Forcepoint DLP

9.0

Upgrade Guide

Revision A

Published 30 September 2022

Contents

Chapter 1

Preparing to Upgrade Forcepoint DLP

Contents

Preparing to Upgrade to Forcepoint DLP 9.0

The existing Forcepoint DLP installation must be at one of the following versions to upgrade to version 9.0

- 8.9.x
- 8.8.x
- 8.7.x

If you have an earlier version, you will need to upgrade to version 8.7.0 first before beginning your upgrade to 9.0.

The existing data security solution must be at least version 8.7.x to upgrade directly to Forcepoint DLP version 9.0. Those currently using an earlier version must perform interim steps, as shown in the table below:

Current version	Step 1	Step 2
8.4 – 8.6.x	Upgrade to 8.7.x	Upgrade to 9.0
8.7.x–8.9.x	Upgrade to 9.0	

Prepare for upgrade

Steps to do before upgrading.

Note

The FSM system may appear unresponsive until the upgrade process is completed.

Steps

1) Unless instructed otherwise by Forcepoint Technical Support, make sure the system is functional prior to upgrade.

2) Verify that the starting version is 8.7.x, 8.8.x, or 8.9.x.

3) Perform a full backup of the system (including both product and infrastructure backups, as described in the appropriate version of the Backup and Restore FAQ).

4) If fingerprinting tasks are running, stop the fingerprinting and disable the scheduler.

5) Ensure that any supplemental fingerprint repositories are fully synchronized with the primary repository. Check for synchronization in the system log.

6) Log on to the management console to make sure all settings are deployed successfully. (If the **Deploy** button is highlighted, click it.)

7) If the existing deployment includes Forcepoint-supplied custom file types, change the name of the following configuration files as follows:

   a) Navigate to the `\policies_store\custom_policies\config_files` sub directory under the installation directory for your product.

   b) Rename `extractor.config.xml` to `custom_extractor.config.xml`.

   c) Rename `extractorlinux.config.xml` to `custom_extractorlinux.config.xml`. The file names are case-sensitive.

8) If administrators have removed applications from the product's predefined endpoint application groups, make a list of the changes. Application groups are restored after upgrade, the applications will need to be removed again. Custom user-defined groups are unaffected.

9) Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation. The UAC settings can be re-enabled following the upgrade.

10) Make sure that at least the Visual C++ version 2022 (or later) Runtime Libraries are installed on the management server. Download the Visual C++ Redistributable for Visual Studio from Microsoft.

Note

The speed and success of the upgrade process are affected by many factors, including:

- Number of online incidents
- Size of the forensics folder
- Number of policies or rules in use
- User directory import size
- Whether GPO restrictions are enforced on the server in domain membership scenarios
- Hardware specification

Download and launch the installer

Downloading and launching the installer.

The Forcepoint Security Installer (`ForcepointDLP90Setup.exe`) is used to upgrade the management server and other Windows-based servers. The management server is always upgraded first. To download the installer onto the management server machine:

Steps

1) Navigate to support.forcepoint.com and log in.

2) Click **Downloads** in the menu bar at the top of the page, then click the **All Downloads** link.

3) Under **Data Security** > **Forcepoint DLP**, click the **9.0** link.

4) Select Forcepoint DLP in the list of installers.

5) On the **Product Installer** page, click the **Download** link near the bottom of the page.

6) When the installer has downloaded successfully, double-click the file to launch the installer.

   It may take several minutes for the installer to unpack files and launch. This is expected behavior.
   The installation package detects that earlier versions of the product are installed, and automatically starts a series of wizards.

   After upgrade, the system has the same configuration as before the upgrade. The upgrade process does not allow the option to change configuration or settings.

Chapter 2

Upgrading Forcepoint DLP

Contents

Start the upgrade process by upgrading the management server. This is critical, because if supplemental servers or agents are upgraded before the management server, they stop communicating. When the management server is upgraded first, it continues communicating with the components until they are upgraded.

1) Perform the management server upgrade steps in the order described in the following sections:
   a) *Upgrade the management infrastructure*.
   b) *Upgrade the data security components on the management server.*
   c) *Complete post-upgrade steps on the management server.*

2) Post upgrade of the management server, upgrade supplemental servers and any other server components as described in following sections:
   - *Upgrade supplemental servers and Windows-based agents.*
   - *Upgrade protectors*
   - *Upgrade the Forcepoint DLP Protector software.*

3) After upgrading the management server and other server components, it is essential to deploy changes. See section *Deploy settings*.

