Forcepoint DLP v8.8 Release Notes

Release Notes | Forcepoint DLP | v8.8 | 27-September-2020

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 8.8.

For information on Forcepoint One Endpoint DLP agent compatibility, see the latest Forcepoint One Endpoint release notes.

Summary of new and changed features

Feature	Short description
Integration with Forcepoint Web Security Cloud and Cloud Security Gateway	Extends DLP policy enforcement to the Forcepoint Secure Web Gateway (SWG) cloud proxy.
Forcepoint Dynamic User Protection integration	Dynamic User Protection integration to provide risk-adaptive data loss protection policies.
Expanded proprietary source code detection	New source code classifiers for the Swift and Kotlin programming languages commonly used in mobile application development.
Taiwan PII and PIPA rules and classifiers	New classifiers and rules for Taiwanese Personally Identifiable Information (PII) and Taiwanese Personal Information Protection Act (PIPA) policies for Taiwanese passport and phone numbers.

Feature and platform support deprecation

Feature	Short description
Microsoft Active Directory Rights Management Services decryption	On-premises Active Directory Rights Management Services (AD RMS) is no longer supported. From DLP 8.8 onwards, only Azure Rights Management (Azure RMS) is supported.

New in Forcepoint DLP

Release Notes | Forcepoint DLP | v8.8 | 27-September-2020

Integration with Forcepoint Web Security Cloud and Cloud Security Gateway

Visibility and control over sensitive data flowing into unsanctioned and sanctioned cloud applications

Forcepoint Cloud Security Gateway provides Secure Web Gateway and CASB functionality. Customers licensed for Cloud Security Gateway or Forcepoint Web Security DLP Add-On (Cloud) can extend their existing enterprise DLP policies to web traffic analyzed and protected through the Forcepoint cloud proxy infrastructure. This includes support for advanced data classification technologies, such as structured and unstructured data fingerprinting and the use of web categories to build targeted DLP policies and enrich incident records.

This integration complements the existing integration with Forcepoint DLP Cloud Applications (DLP Cloud API) and Forcepoint CASB (DLP Cloud Proxy) to:

- Migrate DLP policies from Forcepoint Web Security (on-premises) to Forcepoint Web Security (cloud).
- Detect and prevent sensitive data loss via consumer and unsanctioned cloud applications.
- Detect and prevent sensitive data loss via sanctioned enterprise cloud applications.

✓ **Note**

Existing customers upgrading to Forcepoint DLP 8.8 and adding a Forcepoint Web Security DLP Add-On (Cloud) license should read this article prior to upgrading.

Dynamic User Protection integration providing Risk-Adaptive DLP

The new Dynamic User Protection solution combines a lightweight endpoint agent, user behavior analytics system, entity risk scoring, and a streamlined investigation dashboard to enables data protection analysts to quickly identify and investigate high-risk user activity.

Forcepoint DLP 8.8 integrates with Forcepoint Dynamic User Protection to enable DLP policies on the endpoint to apply different action plans based on a user's analytics-calculated risk level. For example, a low-risk user might have a file upload allowed and audited, while a medium-risk user is prompted by a coaching dialog, and a high-risk user receives a block action and notification.

Deployment is simplified via a combined agent package builder and a single Forcepoint solution system tray icon.

Risk-Adaptive Protection is also still available with Forcepoint Behavioral Analytics.

New and updated policies and classifiers

New rules and classifiers have been added to:

- Taiwan Personally Identifiable Information (PII):
  - Taiwan PII: Machine Readable Passport Number (Wide)
  - Taiwan PII: Machine Readable Passport Number (Default)
  - Taiwan PII: Passport Number (Wide)
  - Taiwan PII: Passport Number (Default)
- Taiwan Personally Identifiable Information (PII) for Discovery):
  - Taiwan PII for Discovery: Machine Readable Passport Number (Wide)
  - Taiwan PII for Discovery: Machine Readable Passport Number (Default)
  - Taiwan PII for Discovery: Passport Number (Wide)
  - Taiwan PII for Discovery: Passport Number (Default)
- Taiwan Personal Information Protection Act (PIPA) policy:
  - Taiwan PIPA: Machine Readable Passport Number (Default)
  - Taiwan PIPA: Passport Number (Wide)
  - Taiwan PIPA: Passport Number (Default)

Deleted predefined policy and rules:

- EU Directive 95/46/EC
  - EU Directive 95/46/EC: Dutch Citizen Service Number and CCN
  - EU Directive 95/46/EC: Italian Codice Fiscale Number and CCN
  - EU Directive 95/46/EC: Norwegian Personal Number and CCN
  - EU Directive 95/46/EC: Spanish DNI Number and CCN
  - EU Directive 95/46/EC: Swiss New Format AHV and CCN
  - EU Directive 95/46/EC: Swiss Old Format AHV and CCN
  - EU Directive 95/46/EC: UK National Insurance Number and CCN

New source code classifiers include:

- C++ Source Code (Wide)
- C++ Source Code (Default)
- Kotlin Source Code (Wide)
- Kotlin Source Code (Wide)
- Swift Source Code (Default)
- Swift Source Code (Default)

Installation and Upgrade

Release Notes | Forcepoint DLP | v8.8 |27-September2020

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,.

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 v8.8 Forcepoint DLP installer also installs Forcepoint Security Manager version 8.5.6, Forcepoint Email Security version 8.5.4, and Forcepoint Web Security version 8.5.4.

Upgrading Forcepoint DLP

Your data security product must be at version 8.5.0 or higher to upgrade to Forcepoint DLP v8.8. If you have an earlier version, there are interim steps to perform. See Upgrading to Forcepoint DLP v8.8.

Important

Customers upgrading from Forcepoint DLP 8.7.1 or 8.7.2 and reconnecting to DLP Cloud Proxy must request a new unique Data Protection Service (DPS) JSON file from Forcepoint technical support in order to successfully connect to the DLP Cloud Proxy post-upgrade. See "Configuring Data Protection Service" in the Forcepoint DLP Administrator Guide on page 386.

Supported operating systems

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 | v8.8 | 27-September-2020

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.