

Release Notes for Forcepoint DLP v8.4.0

Release Notes | Forcepoint DLP | v8.4.0 | 31-July-2017

Use the Release Notes to find information about what's new and improved in Forcepoint DLP v8.4.0.

- *Forcepoint DLP New Features*, page 2
 - *Product and component renaming*, page 2
 - *Fresh toolbar design*, page 2
 - *Improved performance*, page 3
 - *Forcepoint DLP Cloud Applications data in motion support for Box*, page 3
 - *Incident risk ranking enhancements*, page 3
 - *Microsoft RMS integration*, page 4
 - *Data classification enhancements*, page 5
 - *Increased maximum file size for analysis*, page 5
 - *ICAP support for cloud-based deployments*, page 5
 - *Discovery task status reports and error messages*, page 5
 - *New and enhanced policies, rules, and classifiers*, page 6
 - *Other enhancements*, page 15
- *Forcepoint DLP Endpoint New Features*, page 16
 - *Support for macOS 10.12.2, 10.12.3, 10.12.4, and 10.12.5 (Sierra)*, page 16
 - *Support for Secure Boot mode in Windows 10, version 1607*, page 16
 - *Support for Windows 10 Creators Update, version 1703*, page 17
 - *User confirmation dialog timeout updates*, page 17
- *Installation and Upgrade*, page 18
- *Resolved and known issues*, page 19

New in Forcepoint DLP

Release Notes | Forcepoint DLP | v8.4.0 | 31-July-2017

Version 8.4.0 of Forcepoint DLP offers several new features and product updates.

Forcepoint DLP New Features

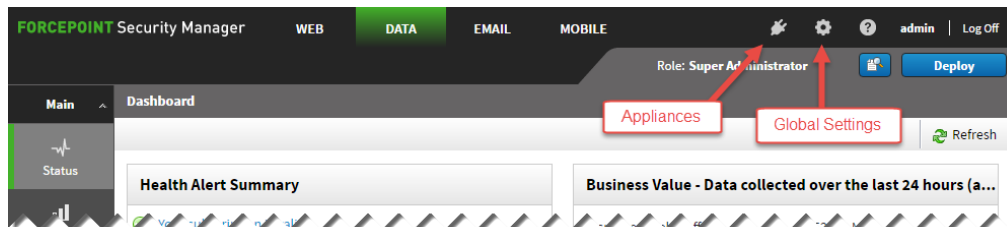
Product and component renaming

In this release, Forcepoint has introduced a simplified and more descriptive product and component naming scheme. Key changes for this product include:

Old Name	New Name
TRITON AP-DATA	Forcepoint DLP
TRITON AP-DATA Cloud App Security	Forcepoint DLP Cloud Applications
TRITON AP-DATA Discover	Forcepoint Data Discovery
TRITON AP-DATA Gateway	Forcepoint DLP Network
TRITON AP-ENDPOINT DLP	Forcepoint DLP Endpoint
TRITON AP-EMAIL	Forcepoint Email Security
TRITON AP-WEB	Forcepoint Web Security
TRITON Manager	Forcepoint Security Manager (Security Manager)
TRITON Settings	Global Settings

Fresh toolbar design

The Forcepoint Security Manager banner and toolbars have been combined and streamlined. The functionality has not changed, but the toolbars now have a smaller footprint, allowing more room to display the main content of the application.



Although the Appliances, Global Settings, and Help toolbar buttons have been made more compact, their functionality is still available. Find the new buttons at the top of the page, next to the name of the logged-on administrator.

