Forcepoint DLP

10.4.1

Maintenance Release Notes

Revision A

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 10.4.1
- Forcepoint Management Infrastructure Maintenance Release 10.4.1

Note

Forcepoint DLP 10.4.1 maintenance package is the maintenance release for the DLP Security Manager, and not for Secondary/Supplemental DLP Servers.

New in Forcepoint Security Manager

Security Manager Behind Proxy

In this release Forcepoint Security Manager can now be operated behind a proxy, enabling deployments in restricted or controlled network environments. For more information on how to configure the Forcepoint Security Manager see Configuring Proxy Settings.

New in Forcepoint DLP

DLP Insights in Forcepoint Data Security Cloud platform's CISO Dashboard

The CISO Dashboard is a unified executive intelligence platform designed to provide Chief Information Security Officers with comprehensive, real-time visibility into their organization's security posture across multiple Forcepoint data protection and web security solutions.

The CISO Dashboard aggregates security incident data from multiple Forcepoint on-premises security products into a single, unified interface accessible via the Forcepoint Data Security Cloud platform.

In this release, customers can configure and send DLP incidents from Forcepoint Security Manager to the Forcepoint Data Security Cloud platform to be aggregated and viewed in the CISO Dashboard. For setup instructions, refer to the CISO Dashboard Solutions Guide.

Policy Export and Import - Classifiers, and Resources

Classifiers and Resources details can now be created or updated on the target system during the policy import process. Prior to this enhancement, a successful import required all DLP entities to already be configured on the target DLP system, matching the source DLP system. This release removes that prerequisite, significantly simplifying policy migration and replication across environments.

Supported Content Classifier Types

- Key phrases
- Regular expressions
- Dictionaries
- File Properties
- File Labeling

Supported Resource Types

- Custom users
- Custom computers
- Networks
- Domains
- Business units
- Action plans
- Notifications

For more information, see Policy Level, Classifier, and Resource Export/Import Support by Version.

New Export Options

While exporting policies, administrators can select the following options:

- **Include classifiers** and **Include resources**- To include or exclude classifiers and resources.
- **Set a password for zip file** - To set a password to encrypt the data and secure the policy zip file.

For more information see Export Policies.

Note

To keep enjoying the benefits of this feature when upgrading from 10.3.2 to 10.4, you must install immediately 10.4.1 maintenance release, since the feature is not supported in DLP 10.4 release.

Telemetry and Usage Data

Forcepoint DLP collects limited, non-personal operational telemetry data to support product diagnostics, service reliability, and continuous improvement. This telemetry does not include end-user content, personally identifiable information (PII), or any customer data subject to DLP policy enforcement. For more information, see Telemetry settings.

Purpose of Telemetry Collection

The telemetry data collected by Forcepoint is used solely for the following purposes:

- Diagnosing and resolving product issues more efficiently
- Improving product stability, performance, and usability
- Identifying underutilized features to guide product enhancements
- Supporting capacity planning and scalability improvements

- Proactively detecting systemic health issues across deployments

Forcepoint does not sell, share with third parties, or use telemetry data for any advertising or commercial profiling purposes.

Telemetry Notification and Default Behaviour

During maintenance release installation, a notification informs customers that telemetry collection is enabled by default.

Important

The telemetry is enabled by default once the upgrade is done. To disable it, go to **Data** > **General** > **Telemetry** in FSM and turn off the toggle.

Consider Disabling Telemetry If:

- The environment is air-gapped and has no external network access.
- The organization's policy does not permit sharing usage data with third parties.

Forcepoint DLP and Forcepoint Management Infrastructure Maintenance Releases 10.4.1

Following package files are available in the 10.4.1 maintenance release:

- Forcepoint DLP Maintenance Release Installer (`dlp_v10_4_1_maintenance_release.exe`) - Includes fixes for a specific Forcepoint DLP version
- Forcepoint Management Infrastructure Maintenance Release Installer (`fsm_v10_4_1_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

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-34923	Data Security Manager	Defect	Fixed the issue where manual installation of the 10.4 policy package failed due to the file size exceeding the default 100MB upload limit.
DLP-34908	Data Security Manager	Defect	Fixed the Web Security Linking Service "Test Connection" failure in DLP 10.4.
DLP-34888	Data Security Manager	Defect	Fixed the stale cache issue where renamed policies continued to display their old names in newly generated incidents.
DLP-34886	Data Security Manager	Defect	Fixed the inability to add administrators with AD Distinguished Names longer than 255 characters in EIP and DLP Manager.
DLP-34797	Data Security Manager	Defect	Resolved an issue which caused user attribute resolution (full name, email, manager) to silently fail for network HTTP incidents.
DLP-34689	Data Security Manager	Defect	Fixed the "Exclude Source from Rules" error in Tune Policy.
DLP-34516	Data Security Manager	Defect	Resolved the post 10.4 upgrade issue where deleting File Fingerprinting entries in Policy Management failed with “Connection to Crawler failed” message.
DLP-34085	Data Security Manager	Defect	Fixed Forensic Archiving failure to purge archive data over max disk space.
DLP-34005	Data Security Manager	Defect	Resolved the DLP 10.4 Management Console “Linking Service” test-connection failure issue.
DLP-33957	Data Security Manager	Defect	Resolved the IRR cases not displaying incident references in DLP 10.4.
DLP-33943	Data Security Manager	Defect	Resolved an issue where CSV directory imports failed when passwords exceeded 40 characters
DLP-33771	Data Security Manager	Defect	Resolved an issue where incident ID links in the “DLP Dashboard (last 7 days)” caused a NullPointerException and prevented opening incident details.

Issue ID	Component	Category	Description
DLP-33768	Data Security Manager	Defect	Resolved an issue where restricted users could bypass UI permissions to view incident details via a direct incident-details URL.
DLP-33521	Data Security Manager	Defect	Fixed the DLP backup process to properly log system messages in **DLP** > **Logs** > **System Log**.
DLP-33231	Data Security Manager	Defect	Resolved an issue where Arabic-numeral regex ranges were incorrectly rejected/handled, preventing customers from saving valid patterns and matching content.
DLP-33131	Data Security Manager	Defect	Resolved the 2026 calendar unavailability in incident reports and Discovery Scan scheduler.
DLP-33109	Data Security Manager	Defect	CSV user-directory import failures were resolved and imports now run successfully without SMB access-denied errors.
DLP-32556	Data Security Manager	Defect	Resolved an issue to allow quarantined emails to be successfully released.
DLP-32419	Data Security Manager	Defect	Resolved an issue to support file labeling.
DLP-32482	Data Security Manager	Defect	Resolved an issue where Analytics Engine top cases were not appearing in the FSM console.

Published 04 June 2026