



F1E

26.02

Install Guide

© 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 12 February 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 Introducing Forcepoint F1E	5
About the Product	5
Forcepoint F1E Agent components	5
About this guide	6
Related Materials	6
About Forcepoint F1E	8
Compatibility	11
System requirements	13
2 Obtaining or Creating the Installation Package	19
Preparing for your Forcepoint Endpoint Context Agent installation	20
Downloading Forcepoint Web Security Endpoint installation packages (Cloud deployments)	22
Guidelines for creating an anti-tampering password	23
Creating installation packages from the package builder (On-premises and Hybrid deployments)	24
3 Deploying Forcepoint F1E in your Enterprise	45
Before you begin	45
Deploying Forcepoint F1E Outlook Add-in	47
Windows Installation	58
macOS Installation	66
Restarting an endpoint machine after an install or uninstall	111
Deploying Forcepoint F1E agents and the Neo agent on an endpoint machine	112
Configuring and managing Forcepoint F1E agents	112

Chapter 1

Introducing Forcepoint F1E

Contents

- [About the Product](#) on page 5
- [Forcepoint F1E Agent components](#) on page 5
- [About this guide](#) on page 6
- [Related Materials](#) on page 6
- [About Forcepoint F1E](#) on page 8
- [Compatibility](#) on page 11
- [System requirements](#) on page 13

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

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.

Forcepoint F1E Agent components

This guide covers details on the following F1E agents:

- **Forcepoint Web Security Endpoint** protects users from web threats on Windows and Mac endpoint machines. 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 remediates sensitive data stored on corporate endpoint machines, including Windows and Mac 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 a Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine managed by the Security Management Center (SMC). Forcepoint ECA is only available for Windows endpoint machines. Requires Forcepoint NGFW v6.10 (or later).

About this guide

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

- *Introducing Forcepoint F1E*: Describes system requirements, browser and operating support, benefits, and other information.
- *Obtaining or Creating the Installation Package*: Describes how to obtain or create installation packages.
- *Deploying Forcepoint F1E in your Enterprise*: Describes how to globally deploy Forcepoint F1E software and install it on endpoint machines.



Important

While Forcepoint F1E can be deployed in an enterprise environment using MDM services such as Jamf, Forcepoint does not document the full deployment process for third-party products in our guides. For more information about deploying Forcepoint F1E agents using MDM, please consult the documentation for the individual products.

Related concepts

[Introducing Forcepoint F1E](#) on page 5

[Obtaining or Creating the Installation Package](#) on page 19

Related reference

[Deploying Forcepoint F1E in your Enterprise](#) on page 45

Related Materials

Forcepoint F1E documentation

The following Forcepoint F1E documents are available on the Forcepoint Documentation site:

- [Release Notes for Forcepoint F1E v25.11](#)
This document details the changes implemented in Forcepoint F1E v25.11. Also lists the resolved and known issues in the releases.
- [Upgrade Guide for Forcepoint F1E Solutions](#)
If your organization has deployed an earlier version of Forcepoint F1E, you can upgrade Forcepoint F1E to a later version. This document covers the procedures and identifies compatibility issues if you want to install different agents on the same endpoint machine.
- [End User's Guide for Forcepoint F1E Solutions](#)
End users can interact with the Forcepoint F1E Diagnostics Tool, view connection status, and view collected information. If Forcepoint DLP Endpoint is installed in stealth mode, users cannot interact with the user interface.

Forcepoint Support site and Knowledge Base

You can get additional information and support for your product on the Forcepoint Support website at <https://support.forcepoint.com>. There, you can access product document, Knowledge Base articles, downloads, cases, and contact information.

The Knowledge Base contains many articles that provide additional information about Forcepoint products, along with troubleshooting information. The following articles might help you as you install, deploy, and use Forcepoint F1E:

- [Endpoint Troubleshooting Features Article](#)
- [Deploying the Forcepoint DLP Endpoint Chrome Extension on Mac endpoints using Jamf](#)
- [Excluding Forcepoint Endpoint from Antivirus Scanning](#)
- [Replacing the Message XML in the Forcepoint Endpoint All-in-One Package Builder](#)
- [Updating Confirmation Dialog message files in Forcepoint F1E](#)

Management server installation documentation

Forcepoint F1E solutions rely on other Forcepoint products for server-side functions. If you have not already done so, you must install these products before beginning a Forcepoint F1E installation.

- [Installing Forcepoint DLP](#) (for Forcepoint DLP Endpoint deployment)
 - If you are installing Forcepoint DLP Endpoint, and you plan to install the Neo endpoint agent, follow the procedures in the [Forcepoint Dynamic User Protection Help](#).
- [Installing Forcepoint Web Security](#) (for hybrid Forcepoint Web Security Endpoint deployment)
Web Security installation is not required for a cloud Forcepoint Web Security Endpoint deployment.
- [Installing Forcepoint URL Filtering](#) (for Remote Filtering deployment)
- [Installing Forcepoint Next Generation Firewall](#) (for Forcepoint ECA deployment)



Note

Forcepoint DLP and Forcepoint Web Security are installed as modules on the Forcepoint Security Manager. For more information about the Forcepoint Security Manager, see the [Forcepoint Security Manager Help](#).

Forcepoint F1E configuration documentation

After Forcepoint F1E is deployed to your endpoint machines, you configure it through the server-side product.

- [Forcepoint DLP Manager Help](#) (for Forcepoint DLP Endpoint)
- [Forcepoint Web Security Manager Help](#) (for hybrid Forcepoint Web Security Endpoint deployment)
- [Forcepoint Cloud Security Gateway Portal Help](#) (for cloud Forcepoint Web Security Endpoint deployment)
- [Forcepoint NGFW Online Help](#) (for Forcepoint ECA deployment)

About Forcepoint F1E

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 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 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 agent for Forcepoint Web Security on Windows and Mac.



Note

Note The Remote Filtering Client has not transitioned to the Forcepoint F1E platform. You can build conventional Remote Filtering Client installation packages through this package builder. They will have the same build number (for example, v21.07.5133) as the installation packages created for Forcepoint F1Es.

Do I have a Forcepoint F1E agent or a conventional Forcepoint Endpoint agent?

To determine which type of agent you have, check the following:

- **User Interface branding:** If you have a Forcepoint F1E agent installed, the package builder, Diagnostics Tool, DLP Endpoint UI, and system tray icon are branded as “Forcepoint F1E”.
- **Version number:**
 - **Conventional Forcepoint Endpoint:** The conventional Forcepoint Endpoint agents have a two or three digit version number consisting of a major and minor version. If your Forcepoint DLP Endpoint or Forcepoint Web Security Endpoint agent has a v8.6 or earlier version number, it is a conventional Forcepoint Endpoint agent. If your version of Forcepoint ECA is v1.4 or earlier, it is a conventional agent.
 - **Forcepoint F1E:** The Forcepoint F1E agents have a longer version number that consists of the year, month, and build number. For example, v20.05.4734 is a Forcepoint F1E release created in May 2020. If your agent has a v18 or later version number, it is a Forcepoint F1E agent.
- **Task bar icon:**
 - **Conventional Forcepoint Endpoint:** Each installed Forcepoint Endpoint agent is a single installed product with its own separate icon in the notification area of the task bar (Windows) or the status menu of the menu bar (Mac). If you have more than one Forcepoint Endpoint agent installed on an endpoint machine, there is a separate Forcepoint icon for each agent.
 - **Forcepoint F1E:** All installed Forcepoint F1E agents are installed as a single product (Forcepoint F1E) with different components (i.e., the agents: Forcepoint DLP Endpoint, Forcepoint Web Security Endpoint, or Forcepoint ECA). If you have more than one Forcepoint F1E agent installed on an endpoint machine, there is only one Forcepoint icon. When you click the icon, Forcepoint F1E opens a menu that shows the options for all installed agents. Also, when you move the mouse over the icon, it shows “Forcepoint F1E”.

Forcepoint F1E package builder

The package builder is used by Enterprise IT team members to generate the Forcepoint F1E installation packages that will be installed on Windows and Mac endpoint machines.

The Forcepoint F1E package builder supports the configuration and creation of the following Forcepoint F1E and conventional Forcepoint Endpoint agents:

- Forcepoint DLP Endpoint on Windows and Mac (Forcepoint F1E)
- Forcepoint Web Security Endpoint:
 - Forcepoint Proxy Connect Endpoint on Windows and Mac (Forcepoint F1E)
 - Forcepoint Direct Connect Endpoint on Windows and Mac (Forcepoint F1E)
 - Remote Filtering Client on Windows and Mac (Conventional Forcepoint F1E)
- Forcepoint ECA on Windows only (Forcepoint F1E)



Important

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 latest package builder from the Forcepoint [Downloads](#) page.



