Forcepoint

F1E

26.04

Upgrade Guide

Revision A

© 2026 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 17 June 2026

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

1 Upgrading Forcepoint F1E Solutions 5
About this guide 5
About the Product 5
Forcepoint DLP Endpoint package builder installation files 6
Automatic software updates 7
Guidelines for creating an anti-tampering password 7

2 Upgrading Forcepoint Web Security Endpoint 9
Forcepoint Web Security Endpoint Hybrid deployments 9
Forcepoint Web Security Endpoint Cloud deployments 14
Remote filtering deployments 19

3 Upgrading Forcepoint DLP Endpoint 21
Compatibility 21
Forcepoint DLP Endpoint Windows and Mac deployments 22
Automatic software updates 26
Post endpoint Upgrade 26

4 Upgrading Forcepoint Endpoint Context Agent 27
Compatibility 27
Forcepoint Endpoint Context Agent Windows deployments 28

5 Upgrading Mixed Deployments 31
Forcepoint F1E compatibility 32
Forcepoint Web Security Endpoint Hybrid, Forcepoint DLP Endpoint, and Forcepoint Endpoint Context Agent deployments 32
Remote filtering and DLP deployments 40

Chapter 1

Upgrading Forcepoint F1E Solutions

Contents

- About this guide on page 5
- About the Product on page 5
- Forcepoint DLP Endpoint package builder installation files on page 6
- Automatic software updates on page 7
- Guidelines for creating an anti-tampering password on page 7

This guide covers the full range of functionality available in the Forcepoint F1E agents.

Important

As a best practice, upgrade a handful of endpoint machines and ensure that they are working before upgrading all of the endpoint machines in your deployment.

About this guide

This guide describes how to upgrade Forcepoint F1E on endpoint machines across your enterprise.

Related concepts

Upgrading Forcepoint Web Security Endpoint on page 9
Upgrading Forcepoint DLP Endpoint on page 21
Upgrading Forcepoint Endpoint Context Agent on page 27
Upgrading Mixed Deployments on page 31

About the Product

Forcepoint™ F1E solutions provide complete real-time protection against advanced threats and data theft for both network and roaming users. Forcepoint advanced technologies help you discover and protect sensitive data stored on endpoint machines and provide actionable forensic insight into potential attacks.

The Forcepoint F1E platform places all installed Forcepoint F1E agents under one icon in the notification area of the task bar (Windows) or the status menu of the menu bar (Mac), instead of under separate icons for each agent. The new Forcepoint F1E agents share the same functionality as the older, conventional Forcepoint Endpoint agents.

Starting with Forcepoint DLP v8.9.x, Forcepoint DLP Endpoint on the Forcepoint F1E platform is the standard Forcepoint Endpoint agent for Forcepoint DLP (Windows and Mac) and Forcepoint Dynamic Data Protection (Windows only).

Starting with Forcepoint Web Security v8.5.5, Forcepoint Web Security Endpoint on the Forcepoint F1E platform is the standard Forcepoint Endpoint agent for Forcepoint Web Security on Windows and Mac. The Remote Filtering Client has not transitioned to the Forcepoint F1E platform.

Important

The new Forcepoint F1E cannot be downgraded to the older, conventional version.

If you update a Forcepoint F1E agent to v25.xx and need to downgrade to an earlier version, you must manually remove the new Forcepoint F1E version before you install the older, conventional version.

Forcepoint F1E Agent Components

This guide covers details on the following F1E agents:

- **Forcepoint Web Security Endpoint** protects users from web threats. Forcepoint offers three Forcepoint Web Security Endpoint options:
  - **Forcepoint Web Security Direct Connect Endpoint**: Requires a Forcepoint Web Security v8.5.5 (or later) on-premises solution with the Hybrid module or Forcepoint Web Security Cloud.
  - **Forcepoint Web Security Proxy Connect Endpoint**: Requires a Forcepoint Web Security v8.5.5 (or later)on-premises solution with the Hybrid module or Forcepoint Web Security Cloud.
  - **Remote Filtering Client**: Requires Forcepoint URL Filtering v8.5.5 (or later) with the Remote Filter module.
- **Forcepoint DLP Endpoint** protects organizations from data loss and data theft. It also identifies and helps secure sensitive data stored on corporate endpoint machines, including laptops. Requires Forcepoint DLP Network v8.9.x (or later) or Forcepoint Data Discovery v8.9.x (or later).
- **Forcepoint Endpoint Context Agent** (Forcepoint ECA) collects per-connection user and application information about Windows endpoint machines that connect through Forcepoint Next General Firewall (Forcepoint NGFW). Requires Forcepoint NGFW v6.10 (or later).

Forcepoint DLP Endpoint package builder installation files

The Forcepoint DLP v8.9.x (and later) installation no longer contains the package builder used to create the Forcepoint DLP Endpoint installation package. To install the latest Forcepoint DLP Endpoint, you must download the package builder from one of the following sections on the Forcepoint Downloads page.

- **Endpoint (DLP)** in **Data Loss Prevention (DLP)**
- **Endpoint (Web)** in **Web Security**
- **Endpoint (NGFW)** in **Next Generation Firewall (NGFW)**

Automatic software updates

Receive automatic software updates (Windows endpoint machines only): When new versions of Forcepoint DLP Endpoint are released, you may upgrade the software on each endpoint machine (this can be done via GPO or SMS), or you can configure automatic updates.

To automate software updates for Forcepoint DLP Endpoint through the package builder, see Automatic Updates for Forcepoint DLP Endpoint for details.

Guidelines for creating an anti-tampering password

For security purposes, anyone who tries to modify or uninstall Forcepoint F1E software (excluding Forcepoint ECA) is prompted for an anti-tampering password. Anti-tampering passwords must follow the following guidelines:

- Contain at least one number (0-9)
- Contain at least one letter (a-z or A-Z)
- Be no more than 65 characters (Mac operating systems)
- Be no more than 259 characters (Windows operating systems)

Using special characters (Mac operating systems)

On Mac endpoint machines, you can use the following special characters within your password:

> < * ? ! [ ] ~ ` ' " | ; ( ) & # \ $

If you include special characters in your password, you must enclose the password in single quotation marks when you type the password into the command line prompt. Otherwise, the operating system interprets the special character as a command and the password does not work.

- Correct: **'MyPa$$word1!'**
  - Password contains special characters and is properly quoted.
- Incorrect: **MyPa$$word1!**
  - Password contains special characters and is not properly quoted.

When you type the password into a field on a screen (like the package builder) or web page (like the Forcepoint Security Portal), you should not enclose the password in single quotation marks.

Using special characters (Windows operating systems)

On Windows endpoint machines, you can use the following special characters within your password:

> < * ? ! [ ] ~ ` ' " | ; ( ) & # \ $

If you use special characters within your password, you must include the ^ character before the special character when you type the password into the command line prompt. Otherwise, the operating system interprets the special character as a command and the password does not work.

- Correct: **MyP^>ssword1^&**
  - Special characters are prefixed by a ^ character.
- Incorrect: **MyP>assword1&**
  - Special characters are not prefixed by a ^ character.

When you type the password into a field on a screen (like the package builder) or web page (like the Forcepoint Security Portal), you should not include the ^ character before the special character.