Improved performance

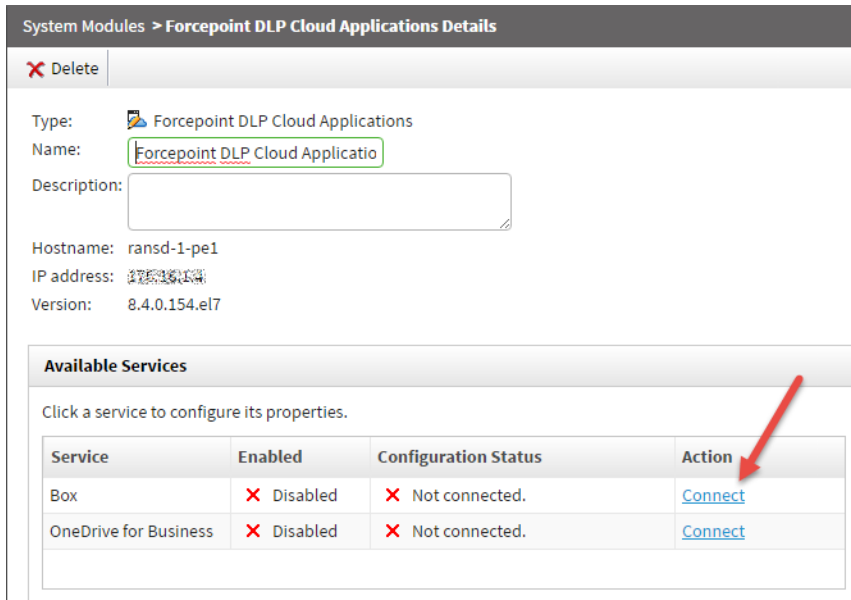
Performance has been enhanced for the following features and functions:

- Fingerprint detection
- Importing Active Directory resources into Forcepoint DLP
- Viewing incidents with large forensics in Incidents reports

Forcepoint DLP Cloud Applications data in motion support for Box


Forcepoint DLP Cloud Applications now includes data-in-motion support for files uploaded and shared within the Box cloud content management platform. As with Microsoft OneDrive for Business, when the Cloud Services channel is enabled in DLP policies, the cloud agent can be used to audit or remediate the uploading or sharing of sensitive data within the cloud service.

Once the cloud agent has been installed and registered, select it on the Settings > Deployment > System modules page to configure its connection to Box.



System Modules > Forcepoint DLP Cloud Applications Details

[Delete](#)

Type:  Forcepoint DLP Cloud Applications

Name:

Description:

Hostname: ransd-1-pe1

IP address: 172.16.1.4

Version: 8.4.0.154.el7

Available Services

Click a service to configure its properties.

Service	Enabled	Configuration Status	Action
Box	✘ Disabled	✘ Not connected.	Connect
OneDrive for Business	✘ Disabled	✘ Not connected.	Connect

Incident risk ranking enhancements

- Administrators can now identify high-risk resources and configure incident risk ranking reports to include the high-risk classification as a factor in calculating a case's risk score.

With this feature, administrators can bring in information about known high-risk employees or contractors from external data sources (such as an HR system) and have that information factored into the incident risk ranking process.

a. Create one or more business units containing users considered to be high-risk on the Main > Policy Management > Resources > Business Units page in the Data Security module of the Security Manager.

b. Add business units as high-risk resources on the Settings > General > Analytics page.

In this release, only user resources can be added as high-risk resources. If a business unit added as a high-risk resource contains other types of resources, the non-user resources are not considered for risk scoring.

c. Select **Use high-risk resources for risk scoring** to enable the feature.

- When administrators view the source associated with a case, a new quick link option can be used to display a report of that source's incidents for the past 30 days.
- Reporting permissions to access **Incident Risk Ranking reports** can now be granted or denied in administrative roles.
- Incident risk ranking case cards now include a new classification: broken business process. This classification indicates that the incidents in this case may be the result of systematic business process deficiencies.

For example, if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong. This classification is based on factors such as recurring patterns that could indicate common behavior.

- The analytics engine now performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.

This gives administrators a more complete picture of a user's activity across multiple channels. It also reduces clutter in the incident risk ranking reports, allowing cases from more users to appear on the same page.

