v8.5.0 Release Notes for Forcepoint DLP

Release Notes | Forcepoint DLP | 29-November-2017

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 8.5.0.

Important

Version 8.5.0 is a Forcepoint DLP only release.

- Version 8.5.0 Forcepoint DLP cannot be installed with Forcepoint Web Security or Forcepoint Email Security.
- Existing Forcepoint DLP deployments that integrate with other Forcepoint products cannot be upgraded to this version and should wait for 8.5.1 that will be released at the end of February 2018.

For installation or upgrade instructions, see:

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

New in Forcepoint DLP

Release Notes | Forcepoint DLP | 29-November-2017

Version 8.5.0 offers several new features and product updates.

New Forcepoint DLP Cloud Applications powered by Forcepoint CASB

Forcepoint DLP Cloud Applications service leverages the Forcepoint CASB platform to provide complete visibility and control over sensitive data uploaded or downloaded from enterprise cloud applications, and prevents sharing of sensitive data to unauthorized users or devices. Benefits include:

- Hybrid solution which enables Forcepoint Security Manager to extend DLP policies via the Forcepoint CASB cloud hosted service
- Minimal implementation and ongoing management overhead
- DLP policy enforcement using Forcepoint CASB is included in the DLP Cloud Applications license
- Straightforward configuration which extends existing DLP policies to supported cloud services, including PreciseID fingerprinting.
- Support for one cloud platform is included in the DLP Cloud Applications license (e.g. Office 365 or G-Suite), with a modular licensing approach for adding support for additional cloud applications.
- At launch support for Microsoft Office 365, Google G-Suite, Box, and Salesforce.
- New cloud applications which are added to the service dynamically. No requirement toupgrade customer infrastructure.

The legacy DLP cloud agent (supported in DLP 8.3 and 8.4) has been replaced with the Forcepoint CASB service to enforce DLP policies in sanctioned cloud applications. Existing AP-DATA Cloud App Security customers will be automatically provided with a Forcepoint DLP Cloud Applications license for the duration of their remaining subscription.

Enable, configure, and manage the DLP Cloud Applications (CASB) service on the Settings > General > Services page in the Forcepoint Security Manager.

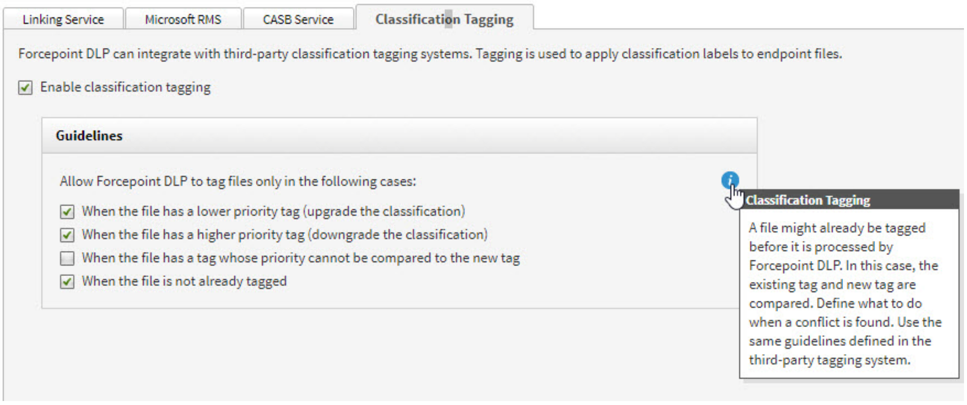
Once the DLP Cloud Applications (CASB) service is enabled and configured to work with one or more cloud applications (like OneDrive for Business or Box):

- Update the Destination tab in one or more DLP policies to include the DLP Cloud Applications (CASB) service.
- Create or update action plans to define the action that the DLP Cloud Applications (CASB) service takes in response to DLP incidents.

Support for classification tagging systems

Forcepoint DLP now includes support for the classification tagging system offered by Boldon James. With Boldon James, organizations can add metadata to files to help classify their data.