Note

Post upgrade of the Forcepoint F1E solution, ensure to also update the Chrome extension on macOS system. Follow either of the methods to update the Chrome extension:

- Using MDM - Follow the steps documented in Installing the agent using Jamf.
- Add extension from the chrome webstore by using the following location: https://chromewebstore.google.com/detail/data-loss-prevention-exte/hlidgbhacggcmajpohnnhbkacekdhjod

Chapter 2

Upgrading Forcepoint Web Security Endpoint

Contents

- Forcepoint Web Security Endpoint Hybrid deployments on page 9
- Forcepoint Web Security Endpoint Cloud deployments on page 14
- Remote filtering deployments on page 19

This chapter covers the steps for upgrading Forcepoint Web Security Endpoint if you are using the Forcepoint Web Security Hybrid Module or Forcepoint Web Security Cloud on a Windows or Mac endpoint machine. If you are upgrading a mixed deployment consisting of Forcepoint DLP Endpoint, Forcepoint Web Security Endpoint, and Forcepoint ECA, see *Upgrading Mixed Deployments*.

Important

If you upgrade endpoint machines to Windows 10 from any of the following operating systems:

- Windows Server 2012
- Windows Server 2016

After upgrading the Forcepoint Web Security Endpoint, you must re-install the Forcepoint Web Security Endpoint software.

Forcepoint Web Security Direct Connect Endpoint cannot be installed on an endpoint machine running Windows Server.

Related concepts

Upgrading Mixed Deployments on page 31
Forcepoint Web Security Endpoint Hybrid deployments on page 9
Forcepoint Web Security Endpoint Cloud deployments on page 14

Forcepoint Web Security Endpoint Hybrid deployments

Compatibility

Forcepoint Web Security Endpoint is recommended for use with these Forcepoint Web Security component versions.

Component	Minimum supported version	Recommended version
Forcepoint Web Security	v8.5.5	Latest v8.5.5 maintenance version or later
Forcepoint URL Filtering (for Remote Filtering Client)	v8.5.5	Latest v8.5.5 maintenance version or later

If your organization is using a Forcepoint Web Security or Forcepoint URL Filtering version earlier than v8.5.5, you must upgrade to at least v8.5.5 before upgrading your endpoint machines to Forcepoint Web Security Endpoint v25.xx.

You do not need to uninstall the earlier version of Forcepoint Web Security Endpoint before installing v25.xx if you are upgrading from Forcepoint Web Security Endpoint v8.5.5 or later. If you are upgrading from a Forcepoint Endpoint version earlier than v8.5.5, Forcepoint recommends that you upgrade to at least v8.5.5 before upgrading to v25.xx, or uninstall the earlier version before you install this Forcepoint F1E version.

Adding a custom DCUserConfig.xml file to a Forcepoint Web Security Direct Connect Endpoint installation package

If you have a custom `DCUserConfig.xml` file that you want to use instead of the default file provided with the installation package, complete the following steps before you deploy the installation package.

Steps

1) Create the installation package through the package builder.

2) Run the following command from the command line to unpack the installation package:

   ```
   All-in-One.exe -fromexe <full_pathname_to_package>
   ```

   where <full_pathname_to_package> is the full path and filename of the installation package executable file.

   For example, if the FORCEPOINT-ONE-ENDPOINT-x64.exe file is located in C:\Test, the full command would be:

   ```
   All-in-One.exe -fromexe C:\Test\FORCEPOINT-ONE-ENDPOINT- x64.exe
   ```

3) The unpacked installation package is now visible in the folder created in step 2 (in this example: C:\Test \FORCEPOINT-ONE-ENDPOINT-x64).

   Copy your `DCUserConfig.xml` file into this folder.

4) Repack the installation package by running the following command from the command line:

   ```
   All-in-One.exe -toexe <full_pathname_to_package>
   ```

5) Deploy the updated installation package using one of the methods below.

Upgrade steps for Windows

Important

The new Forcepoint F1E cannot be downgraded to the older, conventional version.

If you update to Forcepoint Web Security Endpoint v25.xx and need to downgrade to an earlier version, you must manually remove the new Forcepoint Web Security Endpoint version before you install the older, conventional version.

Option 1: Auto-update

You can auto-update in the following scenarios:

- Forcepoint Web Security Proxy Connect Endpoint to Forcepoint Web Security Proxy Connect Endpoint
- Forcepoint Web Security Direct Connect Endpoint to Forcepoint Web Security Direct Connect Endpoint

To auto-update:

1) Log on to the Web module of the Forcepoint Security Manager.

2) Go to **Settings > Hybrid Configuration > Hybrid User Identification**.

3) Select **Automatically update endpoint installations when a new version is released** if you want to ensure that your endpoint machines have the latest version when it is available from the hybrid service.

4) Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

The setting is disabled by default, as most organizations like to control the software on the endpoint machines themselves and test newer versions before deploying them. You may want to enable the option after you have tested the new Forcepoint Web Security Endpoint software so all users (including roaming users) get the latest software installed. After they have all updated the software, you can disable updates again.

When Forcepoint Web Security Endpoint software update is taking place (which can take several minutes), end users are unable to browse, and are shown a web page stating that the software is updating. This page continues to retry the requested web page every 10 seconds until the software finishes updating. After the software update is done, the browser shows the requested page correctly if the user is allowed to access this URL, or alternatively shows a block page if access is not allowed.

Note

- The **wepsvc** service must be running on the endpoint machine for auto-update to run properly.
- You cannot use the auto-update feature in the Web module of the Forcepoint Security Manager to automate updates for a mixed deployment.
- You cannot use auto-update to upgrade from Forcepoint Proxy Connect Endpoint to Forcepoint Direct Connect Endpoint or Forcepoint Web Security Direct Connect Endpoint to Forcepoint Web Security Proxy Connect Endpoint. You must uninstall the installed version before installing the new version.

Option 2: Create a new endpoint installation package using the Forcepoint Endpoint package builder

Note

If you are working with multiple agent installation, refer to the Forcepoint Agent Compatibility Knowledge Base article.

1) Download the latest package builder from the Forcepoint Support site:
   a) Log on to the Forcepoint Downloads page.
   b) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.
   c) Select the desired package builder.
   The **Product Installer** view opens.
   d) Click **Download**.
   A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.
2) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.
   The Forcepoint Endpoint package builder utility extracts required files and launches.
3) On the **Select Endpoint Components** screen, select **Forcepoint Web Security Endpoint**.
4) Under **Forcepoint Web Security Endpoint**, select **Direct Connect Endpoint** or **Proxy Connect Endpoint**.
5) Choose **Windows 64-bit** when prompted.
6) Deploy the v25.xx package to each endpoint machine using GPO, SMS, or a similar deployment method.
   For more information about deploying Forcepoint Web Security Endpoint, see the Forcepoint F1E Installation Guide.
   You do not need to uninstall the earlier version of Forcepoint Web Security Endpoint before installing v25.xx if you are upgrading from Forcepoint Web Security Endpoint v24.03.x or later. Versions earlier than v24.03 must be upgraded to at least v24.03 or uninstalled before this version is installed.

   Important

   If you deploy Forcepoint F1E using GPO, do not restrict access to the command prompt. The **Disable the command prompt script processing also?** option should be set to **No**.
7) Restart the endpoint machine after installation is complete.

Note

Forcepoint Web Security Direct Connect Endpoint end users must join your organization's domain on the endpoint machine. If the end user has not joined and connected to your domain, the disposition server test fails.

Upgrade steps for Mac

Option 1: Auto-update

1) Log on to the Web module of the Forcepoint Security Manager.

