



Forcepoint DLP

10.4.5

Maintenance Release Notes

About this release

The maintenance releases deliver new features, key fixes, and improvements aimed at enhancing the security and stability of our product.

This document provides information on the Forcepoint DLP Maintenance packages for Forcepoint DLP and Forcepoint Management Infrastructure.

New features in this release include:

- AI Security (AI Detection & Response) over the DLP Cloud API channel
- MCP Gateway (AI Agent Gateway) channel
- URL categories for DLP Endpoint
- Data Security Cloud configuration page updates in Forcepoint Security Manager

For details, see [New in Forcepoint DLP](#) and [New in Forcepoint Security Manager](#). For the fixes included in this release, see [List of fixes that are part of this Maintenance package](#).

The following package files are available in the 10.4.x maintenance release:

- Forcepoint DLP Maintenance Release Installer (`dlp_v10_4_x_maintenance_release.exe`) - Includes fixes for a specific Forcepoint DLP version
- Forcepoint Management Infrastructure Maintenance Release Installer (`fsm_v10_4_x_maintenance_release.exe`) - Includes fixes for the Forcepoint Security Manager's global setting interface



Note

The maintenance installers can be run on top of the corresponding Forcepoint DLP version. The Forcepoint DLP 10.4.x maintenance package is the maintenance release for the DLP Security Manager, and not for Secondary/Supplemental DLP Servers.

- For information on installing the maintenance release, see [Forcepoint DLP Install guide v10.4](#).
- For information on the maintenance upgrade, see [Forcepoint DLP Upgrade guide v10.4](#).

New in Forcepoint DLP

This release integrates Forcepoint DLP with the new Forcepoint AI Security solution, extending data loss prevention to AI applications and AI agents. It introduces the following new features:



Note

These features are available only from Forcepoint DLP 10.4.5 and are not included in the Forcepoint DLP 10.4.0 base release. To use them, install the 10.4.5 maintenance release on top of 10.4.0.

AI Security (AI Detection & Response) over DLP Cloud API channel

Forcepoint DLP now extends data loss prevention to sanctioned AI applications by integrating with the new Forcepoint AI Security solution. This integration allows security teams to monitor and mitigate user prompts,

file uploads, and AI responses as potential data transfer events. The events are analyzed by Data Protection Service, and DLP incidents are recorded in Forcepoint Security Manager.

Sanctioned AI applications are defined in Forcepoint Data Security Cloud and synchronized into Forcepoint Security Manager (for more information, see [New in Forcepoint Security Manager](#)). These AI applications can be selected as a destination in a DLP policy rule over the DLP Cloud API channel.

This solution requires a Forcepoint AI Security license, a provisioned Data Protection Service, and a DLP license which provide access to Forcepoint Security Manager's DATA module's DLP policies (i.e. DLP Endpoint, DLP Suite, DLP Network). For more information, see [Getting started with AI Security over DLP Cloud API channel](#).

MCP Gateway (AI Agent Gateway) channel

AI agents can call business applications like Atlassian exactly as an employee would, bypassing DLP inspection and leaving no audit trail. The new Forcepoint AI Security solution addresses this problem with Forcepoint MCP Gateway connectors, which sit between every AI agent or AI application and the business applications it calls. Every call is inspected before it executes. By integrating Forcepoint DLP with the Forcepoint AI Security solution, Data Protection Service analyzes that traffic through a new MCP Gateway channel, and DLP incidents are recorded in Forcepoint Security Manager.

Three resource types - **AI Agents**, **AI Agent Groups**, and **MCP Gateway Connectors** - are defined on Forcepoint Data Security Cloud and synchronized into Forcepoint Security Manager (for more information, see [New in Forcepoint Security Manager](#)). AI agents and agent groups can be selected as the source of a DLP policy rule, and MCP Gateway connectors as the destination.