4) If you have a DLP Cloud Applications license and are not already connected to Data Protection Service, see section *Data Protection Service* before upgrading.

5) If you are using Dynamic Data Protection (Endpoint DLP and Forcepoint Behavioral Analytics), you need to download the RAP User Manager tool to enable users for Dynamic Data Protection on a DLP system. See the Forcepoint Dynamic Data Protection Getting Started Guide for more information.

Related concepts

Upgrade the management infrastructure on page 10
Upgrade data security components on the management server on page 11

Related tasks

Complete post-upgrade steps on the management server on page 12
Upgrade supplemental servers and Windows-based agents on page 13
Upgrading the protector on page 14
Upgrade the Forcepoint DLP Protector software on page 15

Upgrade the management infrastructure

The Forcepoint Infrastructure provides basic framework for all of the components that make up management server. This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Initiates the wizard. 1) Click **Next** to begin the upgrade process. The system checks disk space requirements. 2) When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows information about the upgrade, including: ■ The destination folder for the installation files. ■ ■ The name of the SQL Server machine and the user. name of an authorized database administrator. The user must enter the SQL credentials used in the install of the earlier version of DLP. ■ The IP address of the management server and its administrator credentials. Click **Next** to accept the properties.

Wizard Screen	Fields
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A pop up message appears at this stage, warning that all modules must be upgraded. This pop up may be hidden behind the main installer window, so if the upgrade process appears to freeze, locate the hidden pop up by moving the main installer window, then click **OK** to proceed. In addition, if a Data Task Scheduler window opens, the installer offers the option to stop the Work Scheduler service, or continue running the installer and reboot at the end. Reboot is the recommended approach.
Summary	Provides an overview of what has been upgraded, including: ■ The destination folder for the installation files. ■ The name of the SQL Server machine and the user name of an authorized database administrator. ■ The IP address of the management server and its administrator credentials. Click **Finish** to complete the upgrade for this module. Restart the machine if prompted.

Upgrade data security components on the management server

Before running the Forcepoint DLP upgrade wizard, the installer validates system requirements to ensure the upgrade will be successful.

The pre-upgrade check validates hardware requirements, credentials for the SQL Server management database, endpoint security certificates, manager configuration, administrator upgrade permissions, and the database structure. As it proceeds, it reports whether a step succeeded or failed, or it shows a warning.

- If there is a failure, the upgrade stops. For details, see **\TRITON-PreUpgrade- SystemTests.log** in the product's installation directory.
- If there are only warnings, the installer offers the option to continue the upgrade. Continuing without repairing the issues may cause unexpected behavior, but should not a critical impact.
- If the pre-upgrade check succeeds, or if the administrator continues after viewing warnings, the Forcepoint DLP wizard is launched, followed by wizards for each installed component.

The Forcepoint DLP upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Initial Forcepoint DLP installation wizard launch page. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Configuration	Step through the screens configured during the previous product installation, including Fingerprinting Database, Temporary File Location, and Local Administrator. Click **Next** on each to retain the existing settings.
Installation Confirmation	Review the settings on the Installation Confirmation screen and click **Install** to continue the upgrade.
Installation	Shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more. In certain circumstances, an internal SQL error may appear. If this occurs, do not click OK until the issue has been resolved with Forcepoint Technical Support. Continuing without resolving the issue can cause problems with the reporting database.
Summary	Summarizes the upgrade configuration. 1) Click **Done**. A prompt about updating predefined policies and content classifiers appears. 2) Click **OK** to install the updates. The status of the updates is displayed, including the items being updated and details such as how many policies are updated, deleted, or added. 3) Click **Close** when the updates are complete. Restart the computer, if prompted.

Complete post-upgrade steps on the management server

After the upgrade process has completed successfully perform the following steps:

Steps

1) Log on to the management server machine with Administrator permissions.

2) To re-register all other components to the management server, run the appropriate installer on each host machine (see section *Upgrade supplemental servers and Windows based agents*).

3) Log into the Forcepoint Security Manager.

4) If applications were removed from the predefined endpoint application groups prior to upgrade, go to the **Main** > **>Resources** > **Endpoint Application Groups** page and remove them again.