2) Go to **Settings** > **Hybrid Configuration** > **Hybrid User Identification**.

3) Select **Automatically update endpoint installations when a new version is released**, if you want to ensure that your endpoint machines have the latest version when it is available from the hybrid service.

4) Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Note

The **wepsvc** service must be running on the endpoint machine for auto-update to run properly.

Option 2: Create a new endpoint installation package using the Forcepoint Endpoint package builder

1) Download the latest package builder from the Forcepoint Support site:

   a) Log on to the Forcepoint Downloads page.

   b) Do one of the following:

   - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
   - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
   - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.

   c) Select the desired package builder.
   The **Product Installer** view opens.

   d) Click **Download**.
   A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.

2) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.

The Forcepoint Endpoint package builder utility extracts required files and launches.

3) On the **Select Endpoint Components** screen, select **Forcepoint Web Security Endpoint**.

4) Under **Forcepoint Web Security Endpoint**, select **Proxy Connect Endpoint** or **Direct Connect Endpoint**.

5) Choose **Mac** when prompted.

6) When the wizard completes, unzip the `FORCEPOINT-ONE-ENDPOINT-Mac.zip` package onto your Mac endpoint machines.

7) If you had selected Proxy Connect Endpoint for your installer package, edit `endpoint.config` to add the **WSCONTEXT** value.
The **WSCONTEXT** value is displayed in the GPO script command string on the **Settings** > **Hybrid Configuration** > **Hybrid User Identification** page in the Web Security module of the Forcepoint Security Manager, or the GPO code string under **Deployment Settings** on the **Web** > **Endpoint** > **General** page in the Forcepoint Cloud Security Gateway Portal.

8) Run the `WebsenseEndpoint.pkg` from the unzipped folder **EndpointInstaller**.

9) Follow the steps in the installation wizard.

10) End users may be prompted to log out and re-log on to their endpoint machines.

Forcepoint Web Security Endpoint Cloud deployments

Compatibility

Forcepoint Web Security Cloud is a module of the web-based Forcepoint Security Portal, so it is always at the latest version. The Forcepoint Web Security Endpoint version available through the Forcepoint Security Portal is always compatible with the current Forcepoint Web Security Cloud.

You do not need to uninstall the earlier version of Forcepoint Web Security Endpoint before installing v25.xx if you are upgrading from Forcepoint Web Security Endpoint v24.03.x or later. Versions earlier than v24.03 must be upgraded to at least v24.03 or uninstalled before this version is installed.

Upgrade steps for Windows

Option 1: Auto-update

Note

The **wepsvc** service must be running on the endpoint machine for auto-update to run properly.

1) In the Forcepoint Security Portal, go to **Web** > **Policy Management** > **Policies**. Under the policy you wish to view, open the **Endpoint** tab.

2) Under **Endpoint Installation** and **Enable automatic updates for these endpoint clients**, select the **Windows** check box for either **Proxy Connect** or **Direct Connect**.

3) Click **Submit**.

Important

The new Forcepoint F1E cannot be downgraded to the older, conventional version.

If you auto-update to Forcepoint Web Security Endpoint v25.05 and need to downgrade to an earlier version, you must manually remove the new Forcepoint F1E version before you install the older, conventional version.

Option 2: Download a new endpoint installation package from the Forcepoint Security Portal

Customers with a full-cloud deployment (Forcepoint Web Security Cloud) can download Forcepoint Web Security Endpoint installation packages from the Forcepoint Security Portal.

1) Log on to the Forcepoint Security Portal.

2) Go to **Web > Settings > Endpoint**.

3) Click **Set Anti-Tampering Password** to set the anti-tampering password if you have not already done so.

4) Enter and confirm your anti-tampering password, then click **Submit**.

5) Under **Endpoint Client Download**, select either the **Proxy Connect** or **Direct Connect** Endpoint type, and then select **Windows 64- bit** from the **Platform** drop-down menu. You can deploy a combination of Direct Connect and Proxy Connect Endpoint clients in your organization if desired. However, only one type can be installed on an individual endpoint machine.

6) Click the **Available version** number to download the Forcepoint Web Security Endpoint zip file.

7) When you download Forcepoint Web Security Endpoint, it should include the `Websense Endpoint.msi` file along with a file called `HWSConfig.xml`, which is specific to your account. This file needs to be in the same directory as the .msi file for the Forcepoint Web Security Endpoint agent to successfully install.

If you wish to use Forcepoint Web Security Endpoint over port 80 for proxying and PAC file retrieval, you need to do the following before installing the Endpoint software:

- Ask your Forcepoint support representative to add the “Send HWS endpoint to port 80” template to your account. You can add this template to specific policies or globally.
- Change the HWSConfig line from the following:
  <PACFile URL=“http://webdefence.global.blackspider.com:8082/proxy.pac” /> to this:

  <PACFile URL=“http://pac.webdefence.global.blackspider.com/proxy.pac” />

  By applying this template, you also move any endpoint machines that are already installed to port 80.

8) Deploy the package to each endpoint machine using GPO, SMS, or a similar deployment method.
For more information about deploying Forcepoint Web Security Endpoint, see the Forcepoint F1E Installation Guide.

   You do not need to uninstall the earlier version of Forcepoint Web Security Endpoint before installing v25.05 if you are upgrading from Forcepoint Web Security Endpoint v24.03. Versions earlier than v24.03 must be upgraded to at least v24.03 or uninstalled before this version is installed.

   Important

   If you deploy Forcepoint F1E using GPO, do not restrict access to the command prompt. The **Disable the command prompt script processing also?** option should be set to **No**.

9) Restart the endpoint machine after installation is complete.

Option 3: Create a new endpoint installation package using the Forcepoint Endpoint package builder

1) Download the latest package builder from the Forcepoint Support site:
   a) Log on to the Forcepoint Downloads page.

   b) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.

   c) Select the desired package builder.
   The **Product Installer** view opens.

   d) Click **Download**.
   A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.

2) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.
The Forcepoint Endpoint package builder utility extracts required files and launches.

3) On the **Select Endpoint Components** screen, select **Forcepoint Web Security Endpoint**.

4) Under **Forcepoint Web Security Endpoint**, select **Direct Connect Endpoint** or **Proxy Connect Endpoint**.

5) Choose **Windows 64-bit** when prompted.

6) Deploy the package to each endpoint machine using GPO, SMS, or a similar deployment method.
For more information about deploying Forcepoint Web Security Endpoint, see the Forcepoint F1E Installation Guide.

   You do not need to uninstall the earlier version of Forcepoint Web Security Endpoint before installing v25.xx if you are upgrading from Forcepoint Web Security Endpoint v24.03. Versions earlier than v24.03 must be uninstalled before this version is installed.

Important

If you deploy Forcepoint F1E using GPO, do not restrict access to the command prompt. The **Disable the command prompt script processing also?** option should be set to **No**.

Related concepts
Guidelines for creating an anti-tampering password on page 7

Upgrade steps for Mac

Option 1: Auto-update

Note

The **wepsvc** service must be running on the endpoint machine for auto-update to run properly.

For Mac operating system users, Forcepoint Endpoint can automatically deploy newer versions to browsers without involvement from administrators.

1) In the Forcepoint Security Portal, go to **Web** > **Policy Management** > **Policies**. Under the policy you wish to view, open the **Endpoint** tab.

2) Under **Endpoint Installation** and **Enable automatic updates for these endpoint clients**, select the **Mac** check box for either **Proxy Connect** or **Direct Connect**.