Enable classification tagging on the Settings > General > Services page in the Security Manager.



Forcepoint DLP can integrate with third-party classification tagging systems. Tagging is used to apply classification labels to endpoint files.

☑ Enable classification tagging

Guidelines

Allow Forcepoint DLP to tag files only in the following cases:

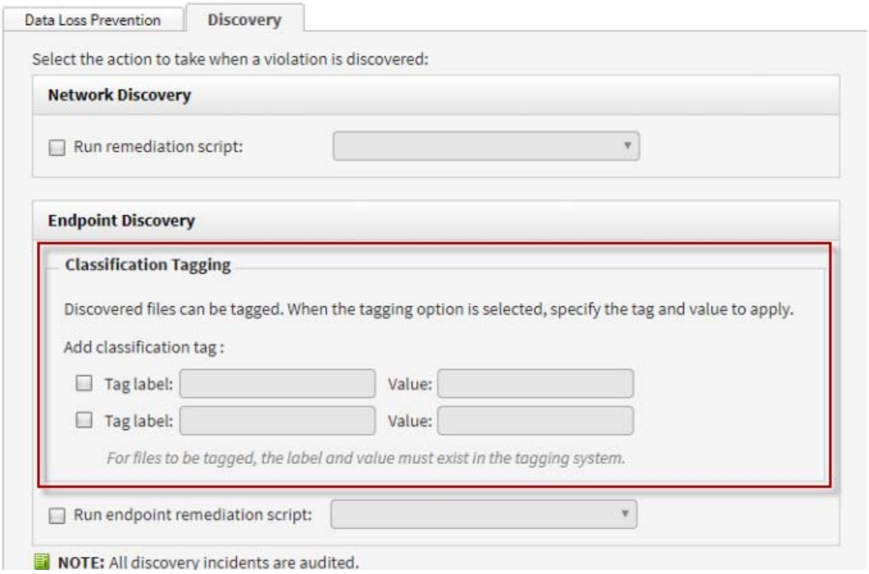
☑ When the file has a lower priority tag (upgrade the classification)
☑ When the file has a higher priority tag (downgrade the classification)
☐ When the file has a tag whose priority cannot be compared to the new tag
☑ When the file is not already tagged

Classification Tagging

A file might already be tagged before it is processed by Forcepoint DLP. In this case, the existing tag and new tag are compared. Define what to do when a conflict is found. Use the same guidelines defined in the third-party tagging system.

Also set the guidelines that determine when Forcepoint DLP adds tags to files, or updates existing tags. The guidelines refer to comparing the labels of the file before the labels are changed by tagging. During tagging, the file is compared as a whole, not per selector field. If one classification fails, neither selector is added to the file.

Once tagging is enabled and configured, create or update action plans to define up to two tags that Forcepoint Data Discovery can add to files found during the discovery process.



Select the action to take when a violation is discovered:

Network Discovery

☐ Run remediation script:

Endpoint Discovery

Classification Tagging

Discovered files can be tagged. When the tagging option is selected, specify the tag and value to apply.

Add classification tag :

☐ Tag label: Value:
☐ Tag label: Value:

For files to be tagged, the label and value must exist in the tagging system.

☐ Run endpoint remediation script:

NOTE: All discovery incidents are audited.

✓ **Note**

Support for additional data classification solutions, including Microsoft Azure Information Protection, is planned for 2018.

