Forcepoint DLP

10.0

Release Notes

Contents

Forcepoint DLP Release Notes

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 10.0.

- *New in Forcepoint DLP*
  - *Policy Management RBAC read only role*
  - *Policy Import/Export*
  - *Forcepoint ONE integration with DLP Forcepoint Security Manager*
  - Customized Endpoint pop-ups
- For installation or upgrade instructions, see:
  - *Installation and Upgrade*
  - Forcepoint DLP Installation Guide
  - Forcepoint DLP Upgrade Guide
- *Resolved and Known Issues for Forcepoint DLP*

For information on Forcepoint DLP Endpoint compatibility, see the latest Forcepoint F1E Release Notes.

Related concepts

New and Changed Features

Feature	Short description
Forcepoint ONE integration with Forcepoint DLP	This release contains support for the Forcepoint Security Manager unified policy to be applied to the Forcepoint ONE Web and CASB channels in addition to the Endpoint and Email channels. **Note** This feature requires the upcoming Forcepoint ONE release.
Policy Management RBAC read only role	Addition of a new read-only role to the Role Based Access Control functionality. This feature allows customers to segregate roles and responsibilities in the Forcepoint Security Manager into users that can modify policies and rules, users that can only view policies and rules and users that are restricted from viewing policies and roles.
Customized Endpoint pop-ups	Options have been added to support the customization of the coaching dialogs. This feature requires the upcoming Endpoint release.
Inline Proxy support	Options have been added to support the configuration of the Endpoint inline proxy capability. This feature requires the upcoming Endpoint release.
Policy Import/Export	This feature allows the user to export and import the policies. This feature can be used to transfer policies from one Forcepoint Security Manager to another.
Deploy API	This feature adds the deploy capability to the Export and Import API released in 9.0 enabling the user to apply changes after an import.
Update of the common diseases list	Update of the Common Diseases list to cover various Covid strains and other information.
EDM Scaling	This feature greatly increases the limit on the maximum number of cells that can be fingerprinted and the performance of fingerprint detection. The limit depends on the amount and type of data being fingerprinted. **Note** This feature requires *EDM standalone fingerprinting tool* that is available only on demand.

> **Related concepts**

New in Forcepoint DLP

This section explains the updates made in Forcepoint DLP version 10.0.

Policy Management RBAC read only role

The read-only mode allows the admin to configure certain roles to be read-only.

This is useful for an auditor role or similar roles where the user needs access to the policy, but they should not have the ability to change it whether deliberately or inadvertently.

Roles can be configured for:

- Users to modify policies and rules.
- Users that can only view policies and rules.
- Users that are restricted from viewing policies and roles.

Policy Import/Export

The Policy Import Export capability allows the customers to transfer DLP and Discovery policies from one Forcepoint Security Manager to another Forcepoint Security Manager.

This is especially useful after developing policy in test environments and copying those to production.

Forcepoint ONE integration with Forcepoint DLP

Integration of the Forcepoint DLP with Forcepoint ONE enhances Forcepoint ONE with the ability to have the unified Forcepoint Security Manager DLP policy applied to the Web and CASB channels when it is used with the corresponding Forcepoint ONE release.

Previously, Forcepoint ONE used a restricted list of the most useful classifiers, but with this release the customer is enabled with the below features:

1) The ability to have the unified policy applied across all channels. This means that the same policy covers Endpoint, Email, Forcepoint ONE Web, Forcepoint ONE CASB.

2) The Forcepoint Security Manager allows access to all the Forcepoint Classifiers to give both broader and deeper control to the customer.

The extra support added to the Forcepoint Security Manager is to enable and align Web Categories.

> **Note**
>
> a new Forcepoint ONE release is required for this feature.

Customized Endpoint pop-ups

With the corresponding Endpoint release (v23.03 or later), the administrator can add their custom logo, customized text and a URL to the coaching dialog.

This is useful so the customer end-users see the logo and understand that the message in the coaching dialog is coming from their organization's policy. Additionally, the text can explain the reason for the block, and when required, the URL can take them to an in-house site for more information or possibly translations of the message.

