Forcepoint DLP Release Notes v8.6

Release Notes | Forcepoint DLP | v8.6.0 | 30-November-2018

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 8.6.

For installation or upgrade instructions, see:

- *Installation and Upgrade*, page 10
- Forcepoint DLP Installation Guide (PDF)
- Forcepoint DLP Upgrade Guide (PDF)

New in Forcepoint DLP

Release Notes | Forcepoint DLP | v8.6.0 | 30-November-2018

DLP Cloud Applications data discovery

The Forcepoint DLP Cloud Applications license now enables data discovery and remediation of sensitive data at rest that is stored in sanctioned cloud applications. Supported cloud applications include Office 365, Box, G-Suite, Salesforce, and ServiceNow, with additional cloud applications added regularly.

DLP Cloud Applications provides complete visibility and API-based remediation controls over uploads, downloads, sharing activities, and data at rest across sanctioned cloud applications.

Existing data discovery policies and classifiers (including fingerprint and machine learning classifiers) can be extended to sanctioned cloud applications. A range of remediation actions is available, including removing sharing permissions and file quarantine (actions vary between cloud applications).

DLP Cloud Applications leverages Forcepoint CASB to apply DLP policies via a Forcepoint hosted service, ensuring that data is scanned and remediated in the cloud. Incidents and forensics are stored securely within your existing Forcepoint DLP infrastructure.

See Forcepoint DLP Administrator Help for more information about cloud discovery scans. See Configuring the CASB service in the Forcepoint DLP Administrator Help for information about configuring the Forcepoint CASB service.

Data labeling framework

Version 8.6 of Forcepoint DLP introduces a new data labeling framework with support for Microsoft Information Protection, Boldon James Classifier, and Titus labeling solutions.

Customers using Microsoft Information Protection (E3 license or higher) can import classification labels directly from the Microsoft Azure Portal into Forcepoint Security Manager and allocate labels to the new File Labeling classifier. This enables labels to be detected within DLP policy rules with a high degree of accuracy. Use of this feature requires authentication with Microsoft Office 365 administrator credentials; it is recommended to use the credentials of an administrator who has visibility over all Microsoft Information Protection labels used in the organization. The ability to apply labels and protection templates as policy actions is planned for future releases.

Forcepoint DLP Endpoint (Windows) supports automated decryption of files protected using Microsoft Rights Management to enable DLP policies to be applied to RMS protected content.

Customers using Boldon James Classifier can import classification labels created using Classifier into Forcepoint Security Manager and allocate labels to the new File Labeling classifier. This enables labels to be detected within DLP policy rules with a high degree of accuracy. It is also possible to automatically apply Boldon James Classifier labels via DLP policy actions plans for data at rest on DLP Endpoint (Windows). Additional automated labeling actions for network discovery can be configured using remediation scripts.

- See Configuring File Labeling in the Forcepoint DLP Administrator Help for more information.

OCR enhancements

Forcepoint DLP now provides a Trade Agreements Act (TAA) certified Optical Character Recognition (OCR) module. U.S. Government customers are subject to the TAA, meaning all products listed on the GSA Schedule Contract must be manufactured or “substantially transformed” in the United States or a TAA “designated country;” https://www.acquisition.gov/sites/default/files/current/far/html/52_223_226.html#wp1169151

The OCR engine also adds support for Arabic and Thai languages, and supports OCR for images embedded within Microsoft Office documents and PDFs.

- See Forcepoint DLP Administrator Help for more information.

Forcepoint One Endpoint introduction

In this release, Forcepoint One Endpoint replaces the legacy Endpoint DLP agent for Windows and macOS. During 2019, additional Forcepoint products will migrate to Forcepoint One Endpoint, providing a single unified endpoint agent for all Forcepoint security products.

In Forcepoint DLP version 8.6.0, the endpoint package builder combines Forcepoint One Endpoint for DLP (and Dynamic Data Protection) with the existing Web Direct Connect Endpoint (DCEP) and Proxy Connect Endpoint (PCEP) endpoint agents into a single package for deployment to managed endpoints. The endpoint upgrade process is the same as in previous DLP releases.

The endpoint package builder is no longer included in the Forcepoint Security Manager installer and must be downloaded from the Forcepoint One Endpoint dedicated download section on www.forcepoint.com.

Endpoint: Enhanced monitoring of browser file uploads

Version 8.6 adds a new feature that enhances the detection of sensitive data being uploaded to specified cloud applications through supported web browsers. Incidents can be generated and activities that put sensitive data at risk can be audited or blocked. This feature is supported on both Windows and Mac endpoints, and can be accessed from the detection tab on the **Settings > General > Endpoint** page.

See Forcepoint DLP Administrator Help for more information about this feature.