Microsoft RMS integration

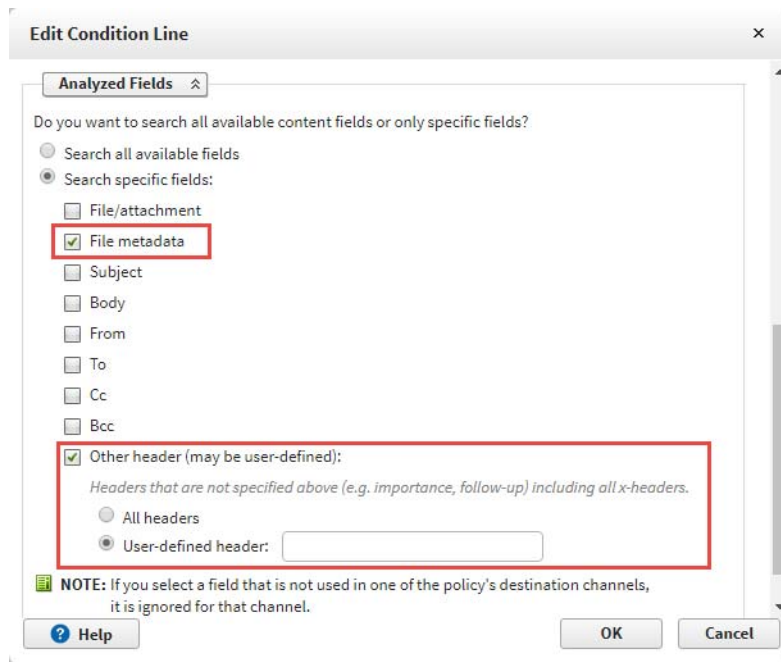
Forcepoint DLP now integrates with Microsoft Azure Information Protection using Microsoft Rights Management Service (RMS). This allows Forcepoint DLP Endpoint to apply DLP policies to Microsoft RMS encrypted files on Windows endpoints.

This feature enables enterprises to maintain sensitive data visibility and control for files protected using Microsoft Azure and AD RMS. It can also be used to better understand how Microsoft RMS is being used by employees to protect sensitive data.

Data classification enhancements

Policy rule configuration now includes the option to target DLP classifiers in file metadata. This allows Forcepoint DLP to detect data classification labels applied by Forcepoint data classification partners, including Microsoft, Boldon James, and Titus.

To configure metadata and custom header analysis, edit content classifier properties on the Condition tab of a selected DLP policy rule.



Increased maximum file size for analysis

The maximum file size for files analyzed through Web Content Gateway and ICAP-based integrated proxies has been raised to 50 MB.

ICAP support for cloud-based deployments

The Forcepoint DLP Cloud Agent can now be configured to use ICAP for web proxy integration. The configuration process for cloud agent ICAP support is the same as for protector ICAP support, and is described in the Forcepoint DLP Administrator Help.

Discovery task status reports and error messages

Administrators creating or editing a discovery task can now configure the product to send a status report via email when the discovery task is complete. By default, the email message includes information about the task name and type, as well as the task start and end time, enabling administrators to keep a detailed audit log of each completed discovery task.

In order for the email report option to function, port **17514** must be open for incoming connections (inbound) in the Windows firewall on the Forcepoint management server machine.

Configure the emailed status report on the new **Email Report** page in the discovery task wizard:

Network: Discovery Tasks > Exchange Discovery Task

Task Properties

- General
- Exchange Servers
- Mailboxes & Folders
- Scheduler
- Policies
- Filtering
- Email Report**
- Advanced

Email Report

Enable this option to have a status report on the scanned files sent via email when the discovery task is complete

Email discovery report

Sender name: Example: John Doe

Sender email address: Example: administrator@mycompany.com

Outgoing mail server: 127.0.0.1 Port: 25

Subject:

Message body: The discovery report for the following task is attached %Task Name% (%Task Type%)
The task started at: %Task Start Time%
The task completed at: %Task End Time%

Recipients: None

Additional email addresses:

Comma-separated list of email addresses for administrators authorized to receive discovery details and other confidential data

To aid in troubleshooting, data discovery error messages have been enhanced to provide more detail about the reason for the scanning failure (for example, when an item was not found, or a connectivity error occurred). In the past, the same error message might appear differently in different places. Now, the message is consistent, regardless of where it appears.

In addition, administrators now have the option to specify whether to include all transactions or only error transactions in downloaded and email discovery reports. Configure this option on the **Advanced** page in the discovery task wizard.

New and enhanced policies, rules, and classifiers

With the policies added in this release, Forcepoint DLP now has full PII policy coverage for EU countries. In addition, a European General Data Protection Regulation (GDPR) policy category has been added.