New and updated policies and classifiers

Updated policies

- France PII
- Romania PII
- Romania PII for Discovery

New rules

- Australian Privacy Act (2012 Revision):
    - Australian Privacy Act: Address and ABN (Wide)
    - Australian Privacy Act: Address and ABN (Default)
- Romania PII
    - Romania PII: Personal numeric code (Wide)
    - Romania PII: Personal numeric code (Default)
- France PII
    - France PII: Passport Number (Wide)
    - France PII: Passport Number (Default)
- Romania PII for Discovery
    - Romania PII: Personal numeric code (Wide)
    - Romania PII: Personal numeric code (Default)

Updated rules

- Australian Privacy Act (2012 Revision):
  - Australian Privacy Act: Name and ABN (Wide)
  - Australian Privacy Act: Name and ABN (Default)
- California Consumer Privacy Act:
  - California Consumer Privacy Act: Name and Address
- California Consumer Privacy Act (CCPA) for Discovery:
  - California Consumer Privacy Act: Name and Address (Wide)
  - California Consumer Privacy Act: Name and Address (Default)
- South Korea PII:
  - South Korea PII: ID Number (Wide)
  - South Korea PII: ID Number (Default)
- South Korea PII for Discovery:
  - South Korea PII: ID Number
- Spain Data Privacy Act:
  - Spain DPA: DNI and Credit Card Number
  - Spain DPA: DNI, Account Number and Password
- Spain PII:
  - Spain PII: DNI and Credit Card Number
  - Spain PII: DNI, Account and Password
- Spain PII for Discovery:
  - Spain PII: DNI and Credit Card Number
  - Spain PII: DNI, Account and Password
- Thailand Official Information Act:
  - Thailand Official Information Act: National ID (Wide)
  - Thailand Official Information Act: National ID (Default)
- Thailand PII:
  - Thailand PII: National ID Number (Wide)
  - Thailand PII: National ID Number (Default)
- Thailand PII for Discovery:
  - Thailand PII: National ID Number
- US PII:
  - US PII: Name and Address
- US PII for Discovery:
  - US PII: Name and Address (Wide)
  - US PII: Name and Address (Default)

Deleted rules

- Australian Privacy Act (2012 Revision):
  - Australian Privacy Act: ABN and Address (Wide)

- Australian Privacy Act: ABN and Address (Default)
- Romania PII:
  - Romania PII: Personal numeric code
- Romania PII for Discovery:
  - Romania PII: Personal numeric code
- South Korea PII:
  - South Korea PII: ID Number (With Proximity)

New classifiers

It lists the new classifiers.

Script classifiers

- Australian Business Number (Wide)
- Australian Business Number (Default)
- Australian Business Number Near Terms
- French Passport Near Terms
- Romanian ID Number (Wide)
- Romanian ID Number (Default)
- Romanian ID Number Near Terms
- South Korean ID Number (Wide)
- South Korean ID Number (Default)
- South Korean ID Number Near Terms
- Thai ID Number (Wide)
- Thai ID Number (Default)
- Thai ID Number Near Terms

Pattern classifiers

- French Passport (Wide)

Enhanced classifiers

It lists the enhanced classifiers.

Script classifiers:

- US SSN - Wide Minus Default
- US SSN (Audit)
- US SSN (Default)
- US SSN (Narrow)
- US SSN (Wide)

- US SSN: not-masked

Dictionary classifiers

- Common Medical Conditions (English)
- US Sensitive Diseases

Deleted classifiers

It gives information about the deleted classifiers.

Script classifiers:

- Romania - ID
- South Korea ID
- South Korea ID - Wide
- Thailand ID number (Default)
- Thailand ID number (Wide)

Dictionary classifiers

- Thailand ID Terms

Installation and Upgrade

For installation or upgrade instructions, see:

- Forcepoint DLP Installation Guide
- Forcepoint DLP Upgrade Guide

Operating system and hardware requirements

For the operating system and hardware requirements of Forcepoint DLP modules, see the Deployment and Installation Center.

For a step-by step guide to installing Forcepoint DLP, see the Forcepoint DLP Installation Guide.

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 version 10.0 Forcepoint DLP installer also installs Forcepoint Security Manager version 10.0, Forcepoint Email Security version 8.5.5, and Forcepoint Web Security version 8.5.5.

Upgrading Forcepoint DLP

Your data security product must be at version 8.8.x or higher to upgrade to Forcepoint DLP version 10.0. If you have an earlier version, there are interim steps to perform. See Upgrading to Forcepoint DLP 10.0

> ⚠️ **Important**
>
> Customers upgrading to Forcepoint DLP 10.0 from any version earlier than 8.8.1 that supports DLP Cloud Applications must connect to Data Protection Service to support the DLP Cloud Proxy, DLP Cloud API, and Cloud Data Discovery channels. To connect to Data Protection Service, request a JSON file with tenant information from Forcepoint Support. If your Data Security Manager is already connected to Data Protection Service, you do not need a new file or any additional action. For more information, see *Configuring Data Protection Service* in the Forcepoint DLP Administrator Guide.

Supported operating systems

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

IPv6 support in Forcepoint DLP

Forcepoint DLP supports IPv6 in the following use cases:

1) Endpoint fully supports IPv6 addressing.

2) Web Proxy supports scanning IPv6 addressed web traffic.

3) UI support for IPv6 addressing in reporting.

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 Customer Hub login prompt. Log in to view the list.

Limitation

- MIP decryption is not supported in Multi-user environments.