Endpoint: Browser extension mode configuration

In version 8.6, you can specify the mode in which Forcepoint Endpoint browser extensions operate for the Google Chrome browser.

On the **Settings > Deployment > Endpoint > Endpoint Profile** page Properties tab, select a mode for the Chrome extension:

- Enabled
- Monitoring only
- Disabled

See Endpoint profile: Properties tab for information about endpoint properties.

Endpoint: Enhanced employee coaching details

Security administrators can now decide to display additional incident detail in employee confirmation dialog boxes and the Endpoint Log Viewer. This information is designed to enable an end user to make a more informed decision about how they handle sensitive business data. This option is set in the **Settings > Deployment > Endpoint > Endpoint Profiles** page Properties tab, under Interactive Mode Options.

Forcepoint DLP Email Gateway and Forcepoint Security Manager deployment via Azure Marketplace

Forcepoint DLP Network and Forcepoint DLP Suite licenses include Forcepoint DLP Email Gateway, an enterprise-grade email Mail Transport Agent (MTA) option for network email DLP policy enforcement.

Forcepoint DLP Email Gateway can be deployed on-premises as a virtual appliance or in a public cloud environment through the Microsoft Azure Marketplace. This version adds support to deploy Forcepoint Security Manager in Azure alongside Forcepoint DLP Email Gateway, allowing your full email protection solution to reside within the Azure cloud environment. This solution will be available in the Azure Marketplace in early 2019.

The steps for installing DLP Email Gateway and Security Manager in Azure are the same as those for Forcepoint Email Security. After installation, enter your subscription key in the Security Manager to enable the options for Forcepoint DLP Email Gateway.

Refer to Forcepoint Email Security and Forcepoint DLP Email Gateway documentation for more information:

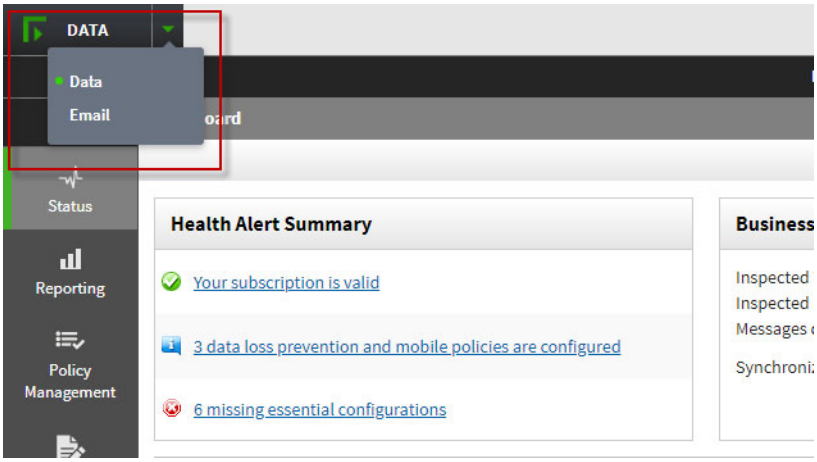
- Installing Forcepoint Email Security in Microsoft Azure
- Forcepoint DLP Email Gateway Administrator Help
- Forcepoint Email Security in Azure Quick-Start Guide

Support for installation on Red Hat 7.x

Starting with version 8.6.0, the Forcepoint DLP Analytics Engine and Protector software packages can be installed on a Red Hat 7.x operating system. See Forcepoint DLP Installation Guide for information about installing the Analytics Engine and the Protector.

Fresh banner design

The Forcepoint Security Manager banner has been slightly redesigned to provide a streamlined experience. A pull-down menu is now used to access installed product modules, as shown in the following image:



Your subscription is valid

3 data loss prevention and mobile policies are configured

6 missing essential configurations

To access the Data Security module, use the following steps:

1. At the top left of the page, hover over the **Forcepoint logo**.

   A pull-down menu displays the available modules.

2. Click **Data**.

   The Data Security module displays.

New and enhanced policies, rules, and classifiers

New policies, rules, classifiers and file types were added in this release, including:

- PII policies for Chile, Colombia, Costa Rica, Mexico, and Peru
- Private Keys policy
- Controlled Unclassified Information (CUI) policy
- Digitally Signed PDF Files policy
- Passport classifiers for China, Mexico, and the U.S.
- Social Security Number (NUSS) classifiers for Spain

- Computer-aided design (CAD) and database classifiers
- Encrypted Microsoft OneNote classifier
- Rules for Email Address and Password and for Credit files (also known as credit reports)