3) Click **Submit**.

Important

The new Forcepoint F1E cannot be downgraded to the older, conventional version.

If you auto-update to Forcepoint Web Security Endpoint v25.xx and need to downgrade to an earlier version, you must manually remove the new Forcepoint F1E version before you install the older, conventional version.

Option 2: Download the new endpoint installation package from the Forcepoint Security Portal

To upgrade Forcepoint Web Security Endpoint manually on a single machine, follow these steps for installing the latest version:

1) Log on to the Forcepoint Security Portal.

2) Go to **Web > Settings > Endpoint**.

3) Click **Set Anti-Tampering Password** to set the anti-tampering password if you have not already done so.

4) Enter and confirm your anti-tampering password, then click **Submit**.

5) Under **Endpoint Client Download**, select either the **Proxy Connect** or **Direct Connect** Endpoint type, and then select **Mac** from the **Platform** drop-down menu. You can deploy a combination of Direct Connect and Proxy Connect Endpoint clients in your organization if desired. However, only one type can be installed on an individual endpoint machine.

6) Click on the version number to download the Forcepoint Web Security Endpoint zip file.

7) Double-click the installation package to open an introductory screen for the installer. Click **Continue** for step-by-step instructions on the installation process.

8) When you reach the “Standard install on Macintosh HD” screen, click **Install** to begin the installation process.
You must install Forcepoint Web Security Endpoint on the local hard disk. You can change the installation location on this screen by clicking **Change Install Location**.

9) Enter a user name and password for a user with administrator rights to install the software.

10) A confirmation screen informs you if the installation is successful. Click **Close.**

Related concepts
Guidelines for creating an anti-tampering password on page 7

Remote filtering deployments

If you are using Remote Filtering Client, use the following upgrade steps:

Upgrade steps for Windows

Steps

1) Download the latest package builder from the Forcepoint Support site:
   a) Log on to the Forcepoint Downloads page.
   b) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.
   c) Select the desired package builder.
      The **Product Installer** view opens.
   d) Click **Download**.

   A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.

2) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.
   The Forcepoint Endpoint package builder utility extracts required files and launches.

3) On the **Select Endpoint Components** screen, select **Forcepoint Web Security Endpoint**.

4) Under **Forcepoint Web Security Endpoint**, select **Remote Filtering Client**.

5) Choose **Windows 64-bit** when prompted.

6) Deploy the package to each endpoint machine using GPO, SMS, or a similar deployment method. You can install this version on top of earlier versions without uninstalling the earlier versions.

   Important

   If you deploy Forcepoint F1E using GPO, do not restrict access to the command prompt. The **Disable the command prompt script processing also?** option should be set to **No**.

   For more information about using the Forcepoint F1E package builder and installing and deploying Forcepoint F1E solutions, see the Forcepoint F1E Installation Guide.

Chapter 3

Upgrading Forcepoint DLP Endpoint

Contents

- Compatibility on page 21
- Forcepoint DLP Endpoint Windows and Mac deployments on page 22
- Automatic software updates on page 26
- Post endpoint Upgrade on page 26

This chapter covers the steps for upgrading Forcepoint DLP Endpoint. If you are upgrading a mixed deployment consisting of Forcepoint DLP Endpoint, Forcepoint Web Security Endpoint, and Forcepoint ECA, see *Upgrading Mixed Deployments*.

Note

If you are working with multiple agent installation, refer to the Forcepoint Agent Compatibility Knowledge Base article.

Related concepts

Upgrading Mixed Deployments on page 31
Forcepoint DLP Endpoint Windows and Mac deployments on page 22
Automatic software updates on page 26
Post endpoint Upgrade on page 26

Related reference

Compatibility on page 21

Compatibility

Forcepoint DLP Endpoint is recommended for use with these Forcepoint DLP component versions.

Component	Minimum supported version	Recommended version
Forcepoint DLP Network	v8.9.x	Latest v8.9.x maintenance version or later
Forcepoint Data Discovery	v8.9.x	Latest v8.9.x maintenance version or later

If your organization is using a Forcepoint DLP version earlier than v8.9.x, please upgrade to at least v8.9.x if you plan to upgrade Forcepoint DLP Endpoint.

You do not need to uninstall earlier Forcepoint F1E versions before installing v25.xx if you are upgrading from Forcepoint DLP Endpoint v24.03 or later.

Note

The Forcepoint DLP v8.9.x (and later) installation no longer contains the package builder used to create the Forcepoint DLP Endpoint installation package. To prepare the latest Forcepoint DLP Endpoint, you must download the package builder from the Forcepoint Support site.

Forcepoint DLP Endpoint Windows and Mac deployments

To upgrade your existing version of Forcepoint DLP Endpoint:

Note

If the user uses custom messages on the endpoint and before upgrading to v25.xx, they have to push these custom messages again via FSM profile after the upgrade.

1) Make sure you have a v8.9.x or later management server installed and functioning. You must be logged on to the Forcepoint DLP server with a Service Account before you run the package builder. Otherwise, incorrect communication keys are created and Forcepoint DLP Endpoint cannot connect to the Forcepoint DLP server.

2) (optional) Make a backup copy of the Endpoint package builder executable file, `WebsenseEndpointPackageBuilder.exe`. This file is found at `C:\Program Files (x86)\Websense\Data Security\client`.

3) Download `ForcepointOneEndpointPackage.zip` from the Forcepoint Downloads page and unzip it into the C:\Program Files (x86)\Websense\Data Security\client folder. Five files are unzipped and placed in the folder:

   - The `WebsenseEndpointPackageBuilder.exe` file is for building the Forcepoint DLP Endpoint software package to install on your endpoint machines.
   - The `WebsenseEPClassifier.pkg.zip` file is a DLP Endpoint Classifier exclusively for Mac endpoints running Forcepoint DLP Endpoint.
     Sites that are not running Forcepoint DLP Endpoint on Mac can ignore the `WebsenseEPClassifier.pkg.zip`.file.
   - The `EPA64.msi` file is the Endpoint Classifier for Win64 endpoint machines.
     Sites that are not running Forcepoint DLP Endpoint on Win 64 machines can ignore the `EPA64.msi` file.

     Important

     Due to a compatibility issue with older Windows Endpoint Classifier files, you must use the Windows Endpoint Classifier files provided in this ZIP file when you build a Windows Forcepoint DLP Endpoint installation package using this package builder.

     If you use older Windows Endpoint Classifier files, the package builder shows an error message and does not build an installation package.
   - The `EndpointMessageTemplates.zip` file contains the updated endpoint message templates for this release. For Forcepoint DLP Endpoint customers, the v20.09 release introduced a new message that

may not be available in Forcepoint DLP yet. To show this message, customers must replace their message templates through the Forcepoint Security Manager:

- If you are replacing the default message template, see the Updating Confirmation Dialog message files in Forcepoint One Endpoint v19.06 and later Knowledge Base article.
- If you use a custom message template, you need to add the new messages to your custom file. See the Customizing Forcepoint DLP Endpoint client messages Knowledge Base article.

4) If you have Mac endpoint machines running Forcepoint DLP Endpoint:

   a) Back up the file `WebsenseEPClassifier.pkg.zip` in the following folder: `C:\Program Files (x86)\Websense\Data Security\client\OS X`. If the OS folder does not exist, create it.

   b) Copy the new `WebsenseEPClassifier.pkg.zip` from the folder in step 3 and place it into the `\OS X` folder.
   You do not need to unzip this file. It is automatically unzipped by the package builder when it creates the new Mac installation package.

