



Forcepoint DLP

10.4.3

Maintenance Release Notes

Maintenance Release Notes

Overview

The maintenance releases address 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 Maintenance Release 10.4.x
- Forcepoint Management Infrastructure Maintenance Release 10.4.x



Note

Forcepoint DLP 10.4.x maintenance package is the maintenance release for the DLP Security Manager, and not for Secondary/Supplemental DLP Servers.

New in Forcepoint Security Manager

The PostgreSQL version upgrade

The PostgreSQL version has a major upgrade from 12 to 18.4. Uninstalling the Forcepoint Management Infrastructure Maintenance Release will not revert the PostgreSQL version back to 12, the version will remain 18.4.



Note

After uninstalling the Forcepoint Management Infrastructure 10.4.3 Maintenance Release, avoid running **Modify** from the Forcepoint Management Infrastructure 10.4 release setup, as this will cause incompatibility issues with the upgraded PostgreSQL component. Should that happen, functionality may be affected until the component is reconfigured. Refer to [Error Handling](#) in the Install Guide for reconfiguration instructions.

Forcepoint DLP and Forcepoint Management Infrastructure Maintenance Releases 10.4.x

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.

- 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](#).

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

The 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-36613	Data Security Manager	Defect	Resolved an issue where Forensics data stopped displaying on the Forcepoint Security Manager Console after installing the 10.4.2 Maintenance Release.
DLP-36321	Data Security Manager	Defect	Resolved an issue where Policy Engine deployment failed with a "Failed to convert content classifiers to XML" error when an external process held a file lock on the cached classifier file.
DLP-36231	Data Security Manager	Vulnerability	Resolved an issue in Forcepoint DLP 10.4.3 by backporting the exclusion of the Plexus utils dependency to address a vulnerability.
DLP-36212	Forcepoint Management Infrastructure	Defect	The maintenance release installer now correctly identifies supplementary server installations (servers without Forcepoint Management Infrastructure) and fails with an appropriate error message instead of proceeding with an invalid installation.

Issue ID	Component	Category	Description
DLP-36085	Data Security Manager	Defect	When editing a DLP Policy and Rule with a cloud email (CES) license, custom users are now displayed alongside Directory Entries when selecting a rule source element.
DLP-36084	Data Security Manager	Defect	The download incidents job in DPS environments no longer gets stuck.
DLP-35966	Data Security Manager	Defect	Resolved an issue where the Management Console UI crashed on the Logs > Debug Log page in version 10.4.2.
DLP-35913	Data Security Manager	Defect	Fixed the Microsoft Graph SDK integration in DLP 10.4 to resolve email addresses to User Principal Names (UPN) before calling the Exchange Online API, restoring mail notifications for users where email and UPN differ.
DLP-35851	Data Security Manager	Defect	Scheduled PDF incident reports emailed from FSM no longer omit incidents that caused the incident count to fail during PDF batch generation has been fixed.
DLP-35829	Data Security Manager	Vulnerability	Upgraded spring-security-web to version 5.8.16 in DLP Manager (10.4) to address a security vulnerability.
DLP-35731	Forcepoint Management Infrastructure	New feature	Upgraded the PostgreSQL version to 18.4.
DLP-35317	Data Security Manager	Defect	In some cases, it is observed that the URL category import from a linking service works incorrectly.
FSM-526	Forcepoint Management Infrastructure and Data Security Manager	Vulnerability	A vulnerable version of jackson-databind bundled in ehcache.jar has been upgraded to resolve the security vulnerability in Forcepoint Security Manager.