New

New Latin American policies, rules, and classifiers

- Added policies “Colombia PII” and “Colombia PII for Discovery” with rules for detection of ID Numbers (Cedula de Ciudadania), based on new script classifiers.
- Added policies “Peru PII” and “Peru PII for Discovery” that contain rules for Unique Identification Code (CUI), Unique Taxpayer Registration Number (RUC) of Individuals and Unique Taxpayer Registration Number (RUC) of Non-Individuals, based on new script classifiers.
- Added policies “Costa Rica PII” and “Costa Rica PII for Discovery” with rules for detection of Identification Numbers (Numero de Cedula Identidad) and Legal Identification Numbers (Numero de Cedula Juridica), based on new script classifiers.
- Added policies “Chile PII” and “Chile PII for Discovery” with rules for detection of National Identity Numbers (RUN/RUT), based on new script classifiers.
- Added policies “Mexico Finance” and “Mexico Finance for Discovery” with rules for detection of Standardized Bank Code (CLABE), based on new script classifiers.
- Added “Social Security Number (NSS)” rules to the policies “Mexico PII” and “Mexico PII for Discovery”, based on new script classifiers.

New Private Keys policy, rules, and classifiers

- Renamed policy “PKCS #12 Files” to “Private Keys” and added rules to it for detection of PKCS #1 Private Key, DSA Private Key, Elliptic Curve Private Key, Unencrypted PKCS #8 Private Key, Encrypted PKCS #8 Private Key, OpenSSH Private Key, SSH2 Private Key, PGP Private Key, Textual PPK Private Key and JSON Keystore File Private Key, based on new script classifiers. An equivalent “Private Keys for Discovery” policy was also created.

New “Controlled Unclassified Information (CUI)” policy, rules, and classifiers

- Added policy “Controlled Unclassified Information (CUI)” for detection of CUI markings, required by some US regulations, like DFARS. The policy contains rules for detection of CUI Banner Markings and Portion Marking, based on new pattern classifiers. New file type classifiers for “Unencrypted Portable Document Format (PDF)” and “Microsoft PowerPoint Binary File (Legacy)” were also created to be used by this policy.

New policies, rules, and classifier for Digitally Signed PDF Files

- Added policies “Digitally Signed PDF Files” and “Digitally Signed PDF Files for Discovery” with a rule for detection of Digitally Signed PDF Files, based on a new file type classifier.

New policy “Risk Management Framework (RMF) for Department of Defense Information Technology (IT)”

- Changed the description of the policy “DIACAP” to indicate that it was deprecated in 2014 and replaced by the Risk Management Framework (RMF) for DoD Information Technology (IT) and added a new policy by that name.

New APAC discovery policies

- Added discovery PII policies for Indonesia and Vietnam.

New passport rules and classifiers

- Added “Passport Number” and “Name and Passport Number” rules to the policies “US PII” and “US PII for Discovery”, based on new script classifiers.
- Added “Passport Number” rules to the policies “People's Republic of China PII” and “People's Republic of China PII for Discovery”, based on new script classifiers.
- Added “Passport Number” rules to the policies “Mexico PII” and “Mexico PII for Discovery”, based on new script classifiers.

New rules and classifiers for Spain

- Added “Social Security Number (NUSS)”-related rules to the policies “Spain Data Privacy Act”, “Spain PII” and “Spain PII for Discovery”, based on new script classifiers.

New computer-aided design (CAD) rules and classifiers

- Added “Abaqus ODB File”, “Autodesk Design Web File”, “Autodesk Maya Binary File”, “Autodesk Maya Textual File”, “Nastran OP2 File”, and “Siemens NX PRT File” rules to the policies “Business and Technical Drawings Files” and “Export Administration Regulations (EAR)”, based on new file type classifiers.

New database rules and classifiers

- Added “Microsoft Program Database File”, “MySQL Table Definition File”, “SAS7BDAT Database Storage File”, and “SQLite Database File” rules to the policies “Database Files” and “Database Files for Discovery”, based on new file type classifiers.

New Encrypted Microsoft OneNote rule and classifier

- Added the rule “Microsoft OneNote Encrypted File” to the policy “Encrypted Files”, based on a new file type and file type classifier, and changed Encrypted Files-related rules to include the new file type.

New rules and improved classifiers for South Africa

- Created new “Wide” rules for the policies “South Africa ECT Act”, “South Africa POPI”, and “South Africa PII For Discovery”.

- Renamed and improved the accuracy of “South African ID Number” script classifiers.

