



Forcepoint DLP

10.3.3

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 10.3.x
- Forcepoint Management Infrastructure Maintenance Release 10.3.x



Note

Forcepoint DLP 10.3.x 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](#).



Note

To keep enjoying the benefits of this feature when upgrading from 10.3.3 to 10.4, you must install immediately 10.4.2 maintenance release, since the feature is not supported in DLP 10.4 release.

New in Forcepoint DLP

DLP Insights in Forcepoint Data Security Cloud platform's Executive Overview Dashboard

The Executive Overview Dashboard is a unified executive intelligence platform designed to provide Business owners with comprehensive, real-time visibility into their organization's security posture across multiple Forcepoint data protection and web security solutions.

The Executive Overview 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 data from Forcepoint Security Manager to the Forcepoint Data Security Cloud platform to be aggregated and viewed in the Executive Overview Dashboard. For setup instructions, refer to the [Executive Overview Dashboard Solutions Guide](#).

**Note**

To keep enjoying the benefits of this feature when upgrading from 10.3.3 to 10.4, you must install immediately 10.4.2 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](#).

**Note**

To keep enjoying the benefits of this feature when upgrading from 10.3.3 to 10.4, you must install immediately 10.4.2 maintenance release, since the feature is not supported in DLP 10.4 release.

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 10.3.x

Following package files are available in the 10.3.x maintenance release:

- Forcepoint DLP Maintenance Release Installer (`dlp_v10_3_x_maintenance_release.exe`) - Includes fixes for a specific Forcepoint DLP version
- Forcepoint Management Infrastructure Maintenance Release Installer (`fsm_v10_3_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 v10.3](#).
- For information on the maintenance upgrade, see [Forcepoint DLP Upgrade guide v10.3](#).

System Requirements

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

- Forcepoint DLP version 10.3.
- Forcepoint Management Infrastructure version 10.3.

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-34884	Data Security Manager	Defect	Resolved an issue where customers with AD Distinguished Names longer than 255 characters could not be added as administrators in either EIP or DLP Manager.

For fixes included in previous 10.3.x releases, see the following:

- [List of fixes in Forcepoint DLP v10.3.2](#)
- [List of fixes in Forcepoint DLP v10.3.1](#)
- [Resolved and Known Issues in Forcepoint DLP v10.3.0](#)