New

- The policy category “EU General Data Protection Regulation (GDPR)” was added to the Data in motion and Discovery policy trees. It includes policies that protect the personal data of individuals within the European Union.
- The following policies were added:

- “Philippines Data Privacy Act” for detection of sensitive personal information, including individuals’ age, color, health, genetics, offense committed, and ID numbers
- “Ukraine CV and Resume” and “Ukraine CV and Resume for Discovery” for detection of documents comprising resumes and CVs in Ukrainian, Russian, and English
- EU PII policies for data in motion and discovery:
 - Bulgaria PII
 - Cyprus PII
 - Estonia PII
 - Latvia PII
 - Lithuania PII
 - Luxembourg PII
 - Malta PII
 - Portugal PII
 - Austria PII for Discovery
 - Bulgaria PII for Discovery
 - Croatia PII for Discovery
 - Cyprus PII for Discovery
 - Estonia PII for Discovery
 - Latvia PII for Discovery
 - Lithuania PII for Discovery
 - Luxembourg PII for Discovery
 - Malta PII for Discovery
 - Portugal PII for Discovery
 - Slovenia PII for Discovery
- EU Finance policies for data in motion and discovery:
 - Bulgaria Finance
 - Croatia Finance
 - Cyprus Finance
 - Latvia Finance
 - Lithuania Finance
 - Malta Finance
 - Portugal Finance
 - Slovenia Finance
 - Austria Finance for Discovery
 - Belgium Finance for Discovery
 - Bulgaria Finance for Discovery
 - Croatia Finance for Discovery
 - Cyprus Finance for Discovery
 - Czech Republic Finance for Discovery
 - Estonia Finance for Discovery
 - Hungary Finance for Discovery

- Latvia Finance for Discovery
- Lithuania Finance for Discovery
- Luxembourg Finance for Discovery
- Malta Finance for Discovery
- Portugal Finance for Discovery
- Romania Finance for Discovery
- Slovakia Finance for Discovery
- Slovenia Finance for Discovery
- The rule “MAR: Form 10-K (Standard Fiscal Year)” was added to policy “Model Audit Rule (MAR).”
- The rule “COPPA: PII of Children (Default)” was added to policy “Children’s Online Privacy Act (COPPA).”
- The rule “Brazil PII: National Register of Legal Entities Number” was added to policies “Brazil PII” and “Brazil Private Information For Discovery.”
- Rules were added to the policies “Philippines PII” and “Philippines PII for Discovery.”
- Rules that detect SPSS text files were added to the policies “Norway Health Data Privacy Act,” “Italy Health Data Privacy Act,” “HIPAA,” “Israeli Health Care,” “Health Data,” “Sweden PHI,” “Health Data For Discovery,” and “Sweden PHI For Discovery.”
- The file type classifier “Borland Reflex 2” and the rule “Database File: Borland Reflex 2” were added to policies “Database Files” and “Database Files For Discovery.”
- There are several new script classifiers:
 - “Maximum Age (Default)” and “Minimum Age (Default)”
 - Classifiers related to the Philippine Data Privacy Act:
 - Philippine Taxpayer Identification Number (Wide)
 - Philippine Taxpayer Identification Number (Default)
 - Philippine Taxpayer Identification Number Near Term
 - Philippine SSS Number (Wide)
 - Philippine SSS Number (Default)
 - Philippine SSS Number Near Term
 - PhilHealth Identification Number (Wide)
 - PhilHealth Identification Number (Default)
 - PhilHealth Identification Number Near Term
 - IBAN-related classifiers:
 - IBAN Bulgaria
 - IBAN Bulgaria (Wide)
 - IBAN Croatia
 - IBAN Croatia (Wide)
 - IBAN Cyprus
 - IBAN Cyprus (Wide)
 - IBAN Latvia

- IBAN Latvia (Wide)
- IBAN Lithuania
- IBAN Lithuania (Wide)
- IBAN Malta
- IBAN Malta (Wide)
- IBAN Portugal
- IBAN Portugal (Wide)
- IBAN Slovenia
- IBAN Slovenia (Wide)
- EU ID-number classifiers:
 - Cypriot Tax Identification Code Near Term
 - Maltese Identity Card Number Near Term
 - Luxembourgian National Identification Number - 11 Digits (Wide)
 - Luxembourgian National Identification Number - 11 Digits (Default)
 - Luxembourgian National Identification Number - 11 Digits Near Term
 - Luxembourgian National Identification Number - 13 Digits (Wide)
 - Luxembourgian National Identification Number - 13 Digits (Default)
 - Luxembourgian National Identification Number - 13 Digits Near Term
 - Bulgarian Unified Civil Number (Wide)
 - Bulgarian Unified Civil Number (Default)
 - Bulgarian Unified Civil Number Near Term
 - Latvian Personal Identity Number (Wide)
 - Latvian Personal Identity Number (Default)
 - Latvian Personal Identity Number Near Term
 - Estonian Personal Identification Code (Wide)
 - Estonian Personal Identification Code (Default)
 - Estonian Personal Identification Code Near Term
 - Lithuanian Personal Code (Wide)
 - Lithuanian Personal Code (Default)
 - Lithuanian Personal Code Near Term
 - Portuguese Document Number (Wide)
 - Portuguese Document Number (Default)
 - Portuguese Document Number Near Term
 - Portuguese Tax Identification Number of Individuals (Wide)
 - Portuguese Tax Identification Number of Individuals (Default)
 - Portuguese Tax Identification Number of Individuals Near Term
 - Portuguese Social Security Number (Wide)
 - Portuguese Social Security Number (Default)
 - Portuguese Social Security Number Near Term
- “National Register of Legal Entities Number (Wide),” “National Register of Legal Entities Number (Default),” and “National Register of Legal Entities Number Near Term”