Note

When creating the installation package with Package Builder on macOS, you can disable the installation of browser extensions. These extensions should then be deployed using our MDM solution.

Related tasks

[Deploying Chrome extension](#) on page 103

Forcepoint Web Security Endpoint

Forcepoint Web Security Endpoint includes three endpoint agent options:

- Forcepoint Web Security Proxy Connect Endpoint (also known as Forcepoint Proxy Connect Endpoint)
- Forcepoint Web Security Direct Connect Endpoint (also known as Forcepoint Direct Connect Endpoint)
- Remote Filtering Client



Important

You can deploy a mix of Forcepoint Proxy Connect Endpoint, Forcepoint Direct Connect Endpoint, and Remote Filtering Client agents within your organization. However, you can only install one agent option on an individual endpoint machine.

Forcepoint Proxy Connect Endpoint

Forcepoint Proxy Connect Endpoint can be deployed to secure endpoint machines whose Internet activity is managed by the hybrid or cloud service. The Forcepoint Proxy Connect Endpoint agent provides transparent

authentication and enforces the use of hybrid or cloud web protection policies. This software also routes Internet requests to the hybrid or cloud service so that the appropriate policy can be applied.

- Forcepoint Proxy Connect Endpoint redirects HTTP and HTTPS traffic to the hybrid or cloud service with an encrypted token that identifies the user, enabling the correct policy to be applied and reporting data to be correctly logged. No password or other security information is included.
- For supported browsers, Forcepoint Proxy Connect Endpoint manipulates proxy settings in real time. For example, if Forcepoint Proxy Connect Endpoint detects it is at a hotspot, but the user has not finished registration, it removes its proxy settings until the gateway has successfully opened.

You can enable Forcepoint Proxy Connect Endpoint for some or all machines managed by the cloud or hybrid service.

Forcepoint Direct Connect Endpoint

Forcepoint Direct Connect Endpoint routes traffic directly to the Internet and contacts a new endpoint cloud service to determine whether to block or permit a request, perform analysis of traffic content, and/or deliver endpoint configuration. Forcepoint Direct Connect Endpoint is available for both full cloud and hybrid deployments.

Forcepoint Direct Connect Endpoint may be beneficial for roaming users where proxy-type connections are problematic. This includes, for example, websites that do not work well with a proxy, areas where geographic firewalls prohibit the use of proxies, situations where localized content is required regardless of user location, and complex/changing network environments.

When to use Forcepoint Direct Connect Endpoint instead of Forcepoint Proxy Connect Endpoint

The Forcepoint Direct Connect Endpoint is now available alongside the existing Forcepoint Proxy Connect Endpoint. The Forcepoint Proxy Connect Endpoint will continue to be available and supported and remains the default solution for securing roaming users in most situations.

The Forcepoint Direct Connect Endpoint extends roaming user protection to use cases where a proxy-based approach can be problematic. In general, you should consider using Forcepoint Direct Connect Endpoint if the following applies to your organization:

- Geo-localized content: Localized content is critical; for example, your Marketing organization translates content into many languages.
- Unmanaged/third-party/complex networks: You have complex networks and changing network connections; for example, you have a remote workforce traveling and operating on client sites.
- Geographic firewalls: A geographical firewall prevents proxy use; for example, due to a national firewall or local network security system.
- Frequently changing network conditions: Frequent switching between different network connections; for example using a mix of mobile, wifi and on-prem networks.
- Proxy unfriendly websites: You use a significant number of websites that do not work well with proxy technology and would otherwise require proxy bypass.
- Proxy unfriendly applications: You have non-browser and/or custom applications that require bypasses due to conflicts with proxy technology.

Forcepoint Direct Connect Endpoint and Forcepoint Proxy Connect Endpoint can both be used in the same customer deployment. However, only one type can be installed on an individual endpoint machine.

**Important**

Although Forcepoint Direct Connect Endpoint can provide improved security coverage as outlined in the use cases above, check that the networking requirements and level of feature support are acceptable in your intended deployment.

Remote Filtering Client

In Forcepoint URL Filtering deployments, you can add the Remote Filter module to manage Internet requests from machines outside the network. By default, remote filtering software monitors HTTP, HTTPS, and FTP traffic. You cannot install the Remote Filtering Client on an endpoint machine with either Forcepoint Proxy Connect Endpoint or Forcepoint Direct Connect Endpoint installed.

Forcepoint DLP Endpoint

Forcepoint DLP Endpoint is designed for organizations concerned about data loss that originates at the endpoint machine, whether malicious or inadvertent. For example, if you want to prevent employees from taking sensitive data home on their laptops and printing it, posting to the web, or copy and pasting it, you would benefit from this endpoint solution.

Forcepoint DLP Endpoint is a comprehensive, secure, and easy-to-use endpoint data loss prevention (DLP) solution. It monitors real-time traffic and applies customized DLP policies over application and storage interfaces. You can also apply discovery policies to endpoint machines to determine what sensitive data they hold.

You can monitor user activity inside endpoint applications, such as the cut, copy, paste, print, and screen capture operations. You can also monitor endpoint web activities and know when users are copying data to external drives.

Forcepoint Endpoint Context Agent

Forcepoint ECA is a client application monitoring tool. It intercepts network system calls on Windows endpoint machines and provides user and application information to the Forcepoint NGFW. Forcepoint NGFW uses the information from Forcepoint ECA to determine whether connections from the endpoint machines are allowed, and to monitor end user and endpoint machine activity.

Compatibility

Forcepoint Web Security Endpoint

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

Component	Minimum support 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

Forcepoint DLP Endpoint

Forcepoint DLP Endpoint is recommended for use with the following Forcepoint DLP component versions.

Component	Minimum supported version	Recommended version
Forcepoint DLP Network	v10.x	Latest v10.x maintenance version or later
Forcepoint Data Discovery	v10.x	Latest v10.x maintenance version or later

Forcepoint Endpoint Context Agent




Forcepoint ECA is recommended for use with the following Forcepoint NGFW component versions.

Component	Minimum compatible version	Recommended version
Forcepoint NGFW	v7.1	Latest v6.10 maintenance version or later
Forcepoint NGFW Security Management Center (SMC)	v7.1	Latest v6.10 maintenance version or later

Endpoint compatibility in a mixed deployment

Most Forcepoint F1E agents can be installed together on the same endpoint machine. However, there are a few scenarios where two 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					

System requirements

Hardware requirements

Windows

Windows endpoint machines must meet the following minimum hardware requirements.

- At least i3 or similar (1.8 GHz or above)
- At least 8 GB RAM
- At least 1.5 GB free hard disk space

Mac

Mac endpoint machines must meet the following minimum hardware requirements.

- At least 8 GB RAM
- At least 1.5 GB free hard disk space

Operating system requirements

Endpoint machines must be running one of the operating systems listed in the Forcepoint [Certified Product Matrix](#).

Endpoint virtualization support

Virtual Desktop Infrastructure (VDI) (DLP and ECA only)

Forcepoint DLP Endpoint and Forcepoint ECA can also be installed on endpoint machines running Windows in Virtual Desktop Infrastructure (VDI) environments with limited functionality.

Forcepoint DLP Endpoint can be deployed to a shared server that hosts Citrix XenApp, Citrix XenDesktop, or Citrix Virtual Apps desktop virtualization software. Forcepoint ECA can be deployed to a shared server that hosts Citrix XenDesktop software. Supported versions are listed in the [Certified Product Matrix](#).

AWS End User Computing DaaS (DLP and Proxy Connect Endpoint only)

Forcepoint DLP Endpoint and Forcepoint Proxy Connect Endpoint can also be installed on endpoint machines running AWS End User Computing DaaS (Desktop-as-a-Service). Supported versions are listed in the [Certified Product Matrix](#).

Azure Windows Virtual Desktop DaaS (DLP only)

Forcepoint DLP Endpoint can also be installed on endpoint machines running Azure Windows Virtual Desktop DaaS (Desktop-as-a-Service). Supported versions are listed in the [Certified Product Matrix](#).

Browser support

Forcepoint Web Security Endpoint

For a list of web browsers that fully support the Forcepoint Web Security Endpoint agent on 64-bit operating systems, see the Forcepoint [Certified Product Matrix](#).

Full support means that the browser supports all installation methods, as well as both policy enforcement and proxy manipulation. In addition to enforcing browser traffic, Forcepoint Web Security Endpoint also enforces other Internet-enabled applications.