5) After upgrading all components, click **Deploy** in the Security Manager.

Related tasks
Upgrade supplemental servers and Windows-based agents on page 13

Upgrade supplemental servers and Windows-based agents

To upgrade a supplemental Forcepoint DLP server, or a Windows-based standalone agent, to v9.0:

Steps

1) Launch the Forcepoint Security Installer, **Forcepoint Infrastructure**. The software is detected and the upgrade wizard appears.

2) Click **Next** until the wizard is completed.
Forcepoint DLP components found on this machine from a supported previous version are upgraded.

3) Complete the upgrade process by deploying changes in the Forcepoint Security Manager. As a best practice, finish upgrading all components, then log into the Forcepoint Security Manager and deploy all of the changes at once.

Note

Wait until the upgrade process is completed. It takes time for downloading the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before completing the upgrade process may cause Potential false positives and File-system discovery problems, where the discovery starts but immediately fails.

Upgrade protectors

Protectors can be upgraded from v8.7.x and later.

Preparing to upgrade the protector

Steps to be done before upgrading the protector.

Use these steps if the protector is at v8.7.0 or later. To download the upgrade script on the protector machine:

Steps

1) Navigate to support.forcepoint.com and click the **My Account** link.
2) Log in, then click **Downloads** in the menu bar at the top of the page.
3) Under **Data Security** > **Forcepoint DLP**, click the **9.0** link.
4) Select **Forcepoint DLP Appliance Upgrade Script from 8.7.x, 8.8.x, or 8.9.x** to **9.0** in the list of installers.
5) On the Product Installer page, click the **Download** link near the bottom of the page.
6) When the download is complete, unzip the **ProtectorUpdate90.zip** file.
7) Copy the resulting file, **protector-update-9.0-yyyy**, to directory /**tmp** directory. Here, yyyy is the latest build number, such as 9.0-3456.

Upgrading the protector

To run the upgrade script:

Steps

1) Enter the following command:
   ```
   chmod +x /tmp/protector-update-9.0-yyyy
   ```
2) Enter the following command:
   ```
   bash /tmp/protector-update-9.0-yyyy
   ```
3) Answer **Y** on the “Are you sure?” question, and complete the wizard, accepting the defaults.
4) Restart the protector machine when the wizard completes.
5) Deploy changes to complete the upgrade process. See section *Deploy settings*.

Note

Wait until the upgrade process is completed. It takes time for downloading the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before completing the upgrade process may result in false positives.

Related concepts
Deploy settings on page 16

Upgrade the Forcepoint DLP Protector software

If your deployment includes the Forcepoint DLP Protector software package, the upgrade process differs slightly from that described in section *Upgrade protectors*. Use the following steps to upgrade the Protector software package.

Steps

1) To download the software protector installer:
   a) Navigate to support.forcepoint.com and log in.
   b) Click **Downloads** in the menu bar at the top of the page.
   c) Under **Data Security** > **Forcepoint DLP**, click the **9.0** link.
   d) Select Forcepoint DLP Network appliance software package (Protector) in the list of installers.
2) Log in to the installation machine as root and copy the installation file into the Protector's `/tmp` directory.
3) Run the following command:
   `chmod +x /tmp/ForcepointDLP90ApplianceSoftwarePackage`
4) Execute `ForcepointDLP90ApplianceSoftwarePackage`
5) Complete the wizard.
6) Restart the Protector.

Updating configuration file

After upgrading of all DLP components on the DLP system, complete the following steps to handle vulnerability during upgrading to PolicyEngine 9.0 on linux.

Note

This section is only applicable for Linux system.

Steps

1) Go to `%DSS_HOME%\policies_store\policies\config_files\`

2) Open `extractorlinux.config.xml` file.

3) Delete the following snippet from the file.

```
<fileType id="291">
  <!-- XML_FMT -->
  <textExtractors>
  </textExtractors>
  <binaryExtractors>
   <name>XML</name>
  </binaryExtractors>
  <metadataExtractors/>
 </fileType>
```

4) Save `extractorlinux.config.xml` file.

5) Perform the same steps for `extractor.config.xml`

6) Make a **'fake deploy'** by changing the severity of one of the rules and click **No** on the **Deployment Needed** screen.

7) Then select the original severity of this rule and click **Yes** on the **Deployment Needed** screen to deploy the changes.