- New policies and a pattern classifier were added to detect the content of Windows registry files.
 - The policies are “.REG Files” and “.REG Files for Discovery.”
 - The pattern classifier is “.REG File.”
- New policies and classifiers were added for detecting records of SQL table data extracted from a database:
 - The policies are “Database Dumps/Backup Files” and “Database Dumps/Backup Files for Discovery.”
 - The file type classifier is “Microsoft Tape Format.”
 - The pattern classifiers are “MySQL-Format Database Dump (Wide)” and “MySQL-Format Database Dump (Default).”
- New policies and script classifiers were added for detecting Austrian private information:
 - The policy is “Austria PII.”
 - The script classifiers are “Austrian Social Security Number (Wide),” “Austrian Social Security Number (Default),” and “Austrian Social Security Number Near Term.”
- New policies and a dictionary classifier were added for detecting bids, proposals, and tenders, such as responses to request for proposal (RFP) and invitation for bids (IFB) documents:
 - The policies are “Bids and Tenders” and “Bids and Tenders for Discovery.”
 - The dictionary classifier is “Bids and Tenders.”
- The file type classifier “DICOM” was added for detection of medical imaging files. It is included in the following policies:

● FDA - 21 CFR	● HIPAA
● Health Data	● Health Data For Discovery
● Australia PHI	● Australia PHI For Discovery
● Israel PHI	● Israel PHI For Discovery
● Israeli Health Care	● Italy Health Data Privacy Act
● Italy PHI	● Italy PHI For Discovery
● Information Governance Toolkit	● Norway Health Data Privacy Act
● Norway PHI	● Norway PHI For Discovery
● US PHI	● US PHI For Discovery
● UK PHI	● UK PHI For Discovery
● Sweden PHI	● Sweden PHI For Discovery
● Swedish Patient Data Act (SFS 2008:355 Patientdatalagen)	● Swedish Patient Data Act (SFS 2008:355, Patientdatalagen) - For Discovery
- New pattern classifiers were added for EU PII:
 - Maltese Identity Card Number
 - Cypriot Tax Identification Code

- There are three new RMS-related file types:
 - RMS-Protected Microsoft Word Documents (Legacy)
 - RMS-Protected Microsoft Excel Spreadsheets (Legacy)
 - RMS-Protected Microsoft PowerPoint Presentations (Legacy)
- There are several additional new file types:

File type	Format Group
B1	Archive formats
Borland Reflex 2	Database formats
Ichitaro Compressed	Word-processing formats
Macro-enabled Microsoft Visio Stencil	Computer-aided design formats
Macro-enabled Microsoft Visio Template	Computer-aided design formats
Microsoft Visio Stencil	Computer-aided design formats
Microsoft Visio Template	Computer-aided design formats
MPEG-4	Multimedia formats
Ogg	Multimedia formats
RAR5	Archive formats
Sony Wave64	Multimedia formats
WavPack	Multimedia formats
xz	Archive formats

- The “Archive formats” file types were added to the Various Archive Formats classifier.
- The “Multimedia formats” files types were added to the Various Multimedia Formats classifier.
- The Visio file types were added to the Microsoft Visio File classifier.
- The Ichitaro Compressed file type was added to the Various Word Processing Formats classifier.