5) If you have Win64 endpoint machines running Forcepoint DLP Endpoint:

   a) Back up the file `EPA64.msi` in the following folder:
   `C:\Program Files (x86)\Websense\Data Security\client`.

   b) Copy the new `EPA64.msi` from the folder in step 3 and place it into
   `C:\Program Files (x86)\Websense\Data Security\client`.

6) Run `WebsenseEndpointPackageBuilder.exe` to generate a new Forcepoint DLP Endpoint installation package.

7) Deploy the v25.xx installation package to each endpoint machine using one of the methods described in the Forcepoint F1E Installation Guide.

8) If you are upgrading to Forcepoint DLP Endpoint v21.12 or later on macOS 11 (Big Sur) onwards, you are prompted to enable full disk access (FDA) for new processes:

   a) When the installer opens the prompt, click **Open Full Disk Access** to open the macOS System Preferences window.

   b) On the **Privacy** tab, select `ESDaemonBundle.app` and `Websense Endpoint Helper.app`.

   c) Click the **+** button under the list.

   d) Go to `Library/Application Support/Websense Endpoint/DLP/`, select **wsdlpd**, then click **Open**.

   e) Verify that **wsdlpd** is included in the list and selected.

   f) Click the **+** button under the list.

   g) Go to `Library/Application Support/Websense Endpoint/EPClassifier/`, select **EndPointClassifier**, then click **Open**.

   h) Verify that **EndPointClassifier** is included in the list and selected.

i) Close the **Security & Privacy** window.

Note

If you are deploying Forcepoint DLP Endpoint using Jamf, you can enable FDA for these processes using a configuration file. For more information, see Deploying the endpoint package through Jamf in the *Forcepoint F1E Install Guide*.

9) Restart the endpoint machine after installation is complete, if needed.

Upgrade from	Restart Required?
Forcepoint DLP Endpoint (Windows)	
v24.03 or later	Yes
Forcepoint DLP Endpoint (Mac)	
v24.03 or later	No, But an account sign out is required

10) If you upgraded Forcepoint DLP Endpoint on a Mac endpoint machine running macOS 10.15 or later, you must enable full disk access, then restart the machine.

Important

The new Forcepoint F1E cannot be downgraded to the older, conventional version (v8.5 or earlier).

If you update to Forcepoint DLP Endpoint v25.xx and need to downgrade to a conventional version, you must manually remove the new Forcepoint DLP Endpoint version before you install the older, conventional version. Forcepoint DLP Endpoint can be downgraded to a previous Forcepoint F1E version (Forcepoint DLP Endpoint v24.x)

Related concepts

Enabling full disk access on macOS

Post endpoint Upgrade on page 26

Enabling full disk access on macOS

For Forcepoint DLP Endpoint agents, you must enable full disk access for certain processes in your mac OS.

When you install or upgrade Forcepoint DLP Endpoint on an endpoint machine running macOS 13 (Ventura), macOS 14 (Sonoma), and macOS 15 (Sequoia), you must enable full disk access (FDA) for the following processes:

- Library/Application Support/Websense Endpoint/DLP/ESDaemonBundle.app
- Library/Application Support/Websense Endpoint/DLP/Websense Endpoint Helper.app
- Library/Application Support/Websense Endpoint/DLP/wsdlpd
- Library/Application Support/Websense Endpoint/EPClassifier/EndPointClassifier

Also, if you install Forcepoint DLP Endpoint v20.12 (or later) or upgrade to v20.12 (or later) on a Mac endpoint machine running macOS 10.x, then upgrade the machine to macOS 11. Forcepoint DLP Endpoint v20.12 (or later) does not work until you enable FDA for the above processes.

You can grant FDA:

- On individual endpoint machines in **System Preferences** > **Security & Privacy** > **Privacy**. If you are upgrading Forcepoint DLP Endpoint manually on an endpoint machine running macOS 11, the installation prompts you to enable FDA.
- On multiple endpoint machines by deploying a configuration file through MDM, such as Jamf. For more information, see Deploying the endpoint package through Jamf in the *Forcepoint F1E Install Guide*.

Deploying Forcepoint F1E Outlook Add in

From version 22.03 onwards, it is required that the Forcepoint F1E Add-in Outlook Feature is deployed to users accounts in order to monitor content on Outlook Clients on macOS. For more information, see the Configuring and deploying Outlook Add-in for Forcepoint F1E.

Enable web file uploads analysis

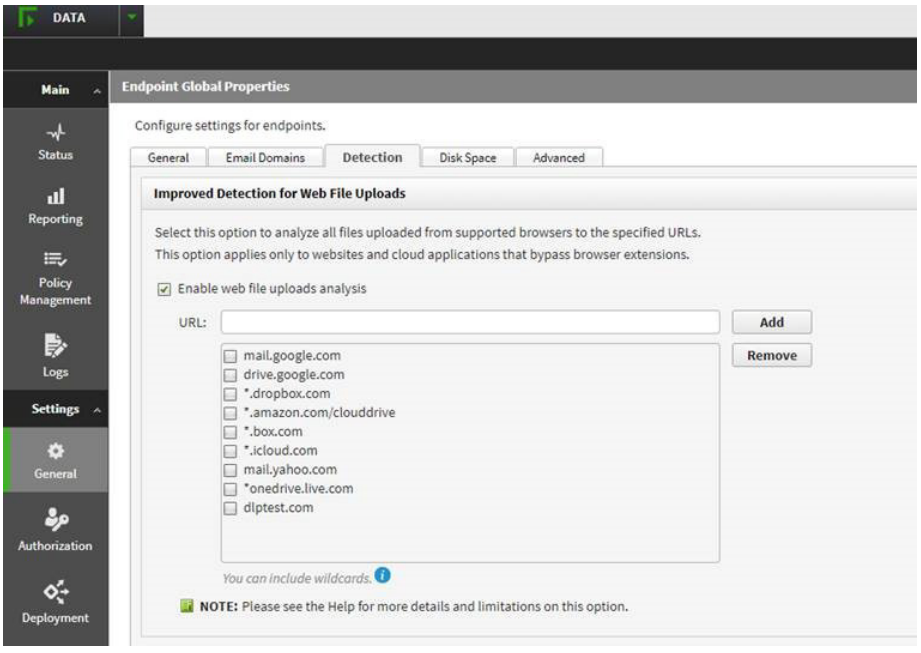
For sites identified that require enhanced file upload detection, enabling web file uploads analysis is required to detect file uploads on the Web channel:

Steps

1) Log on to the Forcepoint Security Manager (FSM) and open the **DATA** module.

2) Go to **Settings** > **General** > **Endpoint**.

3) On the **Detection** tab, select **Enable web file uploads analysis**.



4) Enter the **URL** for the specific domain you want to monitor, then click **Add**. You can add multiple domains. If you want to monitor all domains, enter *, and then click **Add**.

5) Save and deploy the changes.

Automatic software updates

For information about automating software updates for Forcepoint DLP Endpoint through the package builder, see Automatic Updates for Forcepoint DLP Endpoint.

Post endpoint Upgrade

The system provides both name and serial number for each endpoint device, as in "SanDisk Cruzer Blade; 4C530103131102119495".