Forcepoint DLP Endpoint

When Forcepoint DLP analyzes data via the Endpoint HTTP/HTTPS destination, it intercepts HTTP(S) posts as they are being uploaded within the browser. It does not monitor download requests.

Windows endpoint machines using the Forcepoint DLP Endpoint extension for Chrome, Firefox, and Edge Chromium must be joined to your organization's domain.

Forcepoint DLP Endpoint analyzes posts from the browsers listed on the Forcepoint [Certified Product Matrix](#).

Forcepoint DLP Endpoint channel support

Email clients

Forcepoint DLP analyzes all email messages sent from Forcepoint DLP Endpoint users, even if they send them to external web mail services like Yahoo.

On Windows endpoint machines, Forcepoint DLP can analyze endpoint email generated by Microsoft Outlook and IBM Notes. However, rules are not enforced on Notes messages if Notes is configured to send mail directly to the Internet, rather than through the Domino server.

Forcepoint DLP supports the desktop version of Outlook 2010, 2013, and 2016, but not the Windows 8 touch version. Forcepoint DLP supports IBM Notes versions 8.5.1, 8.5.2 FP4, 8.5.3, and 9.

On Mac endpoint machines, Forcepoint DLP can analyze email generated by Outlook 2011, Outlook 2016, and Apple Mail.

Forcepoint DLP can detect incidents in S/MIME encrypted messages sent from Outlook 2013 (Windows), Outlook 2016 (Windows), and Outlook 2016 (Mac).

Printer drivers

You can monitor data being sent from an endpoint machine to a local or network printer. Forcepoint DLP supports drivers that print to a physical device, as well as those that print to file or PDF.

Application controls

You can monitor or prevent sensitive data from being cut, copied and pasted from an application like Microsoft Word or a web browser. This is desirable, because endpoint machines are often disconnected from the corporate network and can pose a security risk.

Forcepoint DLP can monitor cut, copy and paste operations on most browsers, such as Edge, Firefox, Safari, and Chrome.

It can also control access to files. For example, you can monitor uploads to cloud storage clients like DropBox and also VOIP clients like GoToMeeting.

For more information about the applications that Forcepoint DLP can monitor out of the box, see [Applications Monitored in the Endpoint Application channel for Forcepoint DLP Endpoint](#). You can also add custom applications.

Supported removable media

- **Removable media** - You can monitor or prevent sensitive data from being transferred to removable media like thumb drives and external hard drives.

If desired, you can configure Windows endpoint policies to encrypt files being transferred to removable media. Encryption is not supported on Mac endpoint machines.



Note

Forcepoint DLP endpoint only supports flash based removable media devices on Windows endpoints. It does not support SCSI over USB or similar.

Forcepoint DLP Endpoint provides two methods to encrypt sensitive data that is being copied to removable media devices. You can:

- **Encrypt with profile key:** Windows only. Encrypt with a password deployed in the endpoint profile. This option is for users on authorized machines—ones with Forcepoint DLP Endpoint installed—when they try to decrypt files.

Select **Encrypt with profile key** when configuring your action plans for endpoint removable media. The action defaults to permitted on Mac endpoint machines regardless of your action plan setting.

- **Encrypt with user password:** Windows only. Encrypt with a password supplied by the Forcepoint DLP Endpoint user. This option is for users decrypting files from machines without Forcepoint DLP Endpoint installed. Select **Encrypt with user password** when configuring your action plans for endpoint removable media. The action defaults to permitted on Mac endpoint machines regardless of your action plan setting.



Note

macOS only supports password based decryption. A user cannot encrypt files on Windows using a profile key and then decrypt them on macOS.

See [Configuring encryption for removable media](#) in the Forcepoint DLP Administrator Help for more information.

Forcepoint DLP Endpoint supports block and permit actions on file transfers to Windows Portable Devices (WPD), but does not support the encryption of data transferred to a WPD from a Windows endpoint machine.

- **CD/DVD writers** - Forcepoint DLP monitors unencrypted data being copied to native Windows and Mac CD/DVD burner applications. It monitors non-native Windows CD/DVD burner applications as well, but only blocks or permits operations without performing content classification. Non-native CD/DVD blocking applies to CD, DVD, and Blu-ray read-write devices on Windows 8, Windows Server 2012, and Windows Server 2016 endpoint machines.
- **Mobile devices** - On Windows 10 (Creators Update, version 1703 and later), Forcepoint DLP can monitor unencrypted data being copied to mobile devices through the WPD protocol. This allows you to use application file access monitoring on software clients like Apple iTunes and Samsung Kies when needed. Forcepoint DLP Endpoint does not support the encryption of data transferred to a WPD from a Windows endpoint machine.

LAN control

Users commonly take their laptops home and then copy data through a LAN connection to a network drive or share on another endpoint machine. With Forcepoint DLP, you can control LAN operations to protect your data.

Endpoint LAN control is applicable to Microsoft sharing only.

Destination channels by operating system

Endpoint destination support is shown below.

Destination Channel	Windows	macOS
Email	✓	✓
HTTP/HTTPS	✓	✓
Printing	✓	✓
Application control	✓	✓
Removable media	✓	✓
LAN	✓	✓

*The cut, copy, paste, file access, and download operations are not supported for cloud applications on Windows endpoint machines when they are used through a Windows Store browser.

Chapter 2

Obtaining or Creating the Installation Package

Contents

- [Preparing for your Forcepoint Endpoint Context Agent installation](#) on page 20
- [Downloading Forcepoint Web Security Endpoint installation packages \(Cloud deployments\)](#) on page 22
- [Guidelines for creating an anti-tampering password](#) on page 23
- [Creating installation packages from the package builder \(On-premises and Hybrid deployments\)](#) on page 24

For Forcepoint Web Security Endpoint Cloud deployments, download the installation package from the Forcepoint Cloud Security Gateway Portal. For all other onpremises and hybrid deployments, use the Forcepoint F1E package builder to create Forcepoint F1E installation packages.

Before beginning the Forcepoint F1E installation process, you must install the Forcepoint server-side product that is relevant to your environment: Forcepoint DLP, Forcepoint URL Filtering, Forcepoint Web Security (cloud or hybrid), or Forcepoint Next Generation Firewall (Forcepoint NGFW).



Note

The Forcepoint DLP v8.9.x and later installation no longer contains the package builder used to install Forcepoint DLP Endpoint. 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 \(NGFW\)](#)

This chapter covers the following topics:

Related concepts

[Guidelines for creating an anti-tampering password](#) on page 23

[Creating installation packages from the package builder \(On-premises and Hybrid deployments\)](#) on page 24

Related tasks

[Preparing for your Forcepoint Endpoint Context Agent installation](#) on page 20

[Downloading Forcepoint Web Security Endpoint installation packages \(Cloud deployments\)](#) on page 22

Preparing for your Forcepoint Endpoint Context Agent installation

Before you create a Forcepoint Endpoint Context Agent (Forcepoint ECA) installation package and deploy Forcepoint ECA in your organization, you must complete the following procedures before you create the installation package:

Steps

1) Authenticate Forcepoint ECA using client certificates

The Forcepoint NGFW Engine uses a client certificate to authenticate endpoint machines running Forcepoint ECA. In this procedure, you must establish a certificate authority (CA) for Forcepoint ECA, create the client certificate template, then deploy a unique client certificate to each endpoint machine. See *Authenticating Forcepoint ECA using client certificates* for the full procedure.

2) Configure Forcepoint ECA settings in the Security Management Center (SMC)

In this procedure, you must configure the initial Forcepoint ECA settings in the SMC to create a configuration file. This configuration file is added to the installation package through the package builder. See *Configuring Forcepoint Endpoint Context Agent settings in the SMC* for the full procedure.

Related tasks

[Authenticating Forcepoint ECA using client certificates](#) on page 20

[Configuring Forcepoint Endpoint Context Agent settings in the SMC](#) on page 21

Authenticating Forcepoint ECA using client certificates

Using a client certificate, the Forcepoint NGFW Engines authenticate the endpoint machines running Forcepoint ECA. This certificate must be installed on the endpoint machine before installing Forcepoint ECA. Otherwise, the Forcepoint ECA client cannot connect to the Forcepoint NGFW Engines.

Steps

- 1) In the Management Client component of the SMC, establish a CA for Forcepoint ECA in one of the following ways:
 - a) Import your existing Active Directory Certificate Services (AD CS) CA certificates to the SMC, if they have already been used to deploy client computer authentication certificates within your organization. The deployed certificates must have the **Client Authentication** application policy enabled. If such certificates have been deployed to each endpoint machine where the Forcepoint ECA software will be deployed, skip step 2.