Enhanced

- The accuracy of the quick policy “Taiwan PII” was improved.
- The following policies were renamed:
 - “COPPA” became “Children's Online Privacy Protection Act (COPPA).”
 - “HR Russia and Ukraine for Discovery” became “Russia CV and Resume for Discovery.”
 - “Israel Data for Discovery” became “Israel PII for Discovery.”
 - “Resume for HR Cyrillic” became “Russia CV and Resume.”
 - “Resume for HR” became “CV and Resume in English.”

- “Resume for HR Israel” became “Israel CV and Resume.”
- “Self CV Distribution” became “Self CV/Resume Distribution.”
- “Resume for HR English for Discovery” became “CV and Resume in English for Discovery.”
- “Resume for HR Israel for Discovery” became “Israel CV and Resume for Discovery.”
- “Russia Federal Act 152-FZ” became “Russian Federal Law No. 152-FZ.”
- “Russia Private Information for Discovery” became “Russia PII for Discovery.”
- “SOX” became “Sarbanes-Oxley Act (SOX).”
- The following rules were renamed:
 - “Brazil PII: RG” in policy “Brazil PII” became “Brazil PII: Identity Card Number (Default).”
 - “Brazil PII: RG Narrow” in policy “Brazil PII” became “Brazil PII: Identity Card Number (Narrow).”
 - “Brazil PII: RG Numbers” in policy “Brazil PII” became “Brazil PII: Identity Card Number.”
 - “CCN - High Accuracy” in policy “Credit Cards” became “Credit Card Number (Default).”
 - “COPPA: PII and Age” in policy “Children’s Online Privacy Protection Act (COPPA)” became “COPPA: PII of Children (Wide).”
 - “PCI Audit: Wide” in policy “PCI Audit” became “PCI Audit: Credit Card Number (Extra Wide).”
- Using multiple phrases for the following classifiers is now supported:
 - Key Phrases in Headers/Footers
 - Dictionary Phrases in Headers/Footers
- The “Customizable IDs” script classifier was made visible in the Security Manager. In addition, the parameters “Check digit position,” “Support terms pattern,” and “Support terms case sensitivity” were added to it.
- The following classifiers were renamed:
 - “10K Form” became “Form 10-K (Standard Fiscal Year).”
 - “10K Form (Non Standard Fiscal Year)” became “Form 10-K (Non Standard Fiscal Year).”
 - “10Q Form” became “Form 10-Q (Standard Fiscal Year).”
 - “10Q Form (Non Standard Fiscal Year)” became “Form 10-Q (Non Standard Fiscal Year).”
 - “CV in Chinese (wide)” became “CV and Resume in Chinese (Wide).”
 - “CV in Chinese (default)” became “CV and Resume in Chinese (Default).”
 - “CV in Chinese (narrow)” became “CV and Resume in Chinese (Narrow).”
 - “CV in English” became “CV and Resume in English.”

- “CV in Russian or Ukraine” became “CV and Resume in Russian or Ukraine.”
- “CV support - period of years” became “Year Period.”
- “CV terms - Hebrew” became “CV and Resume Terms in Hebrew.”
- “Microsoft Visio File - All Versions” became “Microsoft Visio File.”
- “Russian Individual Personal Account Insurance number” became “Russian Personal Pension Account Number (SNILS).”
- “SOX: 10Q Form Phrases” became “Form 10-Q Phrases.”
- “Support terms for Russian Individual Personal Account Insurance numbers” became “Support terms for Russian Personal Pension Account Numbers (SNILS).”
- Accuracy of the following script classifiers was improved:
 - “Date Of Birth,” “Date Of Birth (ages 20-65),” and “Date Of Birth (ages 10-90)”
 - “Form 10-K (Standard Fiscal Year)” and “Form 10-K (Non Standard Fiscal Year)”
 - “Form 10-Q (Standard Fiscal Year)” and “Form 10-Q (Non Standard Fiscal Year)”
 - “Malaysia ID: with date validation,” “Malaysia ID: with date validation, with proximity,” “Malaysia ID: with date and BP validation,” and “Malaysia ID: with date and BP validation, with proximity”
 - “Mexico RFC Number (Default)” and “Mexico RFC Number (Wide)”
 - “Routing Number (Wide),” “Routing Number (Default),” and “Routing Number (Narrow)”
 - “Russian Personal Pension Account Number (SNILS)”
 - Script classifiers related to credit card numbers
 - “Taiwan ID” and “Taiwan ID with support”
- The following script classifiers were both renamed and given improved accuracy:
 - “US Age: greater than” became “Minimum Age (Wide).”
 - “US Age: smaller than” became “Maximum Age (Wide).”
- Both accuracy and masking were improved for the classifiers “Passwords for HTTP” and “Passwords.”
- Some file types were recategorized under the new format groups:
 - Cryptography formats
 - Project management formats
- Some file types had their format group changed.
- File type classifiers “RMS-Protected Microsoft Office Files” and “Microsoft Office File - All Versions” support additional file types.