New and enhanced policies, rules, and classifiers

Policies, rules and classifiers were added in this release for the protection of Personally Identifiable Information (PII) and Intellectual Property (IP)

New (PII)

- Added “**CV and Resume**” policies and related policy category, classifiers, and regions:
  - Data in motion policies “CV and Resume in French”, “CV and Resume in German”, and “CV and Resume in Spanish”.
  - Discovery policies “CV and Resume in French for Discovery", "CV and Resume in German for Discovery", and "CV and Resume in Spanish for Discovery".
  - Dictionary classifiers “CV and Resume in French”, “CV and Resume in German”, and “CV and Resume in Spanish”.
  - Data in motion policy category “CV and Resume” under “EU General Data Protection Regulation (GDPR)”.
  - Related regions “Monaco”, “Liechtenstein”, “Democratic Republic of the Congo”,“ Ivory Coast”, “Cameroon”, “Colombia", "Argentina", "Peru", "Venezuela", "Chile", "Ecuador", "Guatemala", "Cuba", "Bolivia", "Dominican Republic", "Honduras", "Paraguay", "El Salvador", "Nicaragua", "Costa Rica", "Panama", and "Uruguay”.
- Added **IRS forms-related rules and classifiers**, and renamed existing classifiers –
  - Renamed policies “W-2 Forms” and “W-2 Forms for Discovery” to “IRS Tax Forms” and “IRS Tax Forms for Discovery”, respectably; added wide, default and narrow rules for detection of Form W-4, Form W-4V, Form W-4P, Form W-9, Form W-9S, Form 1040/ Form 1040A, and Form 1040EZ to said policies.
  - Added pattern classifier “SSN or TIN in an IRS Form” and dictionary classifiers “Form W-4", "Form W-4V", "Form W-4P", "Form W-9", "Form W-9S", "Form 1040/Form 1040A", and "Form 1040EZ".
  - Renamed classifiers “W2 Form Support”, “W-2 Form support terms 1”, and “W-2 Form support terms 2” to “US Social Security Number in Form W-2”, “Form W-2 Terms”, and “Form W-2 Header”, respectably.
- Added and renamed **US state regulation policies** -
  - Added data in motion policies “Alabama Information Protection", "Kentucky Data Breach Notification", "Mississippi Data Breach Notification", "Nebraska Notification of Data Security Breach Act", "New Mexico Data Breach Notification Act", "North Dakota Data Breach Notification", "Puerto Rico Data Breach Notification", "South Carolina Data

  Breach Notification", "South Dakota Medical Records Law", "Vermont Security Breach Notice Act", "West Virginia Consumer Credit and Protection Act" and "Wyoming Data Breach Notification".
  - Renamed the regulation policies of 39 US states and the District of Columbia, and updated their description.
  - Added regions “Alabama”, “Kentucky”, “Mississippi”, “Nebraska”, “New Mexico”, “North Dakota”, “Puerto Rico”, “South Carolina”, “South Dakota”, “Vermont”, “West Virginia”, and “Wyoming”.
- Added policies “**Biometric Files**” and “**Biometric Files for Discovery**” and file type classifiers "**NIEM-Conformant XML**", and "**OASIS XML Common Biometric Format (XCBF)**".
- Added policy “**Problem Gambling**” and pattern classifier “**Problem Gambling**” that detect expressions that are indicative of problem gambling.
- Added names-related dictionary classifiers “**Malaysian Name**” and “**Philippine First or Last Name**”.

New (IP)

- Added wide, default and narrow “**Email Address and Password**” rules to the policy “**Password Dissemination**”.
- Added detection of "**Encrypted RAR5 File**" and "**Encrypted B1 File**" **-**
  - Added “Encrypted RAR5 File” and "Encrypted B1 File" rules to the data in motion policy “Encrypted Files”.
  - Added detection of "Encrypted RAR5 File" and "Encrypted B1 File" to the relevant rules in the policies “Suspected Malicious Dissemination”, “Encrypted files - known format”, “Email to Competitors”, “Suspected Mail to Self”, and “Suspected Malicious Dissemination for Discovery”.
- Added file type classifiers “**Raster Graphics Formats**” and “**Vector Graphics Formats**”.
- Added policies “**Security Software Files**” and “**Security Software Files for Discover**y” and related file type classifier “Splunk Enterprise Security Event Log File”.