- b) In the domain where the Forcepoint ECA clients are located, create a CA, then import the CA to the SMC as a Trusted Certificate Authority element. For more information, see Knowledge Base article [Create a certificate authority for Forcepoint Endpoint Context Agent](#). Forcepoint ECA uses the customer-provided CA to authenticate the endpoint machine and uses the SMC's internal CA to authenticate the NGFW Engines.
- 2) After the CA is established, create a new certificate template in AD CS and enroll it to each endpoint machine where Forcepoint ECA is to be installed. This certificate is required to authenticate the endpoint machine with the Forcepoint NGFW Engines. When you create the certificate template in AD CS, you must select the Client Authentication application policy extension.

**Note**

Note Each endpoint machine must have a unique certificate. Only computer certificates are supported. User certificates are not supported.

After the CA is established and each endpoint machine has a valid client certificate, continue with the configuration steps in the next section.

Configuring Forcepoint Endpoint Context Agent settings in the SMC

These high-level steps provide an overview of the configuration process. For detailed information about configuring the Forcepoint ECA settings in the SMC, see the *Integrating Endpoint Context Agent* chapter in the *Forcepoint Next Generation Firewall Product Guide*. This guide is available for download from the [Forcepoint Documentation](#) page.

Steps

- 1) In the Management Client component of the SMC, create a Forcepoint ECA Configuration element that uses the newly created CA.
- 2) Enable Forcepoint ECA on the NGFW Engine, and use the newly created Forcepoint ECA Configuration element.
- 3) Export the Forcepoint ECA configuration XML file (eca_client_yyyymmdd_hhmmss.xml) from the Engine Editor. This configuration file is added to the installation package through the package builder (see *Forcepoint Endpoint Context Agent*).

The configuration file contains the details of all the NGFW Engines that use the same ECA Configuration element. If additional NGFW Engines are added to the configuration, the updated configuration file is automatically sent to the endpoint machines when they connect to the NGFW Engines.

Related tasks

[Forcepoint Endpoint Context Agent](#) on page 42

Downloading Forcepoint Web Security Endpoint installation packages (Cloud deployments)



Note

- These instructions are only valid for Forcepoint Web Security Endpoint deployments in full-cloud environments (Forcepoint Web Security Cloud). If you plan to deploy other Forcepoint One Endpoint agents, you must use the package builder
- If you are running the newest operating system and browsers, you may be directed to get an update from Forcepoint Tech Support.



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

Steps

- 1) Log on to the Forcepoint Cloud Security Gateway Portal.
- 2) Go to **Web > Endpoint > General**.
- 3) Click **Set Anti-Tampering Password**. You must set an anti-tampering password to enable the package download links. For more information about creating an anti-tampering password, see *Guidelines for creating an anti-tampering password*.
- 4) Select the type of Forcepoint Web Security Endpoint you want to download: **Direct Connect** or **Proxy Connect**. You can deploy a combination of Direct Connect and Proxy Connect Endpoint clients in your organization. However, only one type can be installed on an individual endpoint machine.

Endpoint Client Download

Download the version of endpoint client software you want to install on end-user machines.

Endpoint type: ☒ Proxy Connect 
☐ Direct Connect 

Platform: ▼

Available version:  [1.5.8.5.2826](#)  [Release notes](#) *Supported on Windows 7, 8, 8.1, 10*

- 5) Select a **Platform**. Forcepoint Web Security Endpoint packages are available for Windows 64-bit, and Mac endpoint machines.
- 6) Click the **Available version** number to download the selected package.
 See the [Getting Started Guide for Forcepoint Web Security Cloud](#) for more information about cloud deployments of Forcepoint Web Security Endpoint.

Related concepts

[Guidelines for creating an anti-tampering password](#) on page 23

Guidelines for creating an anti-tampering password

Anti-tampering passwords must meet 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 Cloud Security Gateway 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 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 Cloud Security Gateway Portal), you should not include the ^ character before the special character.

Creating installation packages from the package builder (On-premises and Hybrid deployments)

If you are deploying one or more of the following on-premises or hybrid agents, you must use the Forcepoint F1E package builder to create a custom installation package:

- Forcepoint DLP Endpoint
- Forcepoint Web Security Endpoint (hybrid)
- Remote Filtering Client
- Forcepoint ECA

The Forcepoint F1E package builder is a Windows utility that can create Windows 64-bit, and Mac installation packages. The Linux option is currently unavailable.



Note

The packages created by the Forcepoint F1E package builder are backwards compatible with Forcepoint Security Manager and Forcepoint Web Security v8.5.5 and later, and Forcepoint DLP v8.9.x and later.

The Forcepoint ECA installation package is backwards compatible with Forcepoint NGFW versions 6.10 and later.

Downloading the package builder

You can download the Forcepoint F1E installation package for your endpoint.

Steps

- 1) Log on to the Forcepoint [Downloads](#) page.
- 2) 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)**.

- 3) Select the desired package builder.
The **Product Installer** view opens.
- 4) Click **Download**.
A ZIP file named `ForcepointOneEndpointPackage.zip` downloads. It contains:
 - **The package builder utility:** The Windows utility that creates Windows 64-bit and Mac installation packages.
 - **DLP Endpoint Classifier files:** Configuration files that must be copied to a client sub-folder on the Forcepoint DLP Manager.
 - `EPA64.msi`: The Endpoint Classifier file for Windows 64-bit endpoint machines.
 - `websenseEPClassifier.pkg.zip`: The Endpoint Classifier file for Mac endpoint machines.
 - **Updated endpoint message templates:** If you have deployed Forcepoint DLP Endpoint v19.06 or later and do not see the new messages for the confirmation dialog box (added in v19.06) or message 10010047 (added in v20.09), you might need to replace the default message template. For more information, see the [Updating Confirmation Dialog message files in Forcepoint F1E](#) Knowledge Base article.
If you use a custom message XML file, you need to add your custom XML file to your installation:
 - You can add the custom XML file to the package builder before you create your installation packages. For more information, see the [Replacing the Message XML in the Forcepoint Endpoint All-in-One Package Builder](#) Knowledge Base article.
 - You can install the custom XML file on the Forcepoint DLP server. For more information, see the “Install the new XML file” section in the [Customizing Forcepoint DLP Endpoint client messages](#) Knowledge Base article.

Checking file integrity

Before using the Forcepoint F1E package builder, check that the file has not become corrupted or been changed. Using a corrupted file might cause problems at any stage of the configuration process or use of the system. Check file integrity by generating a checksum of the file and comparing it to the checksum provided by Forcepoint:

Steps

- 1) Log on to the Forcepoint [Downloads](#) page and locate the download listing for the file you want to verify. The checksums are listed in the Details section.
- 2) Open the folder that contains the files to be checked.
- 3) Using your preferred tool, generate a checksum of the downloaded file.
- 4) Compare the displayed output to the checksum listed on the Downloads page. They must match.



Warning

Do not use a file that has an invalid checksum. If downloading the file again does not help, contact [Forcepoint Support](#) to resolve the issue.

Creating the installation package from the package builder

This section lists the steps to create the installation package.

Steps

- 1) (optional) If you are creating an installation package for either Forcepoint ECA or Forcepoint DLP Endpoint, complete the following preparation steps first.

If you are not creating a Forcepoint ECA or Forcepoint DLP Endpoint package, skip to step 2.

- a) **Forcepoint ECA**

Configure Forcepoint ECA in the SMC as described in *Preparing for your Forcepoint Endpoint Context Agent installation*.

- b) **Forcepoint DLP Endpoint**

- 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 machine 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.
- Copy the Endpoint Classifier file from the downloaded ZIP file to the folders specified below:
 - Windows 64-bit: Copy the `EPA64.msi` file into the `C:\Program Files(x86)\ Websense\Data Security\client` folder.
 - Mac: Copy the `WebsenseEPClassifier.pkg.zip` file into the `C:\Program Files (x86)\ Websense\Data Security\client\OS X` folder. If this folder does not exist, create it. You do not need to unzip this file. It is automatically unzipped by the package builder when it creates the new Mac installation package.



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 the installation package.