This solution requires a Forcepoint AI Security license, a provisioned Data Protection Service, and a DLP license which provide access to Forcepoint Security Manager's DATA module's DLP policies (i.e. DLP Endpoint, DLP Suite, DLP Network). For more information, see [Getting started with the MCP Gateway channel](#).

URL categories for DLP Endpoint



Note

This feature will be supported in the upcoming Forcepoint F1E 26.09 and in an upcoming Forcepoint DSE Agent release. Stay tuned for the respective release notes notification.

Forcepoint DLP can now enforce URL categories on the endpoint web channel. A DLP rule can use URL categories as a destination for endpoint HTTP and HTTPS traffic. DLP inspects data transfers to a categorized site - including an unsanctioned AI site - and can audit or block the transaction from the endpoint.

The solution is available for customers who purchased a DLP Endpoint or DLP Suite license.

For more information, see [Supporting URL categories for the endpoint web channel](#)

New in Forcepoint Security Manager

Data Security Cloud configuration page updates

The page is used to connect Forcepoint Security Manager to Forcepoint Data Security Cloud for generating the Executive Overview dashboard.

A new **Data Module** section on the **Data Security Cloud** page makes the resources configured on Forcepoint Data Security Cloud available for use in DLP policies.

Each entry shows whether the corresponding license is available; where it is not, the required license is named and no toggle is shown.

Two synchronization toggles are available, both off by default:

- **Enable automatic sync of AI Security applications resources** - the AI applications used by the DLP Cloud API channel.
- **Enable automatic sync of MCP Gateway resources - AI agents, AI agent groups, MCP Gateway connectors** - the resources used by the MCP Gateway channel.

Synchronized resources appear under **Main > Policy Management > Resources** and can be selected in policy rules and action plans.

For more information, see [Before you begin: Check AI Security license availability and enable automatic resource sync](#) in the Forcepoint DLP Getting Started Guide.

System Requirements

Lists the system requirements that must be met for the maintenance release.

- Forcepoint DLP version 10.4.
- Forcepoint Management Infrastructure version 10.4.

List of fixes that are part of this Maintenance package

Each Forcepoint DLP maintenance package contains a set of fixes to bugs and issues.

Fixes included in this version of the maintenance

Issue ID	Component	Category	Description
DLP-37980	DLP Manager	Defect	The Help button in popup windows now open the related help page.
DLP-37784	DLP Manager	Defect	Fixed an issue where domains covered by an existing wildcard domain could not be exported or imported.
DLP-37814	DLP Manager	Defect	Fixed an issue where field restrictions on rule classifiers, such as "Search specific fields: Subject", were not enforced after a DLP policy was imported.
DLP-37762	DLP Manager	Defect	Fixed an issue where adding or removing computers in a Business Unit did not update the Endpoint Discovery tasks assigned to those endpoints.

Issue ID	Component	Category	Description
DLP-37755	DLP Manager	Defect	Fixed an issue where custom incident reports could take several minutes to load in the Forcepoint Security Manager.
DLP-37485	DLP Manager	Defect	The Destination column filter in the Incidents report now shows all resource types, not only Custom Computers, for subscriptions without the full DLP Suite.
DLP-36729	DLP Manager	Defect	The FSM System Log no longer fails to generate a WARNING record when the Incident Archive folder exceeds 100% capacity.
DLP-30986	DLP Manager	Defect	Fixed an issue where HTTP Strict Transport Security (HSTS) was not enforced on Forcepoint Security Manager port 17443 after upgrading.
FSM-563	Forcepoint Management Infrastructure	Defect	Fixed a user enumeration issue in the Forgot Password workflow of the Forcepoint Security Manager.



Note

10.4.5 contains all fixes previously released with a 10.4.x maintenance release. To see the full list of fixes, see the following:

- [List of fixes in Forcepoint DLP v10.4.4](#)
- [List of fixes in Forcepoint DLP v10.4.3](#)
- [List of fixes in Forcepoint DLP v10.4.2](#)
- [Resolved and Known Issues in Forcepoint DLP v10.4.0](#)