An easy way to maintain compatibility with previous releases is to add an asterisk (*) to the end of each device name that you have listed in the Forcepoint Security Manager. For example, change "SanDisk Cruzer Blade" to "SanDisk Cruzer Blade*".

If you do not, rules related to the existing endpoint machines may not monitor or enforce the removable media channel as expected. Only exact matches generate an incident.

Chapter 4

Upgrading Forcepoint Endpoint Context Agent

Contents

- Compatibility on page 27
- Forcepoint Endpoint Context Agent Windows deployments on page 28

This chapter covers the steps for upgrading Forcepoint Endpoint Context Agent (Forcepoint ECA) on Windows endpoint machines. If you are upgrading a mixed deployment consisting of two or more Forcepoint F1E agents, see *Upgrading Mixed Deployments*.

Note

If you are working with multiple agent installation, refer to the Forcepoint Agent Compatibility Knowledge Base article.

This chapter covers the following topics:

Related concepts

Upgrading Mixed Deployments on page 31

Forcepoint Endpoint Context Agent Windows deployments on page 28

Related reference

Compatibility on page 27

Compatibility

Forcepoint ECA is recommended for use with these Forcepoint NGFW component versions.

Component	Minimum supported version	Recommended version
Forcepoint NGFW	v6.10	Latest v6.10 maintenance version or later
Forcepoint NGFW Security Management Center (SMC)	v6.10	Latest v6.10 maintenance version or later

If your organization is using Forcepoint NGFW v6.7.0 or earlier, upgrade to Forcepoint NGFW v6.10 (or later) before upgrading Forcepoint ECA to v25.xx.

If you are upgrading from the conventional Forcepoint ECA (v1.4 or earlier) to this version of Forcepoint ECA, you must uninstall the conventional agent before installing this Forcepoint ECA version. For more information, see *Upgrading from a conventional Forcepoint Endpoint Context Agent (v1.4 or earlier)*.

If you are upgrading from an older version of Forcepoint ECA on the Forcepoint F1E platform (v24.03 or later), you do not need to uninstall the older version before upgrading to this version. For more information, see *Upgrading from a newer Forcepoint Endpoint Context Agent (Forcepoint F1E v24.03 or later)*.

Related tasks

Upgrading from a conventional Forcepoint Endpoint Context Agent (v1.4 or earlier) on page 28
Upgrading from a newer Forcepoint Endpoint Context Agent (Forcepoint F1E v24.03 or later) on page 29

Forcepoint Endpoint Context Agent Windows deployments

Important

Forcepoint ECA installation requires local administrator rights on the endpoint machine.

Upgrading from a conventional Forcepoint Endpoint Context Agent (v1.4 or earlier)

To upgrade your existing version of Forcepoint ECA:

Steps

1) Make sure you have Forcepoint NGFW v6.10 or later installed and functioning.

2) Uninstall the earlier version of Forcepoint ECA to remove all Forcepoint ECA files (including the configuration file) from the endpoint machine.

3) Restart the endpoint machine.

4) Download the latest package builder from the Forcepoint Support site:
   a) Log on to the Forcepoint Downloads page.

   b) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.

   c) Select the desired package builder.
   The **Product Installer** view opens.

d) Click **Download**.
A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.

5) Open `ForcepointOneEndpointPackage.zip`.

6) Run `WebsenseEndpointPackageBuilder.exe` to generate a new Forcepoint ECA installation package. You must provide the local folder location for your configuration file in the package builder on the **Profile Path** screen.

7) Deploy the v25.xx installation package to each endpoint machine using one of the methods described in the Forcepoint F1E Installation Guide.

Upgrading from a newer Forcepoint Endpoint Context Agent (Forcepoint F1E v24.03 or later)

Forcepoint ECA could be installed and deployed as part of Forcepoint F1E. If you are upgrading from v24.03 or later, you do not need to uninstall the earlier Forcepoint ECA installed on the endpoint machine.

Steps

1) Make sure you have Forcepoint NGFW v6.10 or later installed and functioning.

2) Download the latest package builder from the Forcepoint Support site:
   a) Log on to the Forcepoint Downloads page.
   b) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.
   c) Select the desired package builder.
   The **Product Installer** view opens.
   d) Click **Download**.

3) Open `ForcepointOneEndpointPackage.zip`.

4) Run `WebsenseEndpointPackageBuilder.exe` to generate a new Forcepoint ECA installation package. You must provide the local folder location for your configuration file in the package builder on the **Profile Path** screen.

5) Deploy the v25.xx installation package to each endpoint machine using one of the methods described in the Forcepoint F1E Installation Guide.

Chapter 5

Upgrading Mixed Deployments

Contents

- Forcepoint F1E compatibility on page 32
- Forcepoint Web Security Endpoint Hybrid, Forcepoint DLP Endpoint, and Forcepoint Endpoint Context Agent deployments on page 32
- Remote filtering and DLP deployments on page 40

This chapter covers the steps for upgrading mixed deployments where more than one Forcepoint F1E agent is installed on the same endpoint machine.

Although this Forcepoint F1E build is v25.xx, it can be used in conjunction with the following Forcepoint products:

Forcepoint F1E agent	Compatible Forcepoint product
Forcepoint DLP Endpoint	Forcepoint DLP v8.9.x or later
Forcepoint Web Security Endpoint	Forcepoint Web Security v8.5.5 or later
Forcepoint Endpoint Context Agent (Forcepoint ECA)	Forcepoint Next Generation Firewall (Forcepoint NGFW) v6.10 or later

You do not need to uninstall the earlier Endpoint version before installing this version if you are upgrading from the following Forcepoint Endpoint versions:

- Forcepoint DLP Endpoint v24.03 or later
- Forcepoint Web Security Endpoint v24.03 or later
- Forcepoint ECA v24.03 or later

If your Forcepoint Endpoint version is earlier than the version listed above, Forcepoint recommends that you upgrade to one of the above versions before upgrading to this version, or uninstall the earlier version before you install this Forcepoint F1E version.

If you are upgrading to Forcepoint ECA v25.xx from a conventional Forcepoint ECA release (v1.4 or earlier), you must uninstall the earlier version of Forcepoint ECA and restart the endpoint machine before installing this version.

Important

The new Forcepoint F1E cannot be downgraded to the older, conventional version (v8.x).

If you update a Forcepoint F1E agent and need to downgrade to an earlier version, you must manually remove the new Forcepoint F1E version before you install the older, conventional version.

This chapter covers the following topics:

Related concepts

Forcepoint Web Security Endpoint Hybrid, Forcepoint DLP Endpoint, and Forcepoint Endpoint Context Agent deployments on page 32

Remote filtering and DLP deployments on page 40

Related reference
Forcepoint F1E compatibility on page 32

Forcepoint F1E compatibility

Most Forcepoint F1E agents can be installed together on the same endpoint machine. However, there are a few scenarios where agents cannot be installed together. The following table shows which agents can be installed together.

	DLP EP	DCEP	PCEP	RF	ECA
DLP EP		✓	✓	✓	✓
DCEP	✓				
PCEP	✓				✓
RF	✓				
ECA	✓		✓		

Forcepoint Web Security Endpoint Hybrid, Forcepoint DLP Endpoint, and Forcepoint Endpoint Context Agent deployments

Upgrade steps for Windows

Note

If you are working with multiple agent installation, refer to the Forcepoint Agent Compatibility Knowledge Base article.