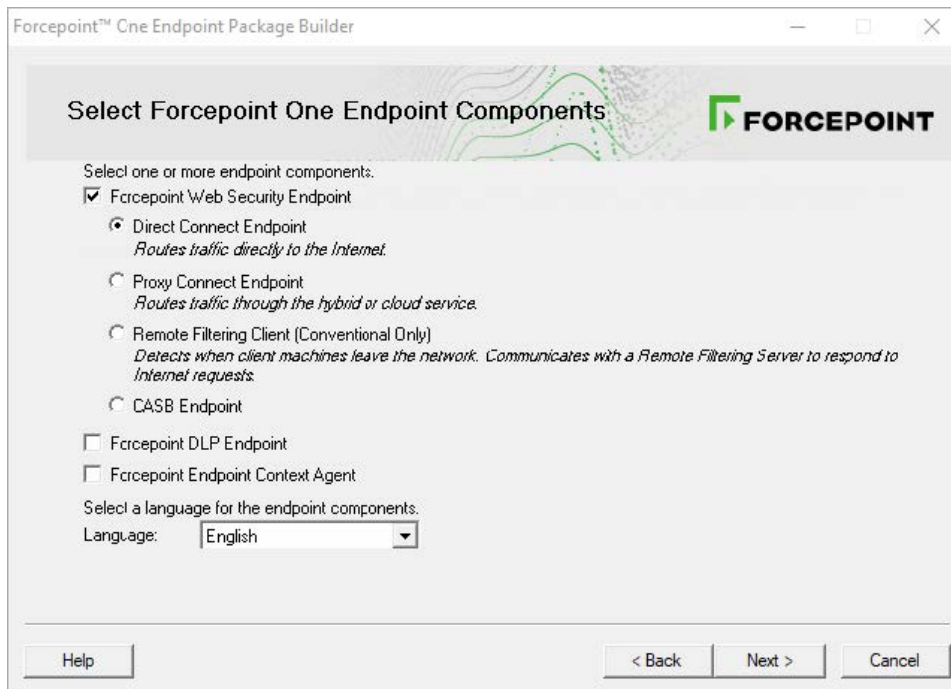
- 2) Launch the Forcepoint F1E package builder:

- a) Open the `ForcepointOneEndpointPackage.zip` file.

- b) Double-click the `WebsenseEndpointPackageBuilder.exe` file.

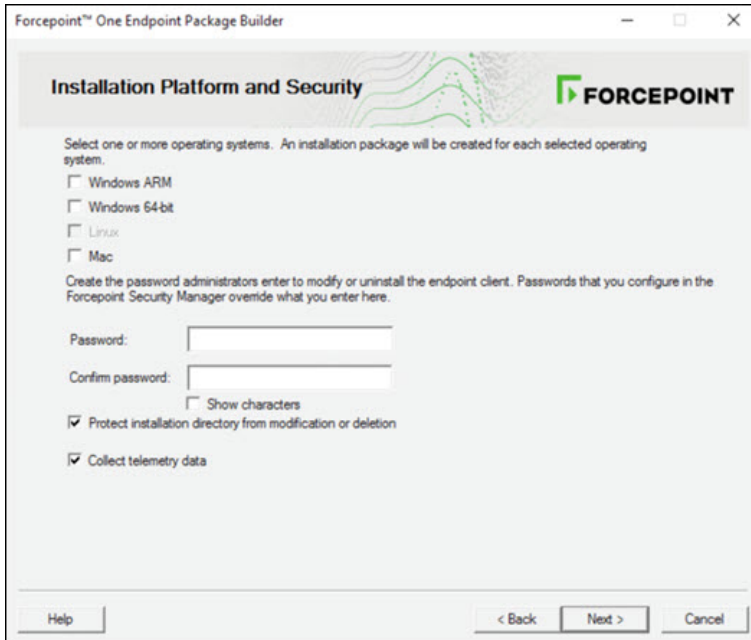
The Forcepoint F1E package builder utility extracts the required files and launches.

- 3) On the **Select Forcepoint One Endpoint Components** screen, select one or more of the following:
- **Forcepoint Web Security Endpoint** (requires Forcepoint Web Security). If you select Forcepoint Web Security Endpoint here, you must select an option in step 4 below.
 - **Forcepoint DLP Endpoint** (requires Forcepoint DLP)
 - **Forcepoint Endpoint Context Agent** (requires Forcepoint NGFW)



- 4) If you selected **Forcepoint Web Security Endpoint**, also select one of the following:
- **Direct Connect Endpoint**: Choose this option to create a Forcepoint Web Security Direct Connect Endpoint installation package for a full cloud deployment (requires Forcepoint Web Security Cloud) or a hybrid cloud/onpremises deployment (requires the Forcepoint Web Security Hybrid Module). Direct Connect Endpoint and Forcepoint ECA cannot be installed together. If you selected **Forcepoint Endpoint Context Agent** above, you cannot select **Direct Connect Endpoint** here.
 - **Proxy Connect Endpoint**: Choose this option to create a Forcepoint Web Security Proxy Connect Endpoint installation package for a full cloud deployment (requires Forcepoint Web Security Cloud) or a hybrid cloud/onpremises deployment (requires the Forcepoint Web Security Hybrid Module).
 - **Remote Filtering Client**: Choose this option to provide remote filtering of endpoint machines (requires Forcepoint URL Filtering).
- 5) Select a language for the client components, then click **Next**.
- In the Forcepoint Security Manager, you can change the language used for displaying messages to Forcepoint DLP Endpoint users, but the language displayed in the user interface (such as buttons, captions, and fields) can only be set during packaging.

- 6) On the **Installation Platform and Security** screen, do the following:



The screenshot shows the 'Forcepoint™ One Endpoint Package Builder' window. The title bar includes standard window controls. The main header is 'Installation Platform and Security' with the Forcepoint logo on the right. Below the header, a text block says: 'Select one or more operating systems. An installation package will be created for each selected operating system.' There are four checkboxes: 'Windows ARM', 'Windows 64-bit', 'Linux', and 'Mac'. Below these, another text block says: 'Create the password administrators enter to modify or uninstall the endpoint client. Passwords that you configure in the Forcepoint Security Manager override what you enter here.' There are two password input fields labeled 'Password:' and 'Confirm password:'. A 'Show characters' checkbox is next to the 'Confirm password:' field. At the bottom of the selection area, there are two checked checkboxes: 'Protect installation directory from modification or deletion' and 'Collect telemetry data'. At the very bottom of the window are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

- a) Select the operating systems (OS) on which Forcepoint F1E will be installed.



Note

You can select Windows ARM only when creating a stand-alone Forcepoint DLP Endpoint package. If you try to install a Windows ARM package on a Windows 64-bit OS, or a Windows 64-bit package on a Windows ARM OS, an error message appears stating that the installation package cannot be run on the system.

- If you are creating a stand-alone Forcepoint Web Security Endpoint package, or a mixed Forcepoint Web Security Endpoint and Forcepoint DLP Endpoint package, you can select Windows 64-bit or Mac.
- If you are creating a stand-alone Forcepoint ECA package, you can only select Windows 64-bit.



Note

The Linux option is unavailable for this release.

- b) Create the administrator password to be used to uninstall or modify Forcepoint F1E agents. If no password is specified, users with admin privileges can uninstall the Forcepoint F1E software from the endpoint machines.

You can click **Show characters** to display the password characters while you type.

For more information about creating an anti-tampering password, see *Guidelines for creating an anti-tampering password*.

For security purposes, anyone who tries to modify or uninstall Forcepoint DLP Endpoint or Forcepoint Web Security Endpoint software is prompted for a password. Standalone Forcepoint ECA installations are not affected by this password.

When Forcepoint F1E contacts the management server, this password is overwritten with the password specified by an administrator on the server. Set this password in one of the following locations:

- Forcepoint DLP Endpoint: In the Data Security module of Forcepoint Security Manager, go to **Settings > General > System > Endpoint**, then on the **General** tab, select **Enable endpoint administrator password** and enter and confirm a password.
- Forcepoint Web Security Endpoint (Hybrid module): In the Web Security module of Forcepoint Security Manager, go to **Settings > Hybrid Configuration > Hybrid User Identification**, then enter and confirm a password.
- Forcepoint Web Security Endpoint (Cloud module): In the Forcepoint Cloud Security Gateway Portal, go to **Web > Endpoint > Deployment Settings > Set Anti-Tampering Password**, then enter and confirm a password.

Note that password hashes are stored in an encrypted file. The system does not store passwords in plain text.



Note

Customers requiring FIPS compliance can set the antitampering password during the Forcepoint DLP Endpoint installation only (Windows and Mac). The anti-tampering password cannot be set on the Forcepoint DLP server. Customers who do not require FIPS compliance are not impacted by this change.

- c) To enable anti-tampering, click **Protect installation directory from modification or deletion**. This prevents users from deleting or modifying the folder where Forcepoint F1E is installed.



Note

Forcepoint recommends that all Forcepoint Web Security Direct Connect Endpoint installation packages enable antitampering on this screen. If anti-tampering is not enabled, some diagnostics tests do not work correctly in the Diagnostics Tool.

