Forcepoint DLP

10.3.1

Maintenance Release Notes

Revision A

Contents

This document provides information on the Forcepoint DLP Maintenance package.

The maintenance installers can be run on top of the corresponding Forcepoint DLP version. The release includes multiple fixes for a given DLP version.

Forcepoint DLP Maintenance packages are supported on the DLP Manager.

The Forcepoint DLP Maintenance release (`Forcepoint_DLP_Maintenance_Release_10.3.1.174.exe`) and Forcepoint Management Infrastructure Maintenance release (`Forcepoint_EIP_Maintenance_Release_10.3.1.173.exe`) are the package files available in the 10.3.1 maintenance release.

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-28608	Data Security Manager	Defect	Resolved an issue where KV.tmp files triggered events since moving to inline proxy.
DLP-28610	Data Security Manager	New feature	Resolved an issue where Extended Actions Support actions were not returned as configured.
DLP-27329	Data Security Manager	Vulnerability	DLP Manager Policy Import has been updated to properly validate and sanitize extracted file paths, preventing Zip Slip attacks.

Issue ID	Component	Category	Description
DLP-27645	Data Security Manager	Defect	Resolved an issue where incident report links displayed a blank page for incidents created in DLP Manager connected to Analytics Engine (AE).
DLP-27353	Data Security Manager	New feature	A user/password authentication option has been added for proxy connections in the DPS-related code, allowing customers to complete the deployment.
DLP-28606	Data Security Manager	Defect	Resolved an issue where the assigned role now correctly receives the latest set of DLP policies.
DLP-28609	Data Security Manager	Defect	Resolved an issue where the REST API for Discovery incidents did not list the history, whereas it was available for data in motion incidents.
DLP-28758	Data Security Manager	Defect	Resolved an issue where customers were unable to change the "Change Status" of incidents in the DLP Manager workflow when opening an incident in a new window after upgrading DLP from version 10.2 to 10.3.
FSM-436	Data Security Manager	Defect	Resolved an issue where excessive SAML assertion validity duration occurred due to the *NotOnOrAfter* condition not being enforced in DLP Manager.
DLP-28798	Data Security Manager	Defect	Resolved an issue where the backup failed due to the error: "Could not find a part of the path".
DLP-28835	Data Security Manager	Defect	Fixed deadlock issues occurring in the HIBERNATE_SEGMENTED_ID_GENERATION table caused by high concurrency when generating IDs.

Published 24 March 2025