Create a new endpoint installation package using the Forcepoint Endpoint package builder

1) Download the latest package builder from the Forcepoint Support site:

   a) Log on to the Forcepoint Downloads page.

   b) Do one of the following:
   - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
   - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
   - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.

   c) Select the desired package builder.
   The **Product Installer** view opens.

   d) Click **Download**.
   A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.

2) Before you create an installation package, complete the following agent-specific tasks:
   - Forcepoint DLP Endpoint:
     - You must be logged on to the Forcepoint DLP server with a Service Account before you run the package builder. Otherwise, incorrect communication keys are created and Forcepoint DLP Endpoint cannot connect to the Forcepoint DLP server.
     - You must copy the Endpoint Classifier files from `ForcepointOneEndpointPackage.zip` to the `C:\Program Files (x86)\Websense\Data Security\client` folder. For more information about this step, see *Forcepoint DLP Endpoint Windows and Mac deployments*.

     Important

     Due to a compatibility issue with older Windows Endpoint Classifier files, you must use the Windows Endpoint Classifier files provided in this ZIP file when you build a Windows Forcepoint DLP Endpoint installation package using this package builder.

     If you use older Windows Endpoint Classifier files, the package builder shows an error message and does not build an installation package.
   - Forcepoint ECA:
     - Verify that you have the configuration file you used when you created the previous Forcepoint ECA package.

3) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.

4) On the **Select Endpoint Components** screen, select **two or more** of the following:
   - **Forcepoint Web Security Endpoint**
   - **Forcepoint DLP Endpoint**
   - **Forcepoint Endpoint Context Agent**

5) If you selected **Forcepoint Web Security Endpoint** above, select one of the options below:
   - **Direct Connect Endpoint** (not available with Forcepoint ECA)

- **Proxy Connect Endpoint**

6) Choose **Windows 64-bit** when prompted.

7) Complete the configuration for each selected component in the installation wizard to create the installation package.
For more information about configuring the components, see the Forcepoint F1E Installation Guide.

Important

If the conventional Forcepoint ECA (v1.4 or earlier) is installed, uninstall it before deploying the new Forcepoint F1E installation package. If you do not uninstall the conventional Forcepoint ECA software, the new Forcepoint F1E software may not open correctly.

8) Deploy the installation package to each endpoint machine manually, or using GPO, SMS, or a similar deployment method, as described in the Forcepoint F1E Installation Guide.
For information about how to upgrade Remote Filtering Client, see the *Upgrading the Remote Filtering Client* section of Deploying the Remote Filtering Module.

Note

- Forcepoint Web Security Direct Connect Endpoint end users must join your organization's domain on the endpoint machine. If the end user has not joined and connected to your domain, the disposition server test fails.
- If you deploy Forcepoint F1E using GPO, do not restrict access to the command prompt.

9) After you finish the upgrade, you may need to restart the endpoint machine:

Upgrade from	Restart Required?
Forcepoint DLP Endpoint	
v8.3 and earlier	Yes You must uninstall Forcepoint DLP Endpoint v8.3 and earlier, then restart the endpoint machine before installing this version.
v8.4 and later	Yes
Forcepoint Proxy Connect Endpoint	
v8.3 and earlier	Yes You must uninstall Forcepoint Proxy Connect Endpoint v8.3 and earlier, then restart the endpoint machine before installing this version.
v8.4 and later	Yes
Forcepoint Direct Connect Endpoint	
v8.3 and earlier	Yes You must uninstall Forcepoint Direct Connect Endpoint v8.3 and earlier, then restart the endpoint machine before installing this version.

Upgrade from	Restart Required?
v8.4 and later	Yes
Forcepoint ECA	
v1.4 and earlier	Yes You must uninstall Forcepoint ECA v1.4 and earlier, then restart the endpoint machine before installing this version.
v24.03 and later	Yes

Automatic software updates

To automate software updates for Forcepoint DLP Endpoint or combined Forcepoint DLP Endpoint/Forcepoint Web Security Endpoint through the package builder, see Automatic Updates for Forcepoint DLP Endpoint for details.

Related concepts
Forcepoint DLP Endpoint Windows and Mac deployments on page 22

Upgrade steps for Mac

Steps

1) Download the latest package builder from the Forcepoint Support site:
   a) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.

   b) Select the desired package builder.
   The **Product Installer** view opens.

   c) Click **Download**.
   A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.

2) Before you create the Forcepoint DLP Endpoint installation package:
   - You must be logged on to the Forcepoint DLP server with a Service Account before you run the package builder. Otherwise, incorrect communication keys are created and Forcepoint DLP Endpoint cannot connect to the Forcepoint DLP server.
   - You must copy the Mac Endpoint Classifier file from `ForcepointOneEndpointPackage.zip` to the `C:\Program Files (x86)\Websense\Data Security\client\OS X folder`. For more information about this step, see *Forcepoint DLP Endpoint Windows and Mac deployments*.

3) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.

4) On the **Select Endpoint Components** screen, select both of the following:
   - **Forcepoint Web Security Endpoint** provides web security to your endpoint machines.
   - **Forcepoint DLP Endpoint** for data loss protection.

5) If you selected **Forcepoint Web Security Endpoint** above, select one of the options below:
   - **Direct Connect Endpoint**
   - **Proxy Connect Endpoint**

6) Choose **Mac** when prompted.

7) Complete the configuration in the installation wizard to create the installation package.

8) Unzip the `FORCEPOINT-ONE-ENDPOINT-Mac.zip` package onto your Mac machines.

9) If you had selected Proxy Connect Endpoint for your installer package, edit `endpoint.config` to add the **WSCONTEXT** value.

   The **WSCONTEXT** value is displayed in the GPO script command string on the **Settings** > **Hybrid Configuration** > **Hybrid User Identification** page in the Web Security module of the Forcepoint Security Manager, or the GPO code string under **Deployment Settings** on the **Web** > **Endpoint** > **General** page in the Forcepoint Cloud Security Gateway Portal.

10) Run the `WebsenseEndpoint.pkg` from the unzipped folder EndpointInstaller.

11) Follow the steps in the installation wizard.

12) If you are upgrading to Forcepoint DLP Endpoint v25.xx on macOS 11 (Big Sur) onwards, you are prompted to enable full disk access (FDA) for new processes: Go to `Library/Application Support/Websense Endpoint/EPClassifier/`, select

a) When the installer opens the prompt, click **Open Full Disk Access** to open the macOS System Preferences window.

b) On the **Privacy** tab, select `ESDaemonBundle.app` and `Websense Endpoint Helper.app`.

c) Click the + button under the list.

d) Go to `Library/Application Support/Websense Endpoint/DLP/`, select wsdlpd, then click **Open**.

e) Verify that wsdlpd is included in the list and selected.

f) Click the + button under the list.

g) Go to `Library/Application Support/Websense Endpoint/EPClassifier/`, select **EndPointClassifier**, then click **Open**.

h) Verify that **EndPointClassifier** is included in the list and selected.

i) Close the **Security & Privacy** window.

Note

If you are deploying Forcepoint DLP Endpoint using Jamf, you can enable FDA for these processes using a configuration file. See the *Enabling full disk access on macOS (Forcepoint DLP Endpoint only)* section.

13) You might need to either restart the endpoint machine, or log off and log on again to complete the upgrade.