- d) To enable the collection of telemetry data, click **Collect telemetry data**. When you enable this option, Forcepoint F1E collects data about the Forcepoint One Endpoint installation (such as status) and the endpoint machine (such as OS, memory, and CPU information), then sends the data back to Forcepoint for analysis.



Important

Starting in Forcepoint F1E v20.12, the **Collect telemetry data** option is enabled by default.

- e) When you are finished, click **Next**.

7) On the **Installation Path and Firefox Settings** screen, do the following:

Forcepoint™ One Endpoint Package Builder

Installation Path, Firefox, and Active Directory Settings

On Mac OS X machines, endpoint client software is installed in the /Applications directory.

For Windows machines, specify where to install endpoint client software:

- ☒ Use default location (%ProgramFiles%\WebSense\WebSense Endpoint)
- ☐ Use this location:
- ☒ Perform Print Detection with Browser Extension (Windows Endpoint only)
- ☐ Use custom Firefox preference files
- Preference file name(.js file):
This file should be located in %ProgramFiles%\Mozilla Firefox\defaults\pref\
- Config file name(.cfg file):
This file should be located in %ProgramFiles%\Mozilla Firefox\
- ☐ Specify default Active Directory domain name (Mac Endpoint only)
Default domain:
- ☐ Disable Chrome Extension (Mac Endpoint only)
- ☐ Disable Firefox Extension (Mac Endpoint only)

Buttons: Help, < Back, Next >, Cancel

- a) Specify the folder where the Forcepoint F1E software will be installed on each Windows endpoint machine. The folder path must contain only English characters.
- **Use default location:** The Forcepoint F1E software is installed in the default folder: \Program Files \WebSense\WebSense Endpoint (*Windows*).
 - **Use this location:** Manually type the installation path for the Forcepoint F1E software. Environment variables are supported.

If you are creating a Mac only installation package, this screen is not shown. On Mac endpoint machines, the Forcepoint F1E software is automatically installed in the /Applications folder.

- b) To disable print functionality using the browser extension on Windows, clear the **Perform Print Detection with Browser Extension (Windows Endpoint only)** checkbox.
- By default, this option is selected to enable print detection through the browser extension.



Note

Print detection for web pages with browser extensions is done by taking a snapshot of the content of the web page that may be printed for analysis. If print actions take place, the Endpoint decides if the action should be blocked or allowed based on the scan result. This content snapshot needs to be transferred from the browser extension to the endpoint via a local download in the background. This can result in a scenario where other applications that track downloads get increased log entries for downloads where the user did not perform the action but rather the agent did. If you are using such applications, you may want to select this option.

- c) If you use custom Firefox preference files within your organization, select **Use custom Firefox preference files**.

In the **Preference file name** field, type the name of the custom preference file (for example, `autoconfig.js`). This file should be located in `C:\Program Files\Mozilla Firefox\defaults\pref\`. If the custom file is not in this folder, Forcepoint F1E cannot use it.

In the **Config file name** field, type the name of the custom configuration file (for example, `mozilla.cfg`). This file should be located in `C:\Program Files\Mozilla Firefox\`. If the custom file is not in this folder, Forcepoint F1E cannot use it.



Note

If you use custom Firefox preference files and do not add them here, the Forcepoint F1E installation process overwrites your custom files.

- d) Only for users with Mac Endpoint machines:
- i) Specify the default domain name of the Active Directory that the Endpoint should use when no Active Directory information is available
 - ii) Select this option if you do not want the installer to add the extensions for these browsers.

- e) Click **Next**.

At this point in the installation, the next screen shown depends on the options selected on the **Select Forcepoint One Endpoint Components** screen. For example, if you selected Forcepoint DLP Endpoint, the next screen is the Server Connection screen.

Follow the instructions for the individual endpoint components below, then continue with *Global Settings*.

Related concepts

[Guidelines for creating an anti-tampering password](#) on page 23

Related tasks

[Preparing for your Forcepoint Endpoint Context Agent installation](#) on page 20

[Forcepoint DLP Endpoint](#) on page 31

[Forcepoint Web Security Direct Connect Endpoint](#) on page 35

[Forcepoint Web Security Proxy Connect Endpoint](#) on page 37

[Remote Filtering Client](#) on page 39

[Forcepoint Endpoint Context Agent](#) on page 42

Forcepoint DLP Endpoint

If you had selected **Forcepoint DLP Endpoint** on the **Select Forcepoint One Endpoint Components** screen, the **DLP Server Connection** screen is displayed after the **Installation Path and Firefox Settings** screen:

Forcepoint™ One Endpoint Package Builder

Forcepoint One Endpoint: DLP Server Connection

Specify the Forcepoint DLP server that will provide initial policy and profile settings.

IP address or hostname:

☐ Receive automatic software updates. (Windows endpoints only)

Specify the URL of the server you will use to stage endpoint updates.

URL:

Example: <http://autoupdate.server.com>

How often should endpoint clients check for updates? minute intervals

Help < Back Next > Cancel

Steps

- 1) In **IP address or hostname**, provide the IP address or hostname of the Forcepoint DLP server that endpoint machines should use to retrieve initial profile and policy information.

When configured, endpoint machines retrieve policy and profile updates from the endpoint server defined in their profiles.

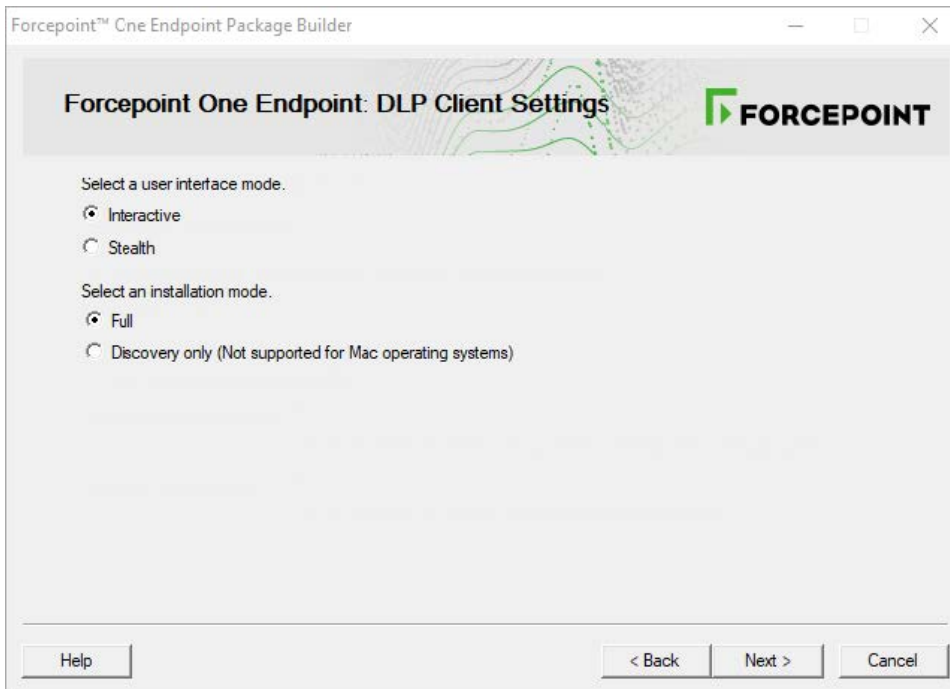


Note

When configuring the Endpoint Profile in the Forcepoint Security Manager (**Data > Settings > Deployment > Endpoint Profiles**), you can change the primary server and configure additional servers for load balancing and/or failover. See [Adding an endpoint profile, Servers tab](#) for details.

- 2) To automate software updates for Forcepoint DLP Endpoint, do the following:
 - a) Prepare a server with the latest updates on it (see [“Automatic updates for Forcepoint F1E \(Forcepoint DLP Endpoint\)”](#) for details).
 - b) Select **Receive automatic software updates**.
 The **Receive automatic software updates** option is for Windows endpoint machines only. When a new version of Forcepoint DLP Endpoint is released, you can upgrade the software on each endpoint machine (manually or via GPO or SMS), or you can configure automatic updates on this screen. You cannot use the auto-update feature in the Web Security module of the Forcepoint Security Manager to automate updates for combined web and DLP endpoints.
 - c) Specify the URL of the server you created. The URL must be HTTP (i.e., <http://>). It cannot be secure HTTP (i.e., <https://>).
 - d) Indicate how often you want endpoint machines to check for updates.

- 3) Click **Next** to view the **DLP Client Settings** screen:




- 4) Select the fields.
- 5) Click **Next**.
- If you are only creating a Forcepoint DLP Endpoint package, the **Save Installation Package** screen appears next. Continue with *Global settings*.
 - If you are creating a package with another agent, continue with the relevant section.

