance for web DLP and SSL decryption.

TRITON AP-EMAIL

TRITON AP-EMAIL includes an on-board DLP policy engine. It must be at v7.8.x or later to work with TRITON AP-DATA v8.3.0.

Installation and Upgrade

Updated: 24-Jan-2017

Applies To:	Forcepoint TRITON AP-DATA v8.3.0

New installation

A step-by-step guide to installing TRITON AP-DATA can be found here:

- Installing TRITON AP-DATA v8.3.x

Before you begin, open Windows Control Panel and verify that the "Current language for non-Unicode programs" in the Administrative tab of the Region and Language settings is set to English. After the installation, you can change it back to the original language.

Upgrading TRITON AP-DATA

Data Security must be at least version 7.8.4 in order to upgrade to TRITON AP-DATA v8.3. If you have an earlier version, there are interim steps to perform. These are shown in the table below.

Your current version	Step 1	Step 2	Step 3	Step 4
7.6.x	Upgrade to 7.7.2	Upgrade to 7.8.4	Upgrade to 8.3.x	
7.7.x	Upgrade to 7.8.4	Upgrade to 8.3.x		
7.8.1 - 7.8.3	Upgrade to 7.8.4	Upgrade to 8.3.x		
7.8.4 - 8.2.x	Upgrade to 8.3.x			

Step-by-step instructions for upgrading your Data Security installation can be found here:

- Upgrading to TRITON AP-DATA v8.3.0.

Resolved and known issues

Updated: 24-Jan-2017

Applies To:	Forcepoint TRITON AP-DATA v8.3

A list of resolved and known issues is available in the Forcepoint Knowledgebase. You must log on to My Account to view the list.