- The new file types listed in the previous section were added to the following file type classifiers:
 - Various Archive Formats
 - Various Computer Aided Design Formats
 - Various Database Formats
 - Various MultiMedia Formats
 - Various Word Processing Formats
 - Microsoft Office Files - Non-RMS-Protected
 - Microsoft Office File - All Versions
 - Microsoft Visio File

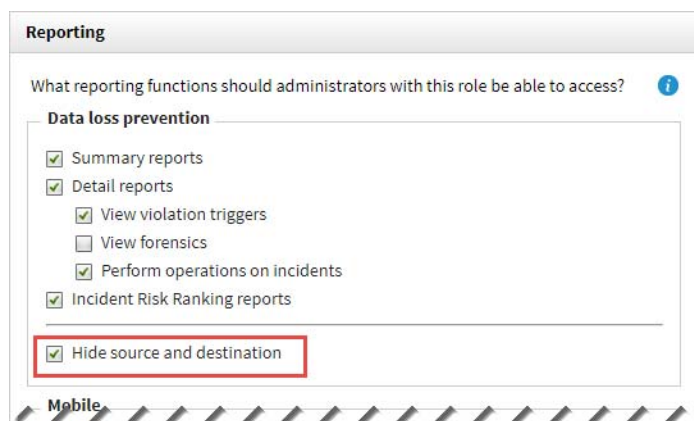
Removed

- The policy “Metadata keywords detection” was removed.
- The rule “Suspected Malware Communication (Narrow)” was removed from policy “Suspected Malware Communication.”
- The following script classifiers were removed:
 - “Malware (Narrow),” “Malware (Strict),” and “Malware (Wide)”
 - “User-defined dictionary (non-unique)” and “User-defined dictionary (unique)”
- The following format groups for file types were removed:
 - Animation formats
 - Communications formats
 - Encapsulation formats
 - Mixed formats
 - Outline/Planning formats
 - Time scheduling formats
 - Binary formats
 - Display formats
 - Graphic formats
 - Movie formats
 - Sound formats
- The following file type classifiers were removed:
 - Access Database Template Files (.accdt)
 - AD1 evidence file
 - BlackBerry Activation File (etp.dat)
 - Disk Image
 - Documentum EMCMP format (.emcmf)
 - eFax file
 - Electronic Publication
 - Ghost Disk Image File (*.gho, *.ghs)
 - Google SketchUp Format (.skp)
 - Health level7 message File
 - IFilter File
 - JBIG2 File Format(.jB2, .jbig2)
 - JPEG-2000 JP2 File Format Syntax (ISO/IEC 15444-1) (.jp2, .j2k, .pgx)
 - Microsoft Compiled HTML Help (.chm)

- Microsoft Outlook Express DBX
- Microsoft Outlook OST
- Milestone Document (.mls,.ml3,.ml4,.ml5,.ml6,.ml7,.ml8,.ml9)
- PostScript Type 1 Font (*.pfb)
- RealLegal E-Transcript File(*.ptx)
- Samsung Electronics Jungum Global document (*.gul)
- Shell Scrap Object File (.shs)
- Skype Log File
- Unicode HTML

Other enhancements

- Reporting permissions for administrative roles now include a setting to anonymize DLP reports:
 - a. Go to the **Settings > Authorization > Roles** page and select or create a role.
 - b. On the Role page, under Reporting > Data loss prevention, mark **Hide source and destination** to anonymize reports for administrators assigned to the role.
 - c. Click **OK** to save the change.



- The tool used for file type detection has been updated. This expands support for some existing file types and adds support for several others.
 - Pages (Legacy)
 - Keynote (Legacy)
 - Ichitaro Compressed
 - Sony Wave64
 - Ogg
 - xz
 - WavPack
 - PKCS #12 (p12) format
 - Numbers (Legacy)
 - Microsoft Visio Drawing
 - Macro-enabled Microsoft Visio Drawing
 - Macro-enabled Microsoft Visio Stencil
 - Macro-enabled Microsoft Visio Template
 - Microsoft Visio Stencil
 - Microsoft Visio Template
 - Borland Reflex 2

- B1
- RAR5
- MPEG-4

The Microsoft Visio File classifier was also updated, and a classifier and rule for detecting Borland Reflex 2 database files were added.