Related tasks

[Global settings](#) on page 44

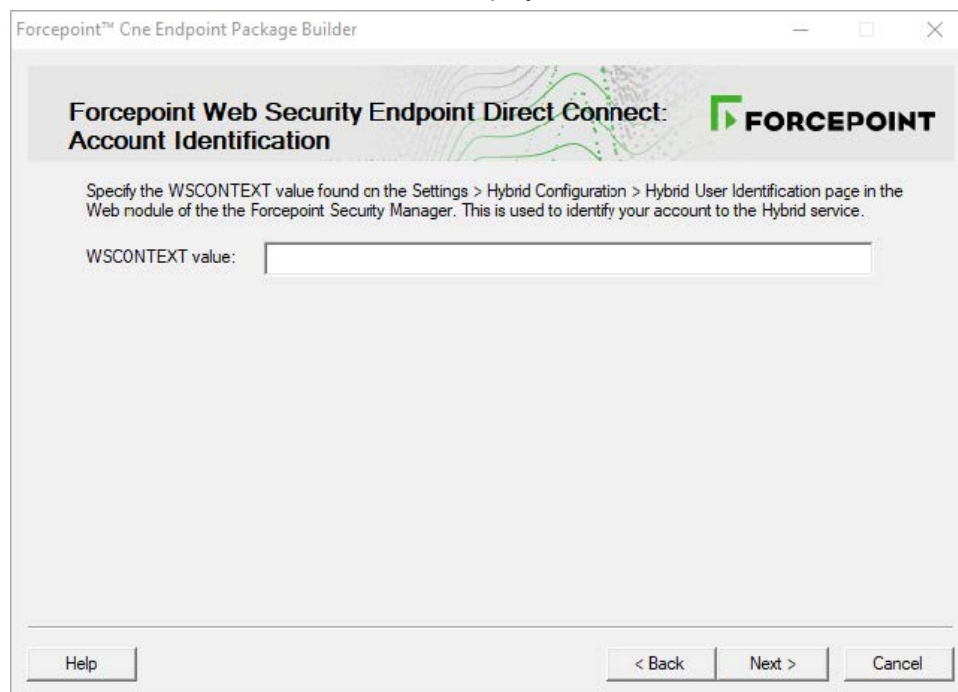
DLP Client Setting fields

User interface mode	<p>Select from the following 2 options:</p> <ol style="list-style-type: none"> 1) Interactive: A user interface is displayed on all endpoint machines. Users know when files have been contained and have the option to save them to an authorized location. 2) Stealth: The Forcepoint DLP Endpoint user interface is not displayed to the user. In this mode, users do not know that Forcepoint DLP Endpoint is operating on their machine. The following features are affected in this mode: <ul style="list-style-type: none"> ■ The Forcepoint DLP Endpoint icon  does not display in the task bar. Users could see the Forcepoint DLP Endpoint installation if they check the Windows Control Panel. ■ Users cannot view the client user interface. As a result, they do not have access to the connection status, the Contained Files viewer, the Log Viewer, or the bypass option. (Experienced users can see contained folders and files in the installation path.) ■ Users do not receive pop-up messages. ■ Although administrators can choose Confirm and Encrypt with user password in the Data Security manager as part of an action plan for the endpoint machine, these are not possible enforcement actions. When these options are selected, operations that violate policy are blocked. The Encrypt with profile key action still takes place, however. ■ When a user attempts to access a blocked page, a 404 error message displays rather than a block page. <p>Because users do not see any notifications, stealth mode is best reserved for discovery tasks and audit-only policies.</p> <p>Note that you must reinstall the endpoint machine and deploy a new profile to switch user interface modes.</p>
----------------------------	---

Installation Mode	<p>Applies to Windows only. Select from the following 2 options:</p> <ol style="list-style-type: none"> 1) Full: Installs Forcepoint DLP Endpoint with full policy monitoring and blocking capabilities upon a policy breach. All incidents are reported in the Forcepoint Security Manager. Full Mode installation requires a restart of the endpoint machine. 2) Discovery Only: Configures Forcepoint DLP Endpoint to run discovery analysis but not data loss prevention. Discovery Only installation does not require a restart.
--------------------------	---

Forcepoint Web Security Direct Connect Endpoint

If you had selected **Direct Connect Endpoint** on the **Select Forcepoint One Endpoint Components** screen, the **Account Identification** screen is displayed after the **Installation Path** and **Firefox Settings** screen:



Forcepoint™ One Endpoint Package Builder

Forcepoint Web Security Endpoint Direct Connect: Account Identification

Specify the WSCONTEXT value found on the Settings > Hybrid Configuration > Hybrid User Identification page in the Web module of the the Forcepoint Security Manager. This is used to identify your account to the Hybrid service.

WSCONTEXT value:

Help < Back Next > Cancel

Steps

- 1) In WSCONTEXT value,** specify the value for your organization's 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. See *Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Cloud Security Gateway Portal (Cloud deployments)* for more information.

2) Click **Next** to view the **Local Block Pages** screen:

On the **Local Block Pages** screen, you can change the description and logo shown at the bottom of the local block pages. Forcepoint Web Security Direct Connect Endpoint uses local block pages when it is in Fallback mode and cannot connect to endpoint services. These pages are only shown when in Fallback mode. If Forcepoint Web Security Direct Connect Endpoint is connected to endpoint services, the default block page is shown.

- a) Click the first **Preview** button to view the local block page with the changes you made at the top of the screen.
- b) Click the second **Preview** button to view the Certificate Error notification page with the changes you made at the top of the screen. The Certificate Error notification page is displayed if you attempt to load a website with an invalid security certificate.

3) Click **Next**.

- If you are only creating a Forcepoint Direct Connect Endpoint package, the **Save Installation Package** screen appears next. Continue with *Global settings*.
- If you are creating a package with another agent, continue with the relevant section.

Related concepts

Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Cloud Security Gateway Portal (Cloud deployments) on page 59

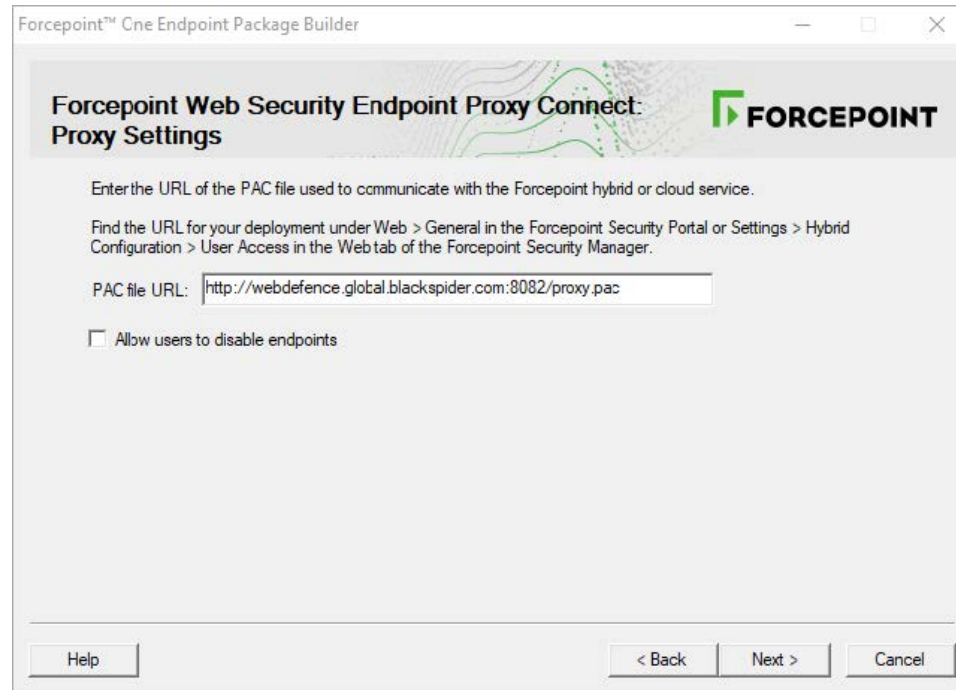
Related tasks

Global settings on page 44

Forcepoint Web Security Proxy Connect Endpoint

You can configure the proxy settings while creating the Forcepoint Proxy Connect installation package.

