# Forcepoint DLP

9.0

## Forcepoint DLP Release Notes

Revision A

**Contents**

# Forcepoint DLP Release Notes

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 9.0.

- *New in Forcepoint DLP*
  - *REST API – Policy Management*
  - *Enforce DLP policies according to Dynamic User Protection's user's risk level on cloud channels*
  - *Forcepoint Security Manager certified for deploying on Google Cloud Platform*
  - Monitor traffic while endpoint is in bypass (in conduction with F1E 22.06)
- 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 in Forcepoint DLP on page 4
REST API – Policy Management on page 4
Enforce DLP policies according to Dynamic User Protection's user's risk level on cloud channels on page 4
Forcepoint Security Manager certified for deploying on Google Cloud Platform on page 4
New and updated policies and classifiers on page 5
Installation and Upgrade on page 7
Resolved and Known Issues for Forcepoint DLP on page 8

# New and Changed Features

| Feature | Short description |
|---|---|
| Forcepoint Security Manager UI refresh | DLP module now looks better than ever, with a new login page, new colors and new icons for a better experience. |
| Policy Management REST APIs | Control your Forcepoint Security Manager policies using REST APIs, including importing and exporting policies from your development and UAT environments to production, move risky users and groups between policies, disable/enable policies and much more. See below for more information. |
| Get Incident Management REST API pull historical actions | Get Incident Management REST APIs now pull historical actions performed on incidents, such as “Change Status” or comments added by administrators. |
| Enforce DLP policies according to user’s risk level on cloud channels | Risk Adaptive Protection by DLP integrated with Dynamic User Protection allows to enforce the DLP policies on cloud channels according to user risk level. See, *Enforce DLP policies according to Dynamic User Protection’s user’s risk level on cloud channels* section for more information |
| RBAC - Hide source or destination | The option to hide source and destination for Administrator Role is split into two separate permissions: Hide source and Hide destination. |
| Forcepoint DLP in Google Cloud Platform | Forcepoint Security Manager and Secondary Server has been certified for deploying on Google Cloud Platform. For more information, see the Installing Forcepoint DLP Google Cloud Platform in the Forcepoint DLP Installation Guide.<br>**Note**<br>SW Protector is not certified on GCP. |
| Procedure to harden DLP components to AES256 | Customers can now force Forcepoint Security Manager, Supplemental Servers, Protector and Analytic Engine to use AES256, the procedure is available in the following Knowledge Base article How to disable AES128 ciphers on servers. |
| Monitor traffic while Endpoint in bypass mode | Now DLP Administrator can configure endpoints to monitor traffic while in bypass, based on endpoint profile.<br>Available in conduction with F1E 22.06 |
| New Classifiers | New, removed, and improved classifiers are listed in *New and updated policies and classifiers*. For more information refer below section. |

**Related concepts**

New and updated policies and classifiers on page 5

Enforce DLP policies according to Dynamic User Protection's user's risk level on cloud channels on page 4

# New in Forcepoint DLP

This section explains the updates made in Forcepoint DLP version 9.0.

## REST API – Policy Management

The REST API service allows customers to remotely pull and manage DLP and Discovery policies from Forcepoint Security Manager to integrate with SOAR, SIEM, BI and other solutions. Use this powerful APIs to import and export policies from your development and UAT environments to production, move risky users and groups between policies, disable/enable policies and more.

For more information about REST API service, see the Forcepoint DLP REST API Guide.

## Enforce DLP policies according to Dynamic User Protection's user's risk level on cloud channels

When a user uploads sensitive data over a web browser (web traffic) or sends an email on his own device, and access remotely to company's cloud applications like OneDrive or SharePoint, the transaction can be enforced according to the user's risk level and DLP policies.

Customers who purchase Dynamic User Protection license with one of the available cloud products: DLP for Cloud Email, DLP Cloud Application, Forcepoint Web Security – Hybrid or Cloud deployments with Data Protection Service, can enforce DLP policies according to user risk level on cloud channels: Web, Email and DLP Cloud Applications channels (i.e., DLP Cloud API and Proxy).