New Email Address and Password rules

- Added “Email Address and Password” rules to the data in motion and discovery policies “South Africa PII”, “Switzerland PII”, “Slovakia PII”, “Czech Republic PII”, “Brazil PII”, “Israel PII”, “India PII”, “South Korea PII”, “Macau PII”, “Sweden PII”, “New Zealand PII”, “People’s Republic of China PII”, “Thailand PII”, “Finland PII”, “Canada PII”, “US PII”, “UK PII”, “Australia PII”, “Turkey PII”, “Japan PII”, “Ireland PII”, “Germany PII”, “Netherlands PII”, “France PII”, “Denmark PII”, “Greece PII”, “Hong Kong PII”, “Taiwan PII”, “Singapore PII”, “Belgium PII”, “Norway PII”, “Mexico PII”, “Spain PII”, “Suspected Malicious Dissemination”, “Russia PII”, “Indonesia PII”, “Vietnam PII”, “Austria PII”, “Portugal PII”, “Colombia PII”, “Peru PII”, “Costa Rica PII”, and “Chile PII”.

New Credit File (also known as Credit Report) rules

- Added Credit File (AKA Credit Report) rules to the data in motion and discovery PII policies for Australia, Canada, U.K. and the U.S.

New File Types

- Added 214 new file types.

Enhanced

Improved classifiers

- Improved the efficiency of the 90 script classifiers that use the script GenericIDNumber.py.
- Replaced script classifiers for Hong Kong Address with new pattern classifiers in order to improve accuracy and efficiency.
- Replaced pattern classifier for “Health Insurance Claim Number (HICN)” with a script classifier that masks the matches.
- Improved the accuracy of script classifiers “Credit Cards: Diners” and “Credit Cards: Visa”.
- Improved the accuracy of “UK National Insurance Number” pattern classifiers.
- Improved the accuracy of script classifiers “1st Magnetic Track” and “1st Magnetic Track (Chinese cards)”.
- Improved the efficiency of “Python Source Code” script classifiers.
- Added validation algorithms for “Italian Fiscal Code” and “French INSEE Code” to the script “Customizable IDs”.
- Improved the accuracy of file type classifiers by adding detection of new file types. This was done for the classifiers “Microsoft Office File“, “Microsoft Office File - All Versions”, “Microsoft Office Files - Non-RMS-Protected “, “Microsoft Word File “, “Various Archive Formats”, “Various Computer Aided Design Formats”, “Various Database Files”, “Various Presentation Formats”, “Raster Graphics Formats”, “Various Spreadsheet Formats”, “Various Word Processing Formats”, and “Vector Graphics Formats”.

- Replaced script classifier “CAD stp text format” with new file type classifier “STP Format” in order to improve efficiency.

Renamed policies

- Replaced “Peoples Republic of China” with “People's Republic of China” in the names and descriptions of policies, rules and classifiers.
- Renamed “Private Information for Discovery” policies as “PII for Discovery” for Australia, Brazil, Denmark, Finland, France, Germany, Greece, Hong Kong, India, Ireland, Japan, Macau, Mexico, New Zealand, Norway, Poland, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, and Turkey.

Removed policies and rules

- Deleted policy “People Republic of China Private Information For Discovery”.
- Deleted “Hong Kong ID (formal form) and Common Surname” rules from policies “Hong Kong Personal Data Privacy Ordinance (Cap. 486)”, “Hong Kong PII”, and “Hong Kong PII For Discovery”.
- Deleted rule “South Africa PII: SA ID (narrow)” from policy “South Africa PII”.
- Deleted rule “Japanese Credit Cards: All Credit Cards” from the policy “Credit Card Numbers for Discovery”.

Installation and Upgrade

Release Notes | Forcepoint DLP | v8.6.0 | 30-November-2018

For installation or upgrade instructions, see:

- Forcepoint DLP Installation Guide (PDF)
- Forcepoint DLP Upgrade Guide (PDF)

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, v8.6.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.

The v8.6 Forcepoint DLP installer also installs Forcepoint Security Manager version 8.5.3

The Forcepoint Security installer can be used to install SQL Server 2017 Express SP1. This only applies to fresh installations. The SQL Express installation does not install the SQL Server Management Studio (SSMS), which can be downloaded for free from Microsoft.

Upgrading Forcepoint DLP

Your data security product must be at version 8.2.x, 8.3.x, 8.4.x, 8.5.0, 8.5.1, or 8.5.2 to upgrade to Forcepoint DLP v8.6. If you have an earlier version, there are interim steps to perform. See Upgrading to Forcepoint DLP v8.6.

Supported operating systems

This version adds support for:

- CentOS 7.5 64-bit
- SQL Server 2017 (including Express)

This version ends support for:

- Windows Server 2008 (all versions)
- SQL Server 2008 (all versions)

See the Certified Product Matrix for information about all supported platforms, including supported browsers.

Resolved and Known Issues for Forcepoint DLP

Release Notes | Forcepoint DLP | v8.6.0 | 30-November-2018

A list of resolved and known issues in this release is available to Forcepoint DLP customers.

If you are not currently logged in to the Forcepoint support website, clicking the link brings up a My Account login prompt. Log in to view the list.