Deploy settings

After upgrading all servers, agents, and appliances to Forcepoint DLP 9.0, deploy changes in the Forcepoint Security Manager. Endpoints do not require a separate deploy step.

1) Log into the Data Security module of the Forcepoint Security Manager.

2) When prompted to update policies, follow the on-screen instructions.
Depending on the number of existing policies, this can take up to an hour. During this time, do not restart the server or any of the services.

3) Click **Deploy**.

Data Protection Service

This section is applicable to users with a Cloud Applications license, who are upgrading from versions earlier than Forcepoint DLP 8.8.1.

If you are not yet connected to Data Protection Service, you must connect using a Data Protection Service JSON configuration file. Request this file from Forcepoint Technical Support before upgrading to Forcepoint DLP 9.0.

To support cloud channels, DLP Cloud Applications must be activated. For more information, see Forcepoint DLP Administrator Help.

Configuring Data Protection Service

Use the **Data Protection Service** tab of the **Settings** > **General** > **Services** page to connect to Data Protection Service. This is done by uploading tenant information from the JSON file you received from Forcepoint. Note that each time a file is uploaded, the system resets as if this is the first connection:

Steps

1) Click **Select File**, and in the dialog box that appears, click **Choose File**. Browse to the JSON file you received from Forcepoint, and then click **OK**.

   The file is uploaded to the server, and the information begins to appear in the Connection area of the **Data Protection Service** tab.

2) Click **Connect** to establish the connection with Data Protection Service:

3) Click **Deploy** to begin enforcing policies in cloud channels.

4) Click **OK** at the bottom of the screen to complete the process.

   When the connection is active, the **Connect** button turns into a **Disconnect** button, enabling disconnection of Data Protection Service from Forcepoint DLP.

   In the Data Protection Service Status area, upon successful connection, the status is marked as **Connected successfully**, the time and date of the connection is displayed, and the **Recheck connection** link is enabled. This link is used to check the connection status in the event of problems. If an error is returned upon checking the connection, the status is listed as **Failed to connect**.

   After a successful connection to Data Protection Service is established, do the following to ensure the service is working properly:

   a) Deploy a policy to Data Protection Service.

   b) Check the incident report to make sure incidents are analyzed by Data Protection Service and not any other system component.

Note

As part of the integration with the Forcepoint Web Security Cloud, URL categories can now be imported from the Forcepoint Web Security Cloud Portal. See Forcepoint DLP Administrator Help for more information.

Error handling

- If Data Protection Service shows the status “Failed to connect”, the module is temporarily unavailable. Click **Connect** or **Recheck Connection** to try to connect again. If the problem continues, contact Forcepoint Technical Support.
- If the JSON file is uploaded for the first time, and when you click **Connect** the connection fails, the status shown is “Never connected”. This is because the Forcepoint Security Manager has never successfully connected to Data Protection Service. Contact Forcepoint Technical Support for assistance.

- If you receive the following message in the Data Protection Service Status area:

This service is not connected to Forcepoint CASB. Incident reporting and policy enforcement will be affected for cloud channels. See "Explain this page" for more information.

This means that there is a connection issue, and DLP Cloud API and Cloud Data Discovery channels will not enforce DLP policies, and the DLP Cloud Proxy channel might not report incidents to the Forcepoint Security Manager. See Forcepoint DLP Administrator Help, "Error handling", section for more information.

Re-enabling fingerprint classifiers

A customer with a version earlier than 8.8, who already uses fingerprint classifiers and upgrades directly to Forcepoint DLP 9.0 (for example, from DLP 8.7.1 to DLP 9.0) must perform a re-activation, as explained below. Until the activation is done, only files fingerprinted after the upgrade are protected.

Steps

1) To analyze structured data: Run a full scan (manually or by scheduler).

2) To analyze unstructured data, you must recreate the fingerprinting database (FPNE files) as follows:

   a) Go to the DLP installation folder `%DSS_HOME%`

   b) Run the following command to rebuild the fingerprinting database:

   ```
   FPRUtils -o UnstructuredInsertion -Command RecreateFPNE
   ```

   It can take about 10 minutes to rebuild the fingerprinting database depending on the size and number of fingerprints. It can also take an additional 10 minutes or so to automatically upload the fingerprints to the cloud.