



Forcepoint DLP

10.3

Release Notes

Contents

- [Forcepoint DLP Release Notes on page 2](#)
- [New in Forcepoint Security Manager on page 3](#)
- [New in Forcepoint DLP on page 3](#)
- [Feature updates in Forcepoint DLP on page 4](#)
- [Feature Deprecation on page 5](#)
- [New and updated policies and classifiers on page 6](#)
- [Installation and Upgrade on page 9](#)
- [Resolved and Known Issues for Forcepoint DLP on page 11](#)
- [Limitation on page 11](#)

Forcepoint DLP Release Notes

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 10.3.

- **New in Forcepoint Security Manager**
 - [Smart Search Feature](#)
- **New in Forcepoint DLP**
 - [MIP Decryption for Network Email and Network Web channels](#)
 - [Improved the controls of sensitivity level for file fingerprinting](#)
 - [Endpoint Profile Settings: Custom Configuration](#)
 - [Source manager place holder for notification's email body](#)
 - [Kerberos support](#)
- **Feature updates in Forcepoint DLP**
 - [Endpoint Settings: Excluded Domains for SSL Decryption by Endpoint Inline Proxy](#)
 - [Endpoint Profile Settings: Domains for JavaScript Injection by inline proxy](#)
 - [Securing Administrator Account: Account lockout after multiple failed attempts](#)
 - [Enhanced auditing of administrator actions](#)
- For installation or upgrade instructions, see:
 - [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](#).

New in Forcepoint Security Manager

This section highlights the new features introduced in the Forcepoint Security Manager version 10.3.

Smart Search

This feature is designed to:

- Provide answers powered by generative artificial intelligence (GenAI) to the search query based on the official Customer Hub content.
- Provide regular search results with links to various knowledge articles, documentation, and other content from Customer Hub.

For more information, see the [Forcepoint Security Manager Help](#).

New in Forcepoint DLP

This section highlights the new features introduced in the Forcepoint DLP version 10.3.

MIP Decryption for Network Email and Network Web channels

Forcepoint DLP integrates with Microsoft Information Protection (MIP), by decrypting the MIP-encrypted files and enforcing DLP policies.

In this release, the Network Email and Network Web channels are supported for MIP Decryption based on the Protector Red Hat Enterprise Linux 8 deployment method.



Note

Currently, this feature is not supported by Web Content Gateway, Email Security Gateway, and DLP Protector on CentOS.

Improved the controls of sensitivity level for File Fingerprinting

Customers can now adjust the sensitivity level for file fingerprinting directly from the Condition tab of the Policy rule wizard.

For more information, see the [Fingerprint classifiers](#) section in the Forcepoint DLP Administrator Help.

Endpoint Profile Settings: Custom Configuration

The custom configuration allows administrators to broaden the existing configuration capabilities in endpoint profiles for future F1E usage (Stay tuned for further announcements regarding F1E custom configuration).



Note

This feature is supported with F1E v24.11 and higher.

Source manager place holder for notification's email body

Now, the DLP administrator can add the source's manager to the emails' body for policy breach notifications. This allows for a more direct and efficient communication channel when addressing such breaches.

For more information, see the [Forcepoint DLP Administrator Help](#).

Kerberos support

For customers interested in implementing Kerberos authentication for their Forcepoint DLP's SQL connection, detailed instructions are available in the [Forcepoint Security Manager with Kerberos authentication](#) knowledge base Article.

Feature updates in Forcepoint DLP

This section explains the updates made in Forcepoint DLP version 10.3

Endpoint Settings: Excluded Domains for SSL Decryption by Endpoint Inline Proxy

This feature enables the administrator to manage the list of domains that will be excluded from SSL decryption done by Endpoint Inline Proxy.

In this release, the maximum limit for URL is increased to 6000. The updated maximum limit is supported with F1E v24.11 and higher.