**Note**

The customers using the older DLP version which is connected to Data Protection Service can also enjoy the benefit of this feature.

## Forcepoint Security Manager certified for deploying on Google Cloud Platform

In this release, Forcepoint Security Manager and Secondary Server have been certified for deploying on Google Cloud Platform (GCP) in addition to Azure and AWS which are already supported in previous versions. For more information, see the Installing Forcepoint DLP in Google Cloud Platform in the Forcepoint DLP Installation Guide.

# New and updated policies and classifiers

**Related concepts**

Updated rules on page 5

New classifiers on page 6

Enhanced classifiers on page 7

Deleted classifiers on page 7

## Updated rules

- California Consumer Privacy Act:
  - California Consumer Privacy Act: Name and Address
- California Consumer Privacy Act for Discovery:
  - California Consumer Privacy Act: Name and Address (Wide)
  - California Consumer Privacy Act: Name and Address (Default)
- Children's Online Privacy Protection Act (COPPA):
  - COPPA: PII of Children (Default)
  - COPPA: PII of Children (Wide)
- Email to Competitors:
  - Contact Information to Competitors
- GLBA:
  - GLBA: Name and Contact Information
- HIPAA:
  - HIPAA: Name and Contact Information
- Japan PII:
  - Japan PII: Email Address
- Japan PIP:
  - JPIP: E-mail Addresses
- PIPEDA:
  - PIPEDA: DOB and Address or SIN or Name
  - PIPEDA: SIN and Address or DOB or Name
- Russia PII:
  - Russia PII: Russian Unified Classifier of Enterprises and Organizations (Default)
- Spain PII:
  - Spain PII: DNI and Credit Card Number
  - Spain PII: DNI and Crime
  - Spain PII: DNI and Disease
  - Spain PII: DNI and Ethnicity
  - Spain PII: DNI, Account and Password
  - Spain PII: Name and DNI
- Spain PII for Discovery:

  - Spain PII: DNI and Credit Card Number
  - Spain PII: DNI and Crime
  - Spain PII: DNI and Diseases
  - Spain PII: DNI and Ethnicity
  - Spain PII: DNI Number
  - Spain PII: DNI, Account and Password
  - Spain PII: Name and DNI
- Spain Data Privacy Act:
  - Spain DPA: DNI and Credit Card Number
  - Spain DPA: DNI and Crime
  - Spain DPA: DNI and Disease
  - Spain DPA: DNI and Ethnicity
  - Spain DPA: DNI, Account Number and Password
- US PII:
  - US PII: Name and Address
- US PII for Discovery:
  - US PII: Name and Address (Default)
  - US PII: Name and Address (Wide)
- 401(k) and 403(b) forms:
  - 401(k) form (Narrow)
  - 403(b) form (Narrow)

# New classifiers

It lists the new classifiers.

## Script classifiers

- South Korean ID Number (Wide)
- South Korean ID Number (Default)
- South Korean ID Number Near Terms
- US Address (Wide)
- US Address (Default
- Spanish DNI Number (Wide)
- Spanish DNI Number (Default)
- Spanish DNI Number Near Terms

## Enhanced classifiers

It lists the enhanced classifiers.

### Script classifiers:

- Brazilian CPF Number (Wide)
- Japan Emails
- Singaporean ID Number Near Terms

## Deleted classifiers

It gives information about the deleted classifiers.

### Script classifiers:

- Spain: DNI Number
- Spain: DNI Number (Wide)
- US Address

# 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 9.0 Forcepoint DLP installer also installs Forcepoint Security Manager version 9.0, 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 8.7.x or higher to upgrade to Forcepoint DLP version 9.0. If you have an earlier version, there are interim steps to perform. See Upgrading to Forcepoint DLP 9.0

⚠ **Important**

Customers upgrading to Forcepoint DLP 9.0 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.

# 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.

Published 20 October 2022