Forcepoint
DLP

8.9.1

Release Notes

Contents

Forcepoint DLP Release Notes

Use the Release Notes to find information about what's new and improved in Forcepoint DLP version 8.9.1.

- *New in Forcepoint DLP*
  - *Forcepoint DLP Incident Scale*
  - *Discovery Incident Scale*
  - *Forensic archiving scaling*
  - *SSL certificate expiration notification*
  - *Forcepoint Security Manager certified for deploying on Azure VM*
  - *Forcepoint DLP Endpoint Server(s) behind Azure load balancer*
  - *New and updated policies and classifiers*
- For installation or upgrade instructions, see:
  - *Installation and Upgrade*
  - Forcepoint DLP Installation Guide
  - Forcepoint DLP Upgrade Guide
- *Resolved and Known Issues for Forcepoint DLP*

For information on Forcepoint DLP Endpoint compatibility, see the latest Forcepoint F1E Release Notes.

Related concepts

Summary of new and changed features

Feature	Short description
Forcepoint DLP Incident Scale	Forcepoint Security Manager has been certified to support up to 5M DLP incidents per online partition.
Discovery Incident Scale	Forcepoint Security Manager has been enabled to support up to 16M Discovery incidents.
Forensic repository scale	Forensic repository has been enabled to support up to 10TB.
SSL certificate expiration notification	When SSL certification is about to expire, the system will display a notification on the dashboard of the DATA module and system logs. In addition, an email notification can be configured in the **General** > **Alerts** page, see the *Viewing the Dashboard* section in the Forcepoint DLP Administrator Guide.
Forcepoint DLP deployment in Azure	Forcepoint DLP has been certified for deploying on Azure EC2. For more information, see the *Installing Forcepoint DLP in Azure* in the Forcepoint DLP Installation Guide.
Endpoint Server behind Load Balancer	How to set up the Forcepoint DLP Endpoint Server(s) behind the Azure load balancer article is now available to provide the information to the customer on how to deploy Endpoint Servers in Azure and to use Azure Load Balancer to balance the load.
Support Windows Server 2022	Forcepoint DLP can be installed on Windows Server 2022.
New Classifiers	New, deleted, and enhanced classifiers are listed in *New and updated policies and classifiers*. For more information refer below section.

Related concepts
New and updated policies and classifiers on page 5

Feature and platform support deprecation

Feature	Short description
Mobile Agent	User interface components related to Mobile Agent will be removed from the DATA module in the Forcepoint Security Manager for future release.

New in Forcepoint DLP

This section explains the updates made in Forcepoint DLP version 8.9.1.

Forcepoint DLP Incident Scale

Forcepoint Security Manager has been enabled to support up to 5M DLP incidents per online partition and a total of 40M online incidents, for allowing customers to collect and access more incidents than before.

Discovery Incident Scale

The limitation of Discovery incidents has been removed, and the Forcepoint Security Manager has been certified to support up to 16M Discovery incidents.

Forensic archiving scaling

By increasing the forensic archiving to 10TB, Forcepoint DLP allows customers to leverage their data protection, and to deal with the increasing amount of data transfer a cross organizations.

SSL certificate expiration notification

Once in five years, the SSL certification that responsible for the secured connection between Forcepoint Security Manager and DLP system modules expires.

Go to, **Forcepoint Security Manager** > **DATA** > **General** > **Alerts**, an option to configure an alert is added, which will send an email notification when the SSL certification is about to expire. In addition, the system will display a notification on the dashboard of the DATA module and system logs. For more information, see the *Viewing the Dashboard* section in the Forcepoint DLP Administrator Guide.

Forcepoint Security Manager certified for deploying on Azure VM

After Forcepoint Security Manager certified for deployment on Amazon Web Services (AWS) in previous DLP release (8.9), a cloud-based environment has been certified to allow customers leverage the DLP solution on cloud-based environment according to their needs.

In this release, Forcepoint Security Manager has been certified for deploying on Azure VM. For more information, see the Installing Forcepoint DLP in Azure section in the Forcepoint DLP Installation Guide.