For more information, see the [Endpoint settings: the Advanced](#) tab section in Forcepoint DLP Administrator Help

Endpoint Profile Settings: Domains for JavaScript Injection by inline proxy

This feature enables the administrator to manage the list of domains that are included or excluded from JavaScript Injection configuration.

In this release, the maximum limit for URL entries is increased to 6,000. Additionally, an option to manage the included domains list has been introduced. The updates are supported with F1E v24.11 and higher.

For more information, see [Endpoint profile: Properties tab](#) section in Forcepoint DLP Administrator Help.

Securing Administrator Account: Account lockout after multiple failed attempts

From Forcepoint DLP v10.3, when an administrator attempting to login fails for 'X' times (default value is set to 6) in an interval of 'Z' seconds (default value set to 30 seconds), the Forcepoint Security Manager will automatically lock the admin account for 'Y' minutes (default value is set to 10 minutes).

Starting with this release, this feature is enabled by default in the database. For disabling the feature or changing the configuration of 'X', 'Y' and 'Z', see the [Enabling Brute Force Login Protection \(Account Lockout\) for Forcepoint Management Infrastructure Access](#) knowledge base article.

Enhanced auditing of administrator actions

DLP Audit log provides granular visibility upon changes in DLP policies by displaying the DLP policy information before and after changes applied.

From this release, auditing changes apply to resources. The following resources are supported:

- User groups
- Networks
- Endpoint application groups
- Business units

Feature Deprecation

ActiveSync

On DLP 8.7.2, we announced the deprecation of Mobile Agent for on-premises Exchange ActiveSync. On this DLP release, all user interface components will be removed from the Forcepoint Security Manager.

**Note**

After upgrading to Forcepoint DLP 10.3, mobile forensics data may not be retained on the disk. Therefore, before upgrading to Forcepoint DLP 10.3, make sure your mobile forensics data is backed up to prevent potential data loss during the upgrade process.

Mobile forensics can be found under: <forensics location>\dss-<generated-id>\mobileData

For example: the default mobile folder location: %DSS_HOME%forensics_repository
\dss-9679E9C60D8B\mobileData

Python 2.5 Deprecation

From Forcepoint DLP 10.3 release, Python 3.6.8 will be used (except for Network Discovery and Fingerprinting which will use Python 2.5). This may impose an issue for customers running their own python 2.5 remediation scripts. For suggested solutions, see the [Python Remediation Scripts Compatibility Matrix](#) knowledge base article.

RSA SecurID authentication

DLP 10.3 is the final release supporting RSA SecurID authentication. Customers using RSA SecurID authentication are advised to migrate to Single Sign-On (SSO) authentication and utilize the Multi-factor authentication (MFA) provided by the identity provider (IdP). Forcepoint Security Manager supports Single Sign-on (SSO) via SAML 2.0 protocol and is certified for Okta and Azure AD as the IdP. This enables the security managers to have access control and improves the user access experience for cross-platform login. For more information, see the [Forcepoint Security Manager Help Guide](#).

New and updated policies and classifiers

This section highlights the new and updated policies and classifiers in the Forcepoint DLP version 10.3.

New Policies

- Puerto Rico PII
- Kenya PII
- Jersey PII
- Bahamas PII
- Tanzania PII
- Trinidad and Tobago PII

Updated Policies

- People's Republic of China PII
- People's Republic of China PII for Discovery
- US PHI

New Rules

- US PHI:
 - US PHI: Name and Medical Form
- People's Republic of China PII:
 - People's Republic of China PII: Surname and Address
- Puerto Rico PII:
 - Puerto Rico: SSN Number (Wide)
 - Puerto Rico: SSN Number (Default)
 - Puerto Rico: Driver License Number (Wide)
 - Puerto Rico: Driver License Number (Default)
- Kenya PII:
 - Kenya PII: ID Number (Wide)
 - Kenya PII: ID Number (Default)
- Jersey PII:
 - Jersey PII: SSN Number (Wide)
 - Jersey PII: SSN Number (Default)
- Bahamas PII:
 - Bahamas PII: National Insurance Number (Wide)
 - Bahamas PII: National Insurance Number (Default)
- Tanzania PII:
 - Tanzania PII: NIN Number (Wide)
 - Tanzania PII: NIN Number (Default)
- Trinidad and Tobago PII:
 - Trinidad and Tobago PII: National ID Number (Wide)
 - Trinidad and Tobago PII: National ID Number (Default)
- People's Republic of China PII:
 - People's Republic of China PII: Name and Phone Number (Wide)
 - People's Republic of China PII: Surname and Phone Number (Default)
 - People's Republic of China PII: Name and Health Identification Number (Wide)
 - People's Republic of China PII: Name and Health Identification Number (Default)
- People's Republic of China PII for Discovery:
 - People's Republic of China PII: Surname and Address