Upgrade from	Restart Required?
Forcepoint DLP Endpoint	
v8.3 and earlier	Yes You must uninstall Forcepoint DLP Endpoint v8.3 and earlier, then restart the endpoint machine before installing this version.
v8.4 v8.5	Yes
v24.03 and later	No
Forcepoint Proxy Connect Endpoint	
v8.3 and earlier	Yes You must uninstall Forcepoint Proxy Connect Endpoint v8.3 and earlier, then restart the endpoint machine before installing this version.
v8.4 and later	No
Forcepoint Direct Connect Endpoint	
v24.03 and later	No

14) If you upgraded Forcepoint DLP Endpoint on an endpoint machine running macOS 10.15 or later, you must enable full disk access, then restart the machine. For more information, see *Enabling full disk access on macOS 10.15, macOS 11, and macOS 12 (Forcepoint DLP Endpoint only)*.

Related concepts

Forcepoint DLP Endpoint Windows and Mac deployments on page 22
Enabling full disk access on macOS (Forcepoint DLP Endpoint only) on page 38

Enabling full disk access on macOS (Forcepoint DLP Endpoint only)

When you install or upgrade Forcepoint DLP Endpoint on an endpoint machine running macOS 13 (Ventura), macOS 14 (Sonoma), and macOS 15 (Sequoia), you must enable full disk access (FDA) for the following processes:

- Library/Application Support/Websense Endpoint/DLP/ESDaemonBundle.app
- Library/Application Support/Websense Endpoint/DLP/Websense Endpoint Helper.app
- Library/Application Support/Websense Endpoint/DLP/wsdlpd
- Library/Application Support/Websense Endpoint/EPClassifier/EndPointClassifier

Also, if you install Forcepoint DLP Endpoint v20.12 or later or upgrade to v20.12 or later on a Mac endpoint machine running macOS 10.x, then upgrade the machine to macOS 11, Forcepoint DLP Endpoint v20.12 does not work until you enable FDA for the above processes.

You can grant FDA:

- On individual endpoint machines in **System Preferences > Security & Privacy > Privacy**. If you are upgrading Forcepoint DLP Endpoint manually on an endpoint machine running macOS 11, the installation prompts you to enable FDA (see step 11 in the procedure above).
- On multiple endpoint machines by deploying a configuration file through MDM, such as Jamf. For more information, see Deploying the endpoint package through Jamf in the *Forcepoint F1E Install Guide*.

Enable web file uploads analysis

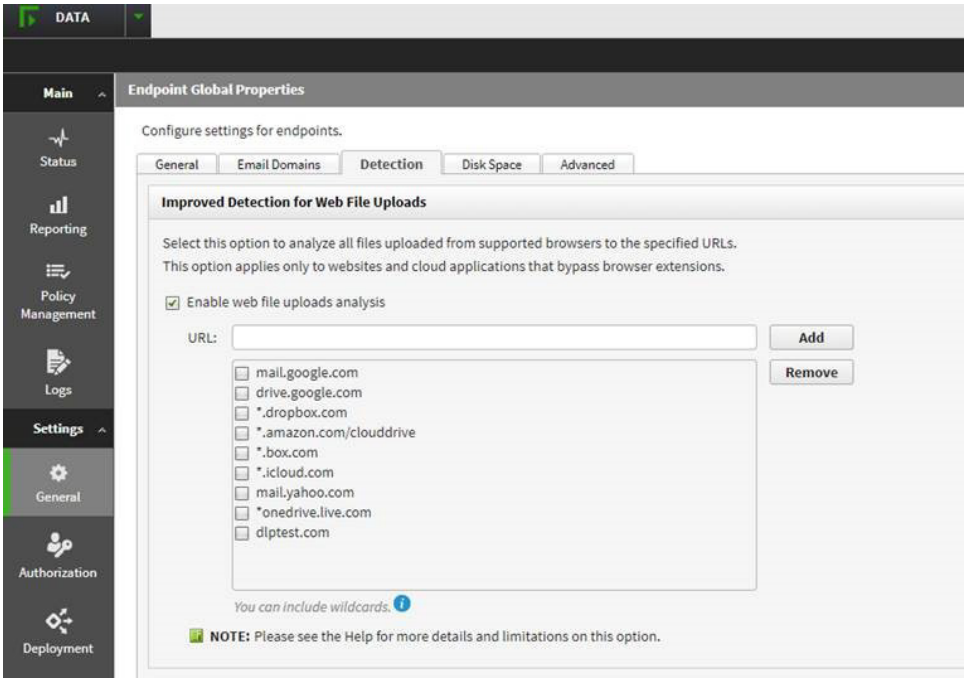
Starting with DLP Endpoint v21.07, the DLP Endpoint will always run enhanced file upload detection on all URLs by default for macOS. This means that the settings in the Forcepoint Security Manager will only apply to Windows Endpoints:

Steps

1) Log on to the Forcepoint Security Manager and open the **DATA** module.

2) Go to **Settings** > **General** > **Endpoint**.

3) On the **Detection** tab, select **Enable web file uploads analysis**.



4) Enter the **URL** for the specific domain you want to monitor, then click **Add**. You can add multiple domains. If you want to monitor all domains, enter *, then click **Add**.

5) Save and deploy the changes.

Remote filtering and DLP deployments

The following are upgrade steps if you are using Remote Filtering Client and Forcepoint DLP Endpoint:

Upgrade steps for Windows

Steps

1) Download the latest package builder from the Forcepoint Support site:
   a) Log on to the Forcepoint Downloads page.
   b) Do one of the following:
      - In **Products** select **Data Loss Prevention (DLP)**, and in **Product Options** select **Endpoint (DLP)**.
      - In **Products** select **Web Security**, and in **Product Options** select **Endpoint (Web)**.
      - In **Products** select **Next Generation Firewall (NGFW)**, and in **Product Options** select **Endpoint (NGFW)**.
   c) Select the desired package builder.
      The **Product Installer** view opens.
   d) Click **Download**.
      A ZIP file named `ForcepointOneEndpointPackage.zip` downloads.
2) Before you create the Forcepoint DLP Endpoint installation package:
   - You must be logged on to the Forcepoint DLP server with a Service Account before you run the package builder. Otherwise, incorrect communication keys are created and Forcepoint DLP Endpoint cannot connect to the Forcepoint DLP server.
   - You must copy the Endpoint Classifier files from `ForcepointOneEndpointPackage.zip` to the `C:\Program Files (x86)\Websense\Data Security\client\OS X folder`. For more information about this step, see *Forcepoint DLP Endpoint Windows and Mac deployments*.
3) Open `ForcepointOneEndpointPackage.zip` and run `WebsenseEndpointPackageBuilder.exe`.
4) On the **Select Endpoint Components** screen, select **both** of the following:
   - **Forcepoint Web Security Endpoint**
   - **Forcepoint DLP Endpoint**
5) Under **Forcepoint Web Security Endpoint**, select **Remote Filtering Client**.
6) Choose **Windows 64-bit** when prompted.
7) Complete the configuration in the installation wizard to create the installation package.

8) Deploy the package to each endpoint machine using GPO, SMS, or a similar deployment method. You can install this version on top of earlier versions without uninstalling the earlier versions.

Important

If you deploy Forcepoint F1E using GPO, do not restrict access to the command prompt. The **Disable the command prompt script processing also?** option should be set to **No**.

9) Restart the endpoint machine after installation is complete.

For more information about using the Forcepoint F1E package builder and installing and deploying Forcepoint F1E solutions, see the Forcepoint F1E Installation Guide.

Related concepts

Forcepoint DLP Endpoint Windows and Mac deployments on page 22

© 2026 Forcepoint