Forcepoint DLP Release Notes v8.7.1

Release Notes | Forcepoint DLP | v8.7.1 | 5-March-2020

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 8.7.1.

For installation or upgrade instructions, see:

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

Summary of new and changed features

- Forcepoint DLP:

Feature	Short description
Integration with Forcepoint CASB Cloud Proxy Gateways	Extend data in motion DLP policies to sanctioned cloud applications for realtime inline policy enforcement.
Windows Server 2019 support	Forcepoint DLP management servers are now supported on Windows Server 2019.
SQL Server 2019 support	Forcepoint DLP management servers are now supported on SQL Server 2019.
Dell appliance hardware V5KG4R2 support	Protector and mobile agent appliances are supported.
CCPA policy set added to policy library	A new policy category has been added to the policy library for the California Consumer Privacy Act (CCPA).
Incident report UI enhancements	A larger number of incidents (500) can be viewed in the incident report table.

- Forcepoint One Endpoint (DLP):

Feature	Short description
macOS 10.15 (Catalina) support	Support for the latest macOS version. Added in F1E 19.10.
Edge Chromium browser support	Support for new Microsoft Edge Chromium browser. Added in F1E 20.02.
Enhanced VMware Horizon support, including support for non-persistent deployments.	VMware Horizon 7.9 support. Added in F1E 20.02.
Enhanced Citrix VDI platform support	Citrix XenApp v7.15 LTSR and Citrix Virtual Apps v7 1906 support with employee coaching. Added in F1E 19.08.

- Planned feature and platform support depreciation:

Feature	Short description
Mobile Agent	DLP 8.7.1 is the last release to support Mobile Agent for on-premises Exchange ActiveSync.
Data discovery for Box using on-premises crawlers	DLP 8.7.1 is the last release to support data discovery for Box using on-premises data crawlers. From Forcepoint DLP 8.7.2 onwards, data discovery for Box will only be supported in the cloud and will require a DLP Cloud Applications license. Support for scanning of both SharePoint Online and Exchange Online using DLP secondary servers will continue.

For more information on Forcepoint One Endpoint DLP enhancements, refer to the following documents:

- Forcepoint One Endpoint v19.08 Release Notes
- Forcepoint One Endpoint v19.10 Release Notes
- Forcepoint One Endpoint v.20.02 Release Notes

New in Forcepoint DLP

Release Notes | Forcepoint DLP | v8.7.1 | 5-March-2020

Apply DLP policies to Forcepoint CASB inline proxy gateways

To audit and control sensitive data uploads and downloads in real time

Customers licensed for Forcepoint DLP Cloud Applications and Forcepoint CASB can now extend their existing Forcepoint DLP data in motion policies to cloud-based Forcepoint CASB, in order to implement realtime inline policy enforcement for sensitive data uploads and downloads to and from sanctioned cloud applications.

This new integration complements the existing DLP Cloud API functionality, already included in the Forcepoint DLP Cloud Applications license, which provides near-realtime visibility into cloud application operations (upload, download, sharing) and cloud data discovery (also known as data at rest).

For sanctioned cloud applications that connect to Forcepoint CASB through a proxy connection, this option provides immediate inline protection through realtime DLP monitoring of operations and content moving to or from the cloud, with realtime enforcement, such as blocking.

To this end, in Forcepoint DLP 8.7.1, a new resource type is available, Cloud Application. This means that rules and action plans can be configured to apply to specific applications, such as Office 365.

The following functions and features of Forcepoint DLP 8.7.1 are part of this integration:

- New resource type: Cloud Application.
- Import of cloud applications that support cloud proxy connections from Forcepoint CASB.
- New rule configuration for specific cloud applications.
- New action plan configuration: Users can now configure specific action per user-monitored operation in DLP Cloud Proxy channel.
- In incident reports, it is now possible to filter by operation for DLP Cloud Proxy channel.

See the DLP-CASB Integration Guide for more information on this feature and its operations.