New classifiers

This section lists the new classifiers.

Script classifiers

- Email Similarity (Wide)
- Email Similarity (Default)
- Email Similarity (Narrow)
- Ireland PPS/PRSI
- Contract Reference of Secretaria de Seguridad Publica (SSP) Near Terms
- Vehicle Identification Number (VIN) Code (Wide)
- Vehicle Identification Number (VIN) Code (Default)
- Vehicle Identification Number (VIN) Code Near Terms
- Puerto Rico SSN Number Near Terms
- Puerto Rico Driver License Number Near Terms
- Kenyan ID Number Near Terms
- Jersey SSN Number Near Terms
- Bahamas NIN Near Terms
- Tanzanian NIN Near Terms
- Trinidad and Tobago NIN Near Terms
- People's Republic of China Phone Number (Default)
- People's Republic of China Phone Number Near Terms

Pattern classifiers

- PRC Personal Address (Chinese)
- PRC Personal Address (English)
- Vehicle Identification Number (VIN) Code No Validation
- Shadow Files Pattern (Wide)
- Shadow Files Pattern (Default)
- Password File Pattern (Wide)
- Password File Pattern (Default)
- Puerto Rico SSN Number (Wide)
- Puerto Rico Driver License Number (Wide)
- Kenyan ID Number (Wide)
- Jersey SSN Number (Wide)
- Bahamas NIN (Wide)
- Tanzanian NIN (Wide)
- Trinidad and Tobago NIN (Wide)
- Chinese Phone Number (Wide)
- People's Republic of China Identification Numbers(PRC)

Dictionary Classifiers

- Taiwan PII: Birthday Terms
- Taiwan PII: Marital Status Terms

Updated classifiers

It lists the updated classifiers.

Script classifiers

- Customizable IDs

Deleted classifiers

It gives information about the deleted classifiers.

Script classifiers

- Contract Reference of Secretaria de Seguridad Publica (SSP)
- Email Similarity
- Ireland PRSI/PPS
- Password Files
- Password Files (Wide)
- Shadow Files
- Shadow Files (Wide)
- Taiwan PII: Birthday
- Taiwan PII: Marital Status
- VIN Code (Default)

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 10.3 Forcepoint DLP installer also installs Forcepoint Security Manager version 10.3, Forcepoint Email Security version 8.5.5, and Forcepoint Web Security version 8.5.6.

Supported Endpoint Applications

The updated list of default operations monitored on each application group in Windows and macOS environments is shown below. The " Development Tools" application group has been added in this release.

Type	Copy/Cut	File Access	Paste	Download
Browsers				
CD Burners				
Cloud Storage				
Development Tools				
Email				
Encryption Software				
FTP				
IM				
Office Applications				
Online medical				
P2P				
Packaging Software				

Type	Copy/Cut	File Access	Paste	Download
Portable Devices				
SaaS (online)				

Upgrading Forcepoint DLP

Your data security product must be at version 8.9.1 or higher to upgrade to Forcepoint DLP version 10.3. If you have an earlier version, there are interim steps to perform. See [Upgrading to Forcepoint DLP 10.3](#)

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

- Machine Learning is not backward compatible after upgrading to Forcepoint Security Manager version 10.3.
- MIP decryption is not supported in Multi-user environments.