Enhanced

- **Improved password detection**:
  - “Password dissemination for Web traffic” rules were improved and renamed into “Password Dissemination for HTTP Traffic (Default)”, and added wide and narrow “Password Dissemination for HTTP Traffic” rules to the following policies:
    - "FDA - 21 CFR"
    - "EU finance"
    - "Arkansas Personal Information Protection Act"
    - "California Personal Information Privacy Act"
    - "Connecticut Data Breach Notification Act"
    - "Delaware Data Breach Notification"
    - "Georgia Personal Data Security Act"

  - "Illinois Personal Information Protection Act"
  - "Indiana Disclosure of Security Breach law"
  - "Massachusetts Protection of Personal Information"
  - "Nevada Security of Personal Information"
  - "New Jersey Personal Information and Privacy Protection Act"
  - "Pennsylvania Breach of Personal Information Notification Act"
  - "Utah Protection of Personal Information Act"
  - "DIACAP"
  - "FFIEC"
  - "FISMA"
  - "MITS"
  - "Ohio Data Security Breach Notification Law"
  - "District of Columbia Security Breach Notification Act"
  - "Iowa Data Breach Notification Law"
  - "Philippines PII"
  - "Oregon Consumer Identity Theft Protection Act"
  - "Alaska Personal Information Protection Act"
  - “Maryland Personal Information Protection Act"
  - "Tennessee Data Breach Notification"
  - "Missouri Breach Notification Law",
  - "Hawaii Security Breach of Personal Information"
  - "Idaho Data Breach Notification"
  - "Oklahoma Security Breach Notification Act"
  - "Rhode Island Identity Theft Protection Act"
  - "Kansas Protection of Consumer Information"
  - "Louisiana Data Breach Notification"
  - "Maine Data Breach Notification Law"
  - "Montana Data Breach Notification Statute"
  - "New Hampshire Notice of Security Breach"
  - "India IT Act"
  - "Password Dissemination"
  - "Philippines Data Privacy Act"

- “**Name and Password**” rules were improved and renamed to “Name and Password (Default)”, and wide and narrow “Name and Password” rules were added to the following policies:
  - "Connecticut Data Breach Notification Act"
  - "Delaware Data Breach Notification"
  - "Indiana Disclosure of Security Breach law"
  - "Massachusetts Protection of Personal Information"
  - "Nevada Security of Personal Information"
  - "Pennsylvania Breach of Personal Information Notification Act"
  - "Ohio Data Security Breach Notification Law"
  - "District of Columbia Security Breach Notification Act"

  - "Iowa Data Breach Notification Law"
  - "South Africa POPI"
  - "Malaysia PDPA"
  - "Oregon Consumer Identity Theft Protection Act"
  - "Alaska Personal Information Protection Act"
  - "Maryland Personal Information Protection Act"
  - "Tennessee Data Breach Notification"
  - "Missouri Breach Notification Law"
  - "Hawaii Security Breach of Personal Information"
  - "Idaho Data Breach Notification"
  - "Oklahoma Security Breach Notification Act"
  - "Rhode Island Identity Theft Protection Act"
  - "Louisiana Data Breach Notification"
  - "Kansas Protection of Consumer Information"
  - "Maine Data Breach Notification Law"
  - "Montana Data Breach Notification Statute"
  - "New Hampshire Notice of Security Breach"
  - "Singapore PDPA"
  - "India IT Act"
  - “Philippines PII for Discovery”

- “**Suspected passwords”** rules were improved and renamed to “Password Dissemination for non-HTTP/S Traffic (Default)”, and wide and narrow “Password Dissemination for non-HTTP/S Traffic” rules were added to the policies:
  - “EU finance”
  - “Arkansas Personal Information Protection Act”
  - “California Personal Information Privacy Act”
  - “Florida Information Protection Act”
  - “Georgia Personal Data Security Act”
  - “Illinois Personal Information Protection Act”
  - “New Jersey Personal Information and Privacy Protection Act”
  - “Utah Protection of Personal Information Act”
  - “DIACAP”
  - “FFIEC”
  - “FISMA”
  - “MITS”
  - “Suspected Malicious Dissemination”
  - “Password Dissemination”
  - “India IT Act”
- Improved “**SSN with possible password”** rules and renamed them to “SSN and Password (Default)”, and added wide and narrow “SSN and Password” rules to the following policies “Michigan Identity Theft Protection Act”, and “Wisconsin Data Breach Notification”.