Forcepoint DLP Endpoint Server(s) behind Azure load balancer

How to set up the Forcepoint DLP Endpoint Server(s) behind the Azure load balancer article is now available to provide the information to the customer on How to deploy Forcepoint DLP Endpoint Server(s) in Azure and to use Azure load balancer to balance the load.

New and updated policies and classifiers

> **Related concepts**

New policies

- Brazilian General Data Protection Law (LGPD)
- Brazilian General Data Protection Law (LGPD) for Discovery
- Ecuador PII
- Ecuador PII for Discovery
- Ukraine PII
- Ukraine PII for Discovery
- United Arab Emirates PII
- United Arab Emirates PII for Discovery

Updated policies

- Germany PII
- Germany PII for Discovery
- Slovakia PII
- Slovakia PII for Discovery

New rules

- Brazilian General Data Protection Law (LGPD):
  - Brazilian General Data Protection Law: CPF and Sensitive Disease
  - Brazilian General Data Protection Law: Email Address and Password (Wide)

- Brazilian General Data Protection Law: Email Address and Password (Default)
- Brazilian General Data Protection Law: Identity Card Number
- Brazilian General Data Protection Law: Name and CPF
- Brazilian General Data Protection Law: Name and Sensitive Disease
- Brazilian General Data Protection Law: National Register of Legal Entities Number (Wide)
- Brazilian General Data Protection Law: National Register of Legal Entities Number (Default)
- Brazilian General Data Protection Law (LGPD) for Discovery:
  - Brazilian General Data Protection Law: CPF and Sensitive Disease
  - Brazilian General Data Protection Law: Email Address and Password (Wide)
  - Brazilian General Data Protection Law: Email Address and Password (Default)
  - Brazilian General Data Protection Law: Identity Card Number
  - Brazilian General Data Protection Law: Name and CPF
  - Brazilian General Data Protection Law: Name and Sensitive Disease
  - Brazilian General Data Protection Law: National Register of Legal Entities Number (Wide)
  - Brazilian General Data Protection Law: National Register of Legal Entities Number (Default)
- Ecuador PII:
  - Ecuador PII: Ecuadorian ID Number (Wide)
  - Ecuador PII: Ecuadorian ID Number (Default)
- Ecuador PII for Discovery:
  - Ecuador PII: Ecuadorian ID Number (Wide)
  - Ecuador PII: Ecuadorian ID Number (Default)
- Germany PII:
  - Germany PII: German ID Number (Wide)
  - Germany PII: German ID Number (Default)
  - Germany PII: German ID Machine Readable Number (Wide)
  - Germany PII: German ID Machine Readable Number (Default)
- Germany PII for Discovery:
  - Germany PII: German ID Number (Wide)
  - Germany PII: German ID Number (Default)
  - Germany PII: German ID Machine Readable Number (Wide)
  - Germany PII: German ID Machine Readable Number (Default)
- Italy PII:
  - Italy PII: Phone Number (Wide)
  - Italy PII: Phone Number (Default)
- Italy PII for Discovery:
  - Italy PII: Phone Number (Wide)
  - Italy PII: Phone Number (Default)
- Slovakia PII:
  - Slovakia PII: Slovakian ID Number (Wide)
  - Slovakia PII: Slovakian ID Number (Default)
- Slovakia PII for Discovery:
  - Slovakia PII: Slovakian ID Number (Wide)

- Slovakia PII: Slovakian ID Number (Default)
- Ukraine PII:
  - Ukraine PII: Ukrainian ID Number (Wide)
  - Ukraine PII: Ukrainian ID Number (Default)
- Ukraine PII for Discovery:
  - Ukraine PII: Ukrainian ID Number (Wide)
  - Ukraine PII: Ukrainian ID Number (Default)
- United Arab Emirates PII:
  - United Arab Emirates PII: Emirati ID Number (Wide)
  - United Arab Emirates PII: Emirati ID Number (Default)
- United Arab Emirates PII for Discovery:
  - United Arab Emirates PII: Emirati ID Number (Wide)
  - United Arab Emirates PII: Emirati ID Number (Default)

Updated rules

- Singapore PII:
  - Singapore PII: Singaporean ID Number (Default)
  - Singapore PII: Singaporean ID Number (Wide)
  - Singapore PII: Singaporean ID Number and CCN
- Singapore PII For Discovery:
  - Singapore PII: Singaporean ID Number

New classifiers

It lists the new classifiers.