Forcepoint DLP Endpoint New Features

Support for macOS 10.12.2, 10.12.3, 10.12.4, and 10.12.5 (Sierra)

Forcepoint DLP Endpoint can now run on the macOS operating systems 10.12.2, 10.12.3, 10.12.4, or 10.12.5.

Also, Mac Mail 10.3, which was introduced with macOS 10.12.4, is supported.



Note

This Forcepoint DLP Endpoint release does not support macOS 10.12.1; however, it does support Mac OS X 10.10.x, Mac OS X 10.11.x, macOS 10.12.0, and macOS 10.12.2 and later.

Some features are not supported in this release:

- Clipboard support is only available between Microsoft Office 2011, Microsoft Office 2016, and Firefox. If either the source or the destination is not a supported application, the application name is empty.
- The Grab application only blocks when saved to a file and cannot block while capturing.
- Printer support is only available from Microsoft Office 2011, Microsoft Office 2016, and Firefox. Print support is not available for other applications.

Support for Secure Boot mode in Windows 10, version 1607

Forcepoint DLP Endpoint can now be installed on Windows 10 endpoints with Secure Boot enabled. When Secure Boot is enabled, Windows only loads kernel mode drivers that are digitally signed by Microsoft. In this release of Forcepoint DLP Endpoint, all affected drivers are digitally signed.

This change affects all new installations of Windows 10, version 1607. Starting with Windows 10, version 1607, Microsoft has enabled Secure Boot by default for all new installations. System upgrades from an earlier Windows operating system to Windows 10, version 1607, are not affected by this change.

For more information on driver signing changes in Windows 10, version 1607, see the following [Microsoft article](#).

Support for Windows 10 Creators Update, version 1703

Forcepoint DLP Endpoint can now be installed on the new Windows 10 Creators Update, version 1703.



Note

This Forcepoint DLP Endpoint release does not support the Edge 40 browser that is included as part of the Windows 10 Creators Update.

User confirmation dialog timeout updates

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

Users are still given 30 seconds to respond, by default, but the time may now be customized. You may now set the timeout length, per channel, to between 9 and 58 seconds.

Also, the confirm action now works on the HTTP/HTTPS channel. The confirm action was disabled on the HTTP/HTTPS channel in TRITON AP-ENDPOINT v8.3. With the addition of HTTP/HTTPS support in v8.4, all endpoint channels are now supported.

The confirmation dialog is shown when the **Confirm** action is selected for one or more endpoint channels in an action plan in the Forcepoint Security Manager.

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

Installation and Upgrade

Release Notes | Forcepoint DLP | v8.4.0 | 31-July-2017

Operating system and hardware requirements

For the operating system and hardware requirements of Forcepoint DLP modules, see the [Deployment and Installation Center](#).

New installation

For a step-by-step guide to installing Forcepoint DLP, see the [Forcepoint DLP Installation Guide, v8.4.x](#).

Before you begin, open the 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 installation, you can change it back to the original language.

Upgrading Forcepoint DLP

Your data security product must be at version 7.8.4, 8.1.x, 8.2.x, or 8.3.x in order to upgrade to Forcepoint DLP v8.4. If you have an earlier version, there are interim steps to perform. See [Upgrading to Forcepoint DLP v8.4.0](#).

Resolved and known issues

Release Notes | Forcepoint DLP | v8.4.0 | 31-July-2017

A list of resolved and known issues is available in the [Forcepoint Knowledge Base](#). Use the My Account link at support.forcepoint.com to log in and view the list.



Warning

Forcepoint DLP 8.4 does not include an updated version of the TRITON AP-DATA Email Gateway.

The v8.4 Forcepoint Security Manager is not backward-compatible with the v8.3 TRITON AP-DATA Email Gateway.

Customers are advised to continue managing TRITON AP-DATA Email Gateway 8.3 with the v8.3 TRITON Manager.

This does not affect customers using Forcepoint Email Security (formerly TRITON AP-EMAIL).

©2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