  - Improved “**Passwords”/“Password Information”** rules and renamed them to “Password (Default)”, and added wide and narrow “Password” rules to the following policies “General Sensitive Information for Discovery”, and “Suspected Malicious Dissemination for Discovery”.
  - Replaced the pattern classifier “**Explicit Password**” with a script classifier by the same name.
  - Renamed dictionary classifier “Common salted passwords” to “Common Hashed Passwords”.”
  - Replaced the “Sofi and Account with Password” rules of the policies “Netherlands Personal Data Protection Act”, “Netherlands PII” and “Netherlands PII for Discovery”, with wide and default “Bank Account Number” rules and wide, default and narrow “Citizen Service Number and Password” rules, where there were none.
  - Replaced the pattern classifier “Explicit Password” with a script classifier by the same name.
  - Removed pattern classifiers “Password Terms” and “General Password”, dictionary classifier “Common passwords in English” and script classifiers “Passwords”, “Passwords for HTTP”, and “Passwords - keyboard sequence”.
  - Renamed dictionary classifier “Common salted passwords” to “Common Hashed Passwords”.”
- Improved the accuracy of **credit card number-related script classifiers**.
- Improved the accuracy of the script classifier “**Credit Card Magnetic Tracks**”.
- Improved the accuracy of pattern classifier “**Confidential Header/Footer**”.
- Improved the accuracy of **Australian Tax File Number (TFN)** detection –
  - Improved TFN rules in policies “Australia PII”, “Australian Privacy Act (2012 Revision)”, and “Australia Private Information For Discovery”.
  - Added “Australia PII: Tax File Number (Wide)” rules to policies “Australia PII” and “Australia Private Information for Discovery”.
  - Added rules “Name and Tax File Number (Wide)” and “Australian Privacy Act: Address and Tax File Number (Wide)” to policy “Australian Privacy Act (2012 Revision)”.
  - Added script classifiers “Australian Tax File Number (Default)” and “Australian Tax File Number Near Term”.
  - Renamed script classifier “Australian TFN” to “Australian Tax File Number (Wide)”.
- Replaced references to the name “Sofinummer” with “Dutch Citizen Service Number”.
  - Renamed script classifier “Netherlands: Sofinummer” to “Dutch Citizen Service Number”.
  - Renamed relevant rules in the policies “Netherlands Personal Data Protection Act”, “EU Directive 95/46/EC”, “Netherlands PII”, and “Netherlands PII for Discovery”.
- Renamed South Africa-related policy and classifier names and descriptions.
  - Renamed policies “SA ECT Act” and “SA POPI” to “South Africa ECT Act” and “South Africa POPI”, respectably.
  - Renamed dictionary classifier “Afrikaans first names” to “Bantu First Name”.

Removed

- The following policies and rules were removed:
  - Removed the rule “Password Dissemination: Common Passwords without term” from the policy “Password Dissemination”.
  - Removed pattern classifiers “Password Terms” and “General Password”, dictionary classifier “Common passwords in English” and script classifiers “Passwords”, “Passwords for HTTP”, and “Passwords - keyboard sequence”.
  - Removed policies “California SB1”, “California SB1386/CC1798”, “California AB 1298", and “California SB 541 and AB 211" and recreated their rules in the policy “California Personal Information Privacy Act”.
  - Removed policy “Nevada SB 227 and NRS 603A for Discovery”.
  - Removed dictionary classifier “Australian TFN Terms”.

New in Forcepoint DLP Endpoint

For information on the latest Forcepoint DLP Endpoint features, see the Forcepoint Endpoint Release Notes on the Forcepoint Documentation site.

Resolved and known issues for Forcepoint DLP

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.