Script classifiers

- Ecuadorian ID Number (Wide)
- Ecuadorian ID Number (Default)
- Ecuadorian ID Number Near Terms
- Emirati ID Number (Default)
- Emirati ID Number (Wide)
- Emirati ID Number Near Terms
- German ID Machine Readable Number (Default)
- German ID Machine Readable Number (Wide)
- German ID Machine Readable Number Near Terms
- German ID Number Near Terms
- Italian Phone Number Near Terms
- Singaporean ID Number (Wide)
- Singaporean ID Number (Default)

- Singaporean ID Number Near Terms
- Slovak ID Number Near Terms
- Ukrainian ID Number Near Terms

Pattern classifiers:

- German ID Number (Wide)
- Italian Phone Number (Wide)
- Slovak ID Number (Wide)
- Ukrainian ID Number (Wide)

Enhanced classifiers

It lists the enhanced classifiers.

Script classifiers:

- Swedish ID Number (Default)
- Swedish ID Number (Wide)
- Swedish ID Number Near Terms

Deleted classifiers

It gives information about the deleted classifiers.

Script classifiers:

- Singapore ID Number
- Singapore ID with support

Pattern classifiers:

- Singapore ID Terms

Installation and Upgrade

For installation or upgrade instructions, see:

- Forcepoint DLP Installation Guide

    Important updates for the installation guide:

    Note

    You must have Microsoft Visual C++ redistributable version 2022 (or later) to install the Forcepoint DLP Manager.

> 📝 **Note**
>
> The Secondary Forcepoint DLP server must be uninstalled from the Windows Control Panel and not from the Forcepoint Security Installer.

■ Forcepoint DLP Upgrade Guide

Operating system and hardware requirements

For the operating system and hardware requirements of Forcepoint DLP modules, see the Deployment and Installation Center.

For a step-by step guide to installing Forcepoint DLP, see the Forcepoint DLP Installation Guide.

Before you begin, open the Windows Control Panel and verify that the "Current language for non- Unicode programs" (in the Administrative tab of the Region and Language settings) is set to English. After installation, you can change it back to the original language.

The version 8.9.1 Forcepoint DLP installer also installs Forcepoint Security Manager version 8.6.4, Forcepoint Email Security version 8.5.4, and Forcepoint Web Security version 8.5.4.

Upgrading Forcepoint DLP

Your data security product must be at version 8.6.0 or higher to upgrade to Forcepoint DLP version 8.9.1. If you have an earlier version, there are interim steps to perform. See Upgrading to Forcepoint DLP 8.9.1

> ⚠️ **Important**
>
> Customers upgrading to Forcepoint DLP 8.9.1 from any version earlier than 8.8.1 that supports DLP Cloud Applications must connect to Data Protection Service to support the DLP Cloud Proxy, DLP Cloud API, and Cloud Data Discovery channels. To connect to Data Protection Service, request a JSON file with tenant information from Forcepoint Support. If your Data Security Manager is already connected to Data Protection Service, you do not need a new file or any additional action. For more information, see Configuring Data Protection Service in the Forcepoint DLP Administrator Guide.

Supported operating systems

See the Certified Product Matrix for information about all supported platforms, including supported browsers.

IPv6 support in Forcepoint DLP

Forcepoint DLP supports IPv6 in the following use cases:

1) Endpoint fully supports IPv6 addressing.

2) Web Proxy supports scanning IPv6 addressed web traffic.

3) UI support for IPv6 addressing in reporting.

Resolved and Known Issues for Forcepoint DLP

A list of Resolved and Known issues in this release is available to Forcepoint DLP customers.

If you are not currently logged in to the Forcepoint support website, clicking the link brings up a Customer Hub login prompt. Log in to view the list.