Important

Fingerprint classifiers (structured and unstructured) are not initially supported for the new DLP Cloud Proxy channel in Forcepoint DLP 8.7.1. All other classifier types are supported. Fingerprinting support will be included in Forcepoint DLP 8.7.1 R2 which is planned for release in Q2 2020. Please take this into consideration when planning production deployments.

New and updated policies and classifiers

- A new policy has been added: California Consumer Privacy Act (CCPA) for Discovery. The rules included in this policy are:
  - California Consumer Privacy Act: California Driver License and Sensitive Disease or Drug
  - California Consumer Privacy Act: CCN (Default)
  - California Consumer Privacy Act: CCN (Narrow)
  - California Consumer Privacy Act: CCN and California Driver License Number
  - California Consumer Privacy Act: CCN and Sensitive Disease or Drug
  - California Consumer Privacy Act: Celebrity Name and Sensitive Disease or Drug
  - California Consumer Privacy Act: Celebrity Name and Common Medical Condition
  - California Consumer Privacy Act: CCN and Common Medical Condition
  - California Consumer Privacy Act: DNA Profile
  - California Consumer Privacy Act: ICD9 Code and Name
  - California Consumer Privacy Act: ICD9 Description and Name
  - California Consumer Privacy Act: ICD10 Code and Name
  - California Consumer Privacy Act: ICD10 Description and Name
  - California Consumer Privacy Act: Name and Common Medical Condition (Default)
  - California Consumer Privacy Act: Name and Common Medical Condition (Narrow)
  - California Consumer Privacy Act: Name and HICN
  - California Consumer Privacy Act: Name and Sensitive Disease or Drug (Default)
  - California Consumer Privacy Act: Name and Sensitive Disease or Drug (Narrow)
  - California Consumer Privacy Act: SSN
  - California Consumer Privacy Act: SSN and Common Medical Condition
  - California Consumer Privacy Act: SSN and Sensitive Disease or Drug
  - California Consumer Privacy Act: SSN and California Driver License Number
  - California Consumer Privacy Act: SSN and CCN
  - California Consumer Privacy Act: Name and MBI (Default)
  - California Consumer Privacy Act: Name and MBI (Wide)
- The California Consumer Privacy Act (CCPA) predefined Data Loss Prevention policy has been updated with enhanced search capabilities. Several rules have been removed:
  - California Consumer Privacy Act: Password Dissemination for HTTP Traffic (Default)
  - California Consumer Privacy Act: Password Dissemination for HTTP Traffic (Narrow)
  - California Consumer Privacy Act: Password Dissemination for HTTP Traffic (Wide)
  - California Consumer Privacy Act: Password Dissemination for non-HTTP/S Traffic (Default)
  - California Consumer Privacy Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

- California Consumer Privacy Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- California Consumer Privacy Act: 10-Digit Account Number
- California Consumer Privacy Act: 5-8-Digit Account Number
- California Consumer Privacy Act: 9-Digit Account Number

Updated documentation on supported file types

A new Forcepoint DLP document listing all types of file support is now available on the support site. The document lists all file types that DLP can detect, as well as those that support content extraction or metadata extraction.

For more details, see Forcepoint DLP File Support and Size Limits.

Installation and Upgrade

Release Notes | Forcepoint DLP | v8.7.1 | 5-March-2020

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, v8.7.1.

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 v8.7.1 Forcepoint DLP installer also installs Forcepoint Security Manager version 8.5.4, Forcepoint Email Security version 8.5.3, and Forcepoint Web Security version 8.5.3.

Upgrading Forcepoint DLP

Your data security product must be at version 8.4.x, 8.5.0, 8.5.1, 8.5.2, 8.6.x or 8.7 to upgrade to Forcepoint DLP v8.7.1. If you have an earlier version, there are interim steps to perform. See Upgrading to Forcepoint DLP v8.7.1.

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 | v8.7.1 | 5-March-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.