If you had selected **Proxy Connect Endpoint** on the **Select Forcepoint One Endpoint Components** screen, the **Forcepoint Web Security Endpoint Proxy Connect Proxy Settings** screen is displayed after the **Installation Path and Firefox Settings** screen:



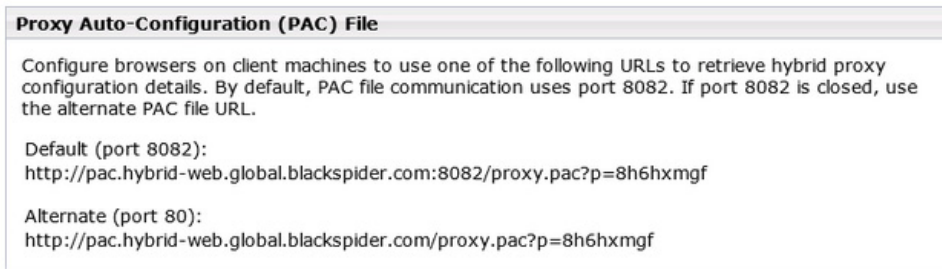
The screenshot shows a window titled "Forcepoint™ One Endpoint Package Builder". The main heading is "Forcepoint Web Security Endpoint Proxy Connect: Proxy Settings". To the right of the heading is the Forcepoint logo. Below the heading, there is instructional text: "Enter the URL of the PAC file used to communicate with the Forcepoint hybrid or cloud service." and "Find the URL for your deployment under Web > General in the Forcepoint Security Portal or Settings > Hybrid Configuration > User Access in the Web tab of the Forcepoint Security Manager." Below this text is a text input field labeled "PAC file URL:" containing the text "http://webdefence.global.blackspider.com:8082/proxy.pac". Below the input field is a checkbox labeled "Allow users to disable endpoints" which is currently unchecked. At the bottom of the window, there are three buttons: "Help", "< Back", and "Next >", and a "Cancel" button.

Steps

- 1) In the **PAC file URL** field, specify the URL for your organization's PAC file. Replace the default URL with the customized URL for your deployment.

- **Hybrid deployments**

For *hybrid* deployments, the URL can be found on the **Settings > HybridConfiguration > User Access** page in the Web Security module of the Forcepoint Security Manager.



Select the URL appropriate for your environment (either port 8082 or port 80). For example: Default (port 8082): `http://pac.hybridweb.global.blackspider.com:8082/proxy.pac?p=8h6hxmfg` Alternate (port 80): `http://pac.hybridweb.global.blackspider.com/proxy.pac?p=8h6hxmfg`

In this example, **8h6hxmfg** is a unique identifier for an organization. Your identifier is different and defines your organization.

Note the difference between the sub-domains of the default PAC file URL and the sample customized URL. The “hybrid-web” sub-domain is used for on-premises Forcepoint Web Security deployments that use Forcepoint Web Security Endpoint.

- **Full cloud deployments**

For *full cloud* deployments, the “webdefence” sub-domain is used. For example, a policy-specific PAC file URL looks something like this:

Default (port 8082): `http://webdefence.global.blackspider.com:8082/proxy.pac?p=8h6hxmfg`
Alternate (port 80): `http://webdefence.global.blackspider.com/proxy.pac?p=8h6hxmfg`

In this example, **8h6hxmfg** is a unique identifier for an organization. Your identifier is different and defines your organization.

You can find policy-specific URLs for your cloud deployment on the **General** tab of a policy in the Forcepoint Cloud Security Gateway Portal. If you would rather use an account-level PAC file, go to the **Web > General** page to find the PAC file URL.

- 2) Select **Allow users to disable endpoints**, if you want to allow users to disable the Forcepoint Web Security Proxy Connect Endpoint web protection on their own endpoint machines.

For example, selecting this option allows users to modify local proxy settings, which can potentially bypass the protections provided by the Forcepoint Web Security Proxy Connect Endpoint software.

- 3) Click **Next**.

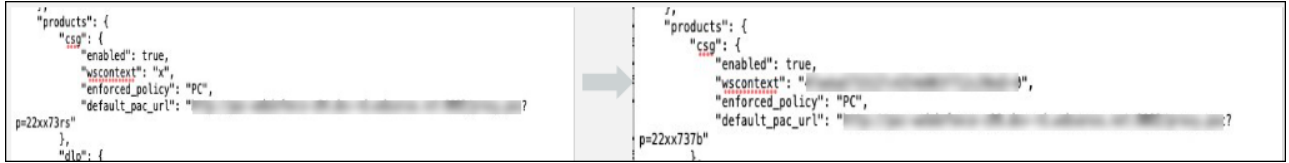
- If you are only creating a Forcepoint Proxy Connect Endpoint package, the **Save Installation Package** screen appears next. Continue with *Global settings*.
- If you are creating a package with another agent, continue with the relevant section.

- 4) If you had selected Proxy Connect Endpoint or Proxy Connect Endpoint with Forcepoint DLP Endpoint for your MAC installer package, do the following:

- a) Unzip the MAC installer package.

- b) Edit `endpoint.config` to add `wscontext`.

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. See *Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Cloud Security Gateway Portal (Cloud deployments)* for more information.



- c) When deploying the F1E package, you can double-click `WebsenseEndpoint.pkg`, and start the installation.

Related concepts

Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Cloud Security Gateway Portal (Cloud deployments) on page 59

Related tasks

Global settings on page 44

Remote Filtering Client

Steps

- 1) Prepare Remote Filtering Server components as described [here](#).

- 2) If you selected **Remote Filtering Client** on the **Select Forcepoint One Endpoint Components** screen, the **Internal Connections** screen is shown after the **Installation Path and Firefox Settings** screen:

The screenshot shows a window titled "Forcepoint™ One Endpoint Package Builder". The main heading is "Remote Filtering: Internal Connections" with the Forcepoint logo to the right. Below the heading, there is a background image of a network map. The text reads: "Specify the internal IP address or hostname and port of each Remote Filtering Server in your deployment. Remote Filtering Client uses this information to determine whether or not it is inside the network." There is a section titled "Internal Connection Details" containing two input fields: "IP address or hostname:" and "Port:". To the right of these fields is a large empty box and a ">" button. Below the large box is a "Remove" button. At the bottom of the window are three buttons: "Help", "< Back", and "Next >", and a "Cancel" button.

- 3) On the **Internal Connections** screen, enter the internal IP address or hostname and internal Port of each Remote Filtering Server to which this client will connect. Use the > button to move the information to the selected list.

Remote Filtering Client sends its heartbeat to these IP addresses and ports to determine whether or not it is inside the network. If you have multiple Remote Filtering Server instances, Remote Filtering Client rotates through the list in order until a functioning server is located.

Remote Filtering Server has a 2-minute inactivity timeout period. If the client connects, and then does not send an Internet request in the timeout period, the server drops the connection. When the next request is made, Remote Filtering Client goes through its list to connect again. This protects server performance by reducing the number of unused connections that might otherwise accumulate.

- 4) When you are finished, click **Next** to show the **External Connections** screen.

- 5) On the **External Connections** screen, enter the external IP address or hostname and internal Port of each Remote Filtering Server. Use the > button to move the information to the selected list. Indicate whether or not to **Log user Internet activity** seen by Remote Filtering Client instances installed using this customized installation package.

The screenshot shows the 'Remote Filtering: External Connections' window. It has a title bar 'Forcepoint™ One Endpoint Package Builder'. The main header area contains the title 'Remote Filtering: External Connections' and the Forcepoint logo. Below the header, there is instructional text: 'Specify the external IP address or hostname and port of each Remote Filtering Server in your deployment. Remote Filtering Client uses this information to forward requests to Remote Filtering Server when it is outside the network.' The main area is divided into two sections. On the left, 'External Connection Details' contains two input fields: 'IP address or hostname:' and 'Port:'. To the right of these fields is a '>' button. Further right is a large empty rectangular box, and to its right is a '->' button. Below the input fields is a checkbox labeled 'Log user Internet activity' which is checked. A 'Remove' button is located below the large empty box. At the bottom of the window are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button on the far right.

- 6) Click **Next** to show the **Trusted Sites** screen.

The screenshot shows the 'Remote Filtering: Trusted Sites' window. It has a title bar 'Forcepoint™ One Endpoint Package Builder'. The main header area contains the title 'Remote Filtering: Trusted Sites' and the Forcepoint logo. Below the header, there is instructional text: 'List any sites that Remote Filtering Client users should be able to access directly, without being filtered or logged. You can use a maximum of 4 regular expressions to define these trusted sites. Example: http://.\\forcepoint\\.com'. Below the text is a large empty rectangular text area. At the bottom right of the text area are three buttons: 'Add', 'Edit', and 'Remove'. At the bottom of the window are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button on the far right.

- 7) Use the **Trusted Sites** list to enter up to 4 URLs, IP addresses, or regular expressions for sites that Remote Filtering Client users can access directly, without being filtered or logged. Click **Add** to enter a URL, IP address, or regular expression.

- 8) Click **Next** to show the **Client Settings** screen.

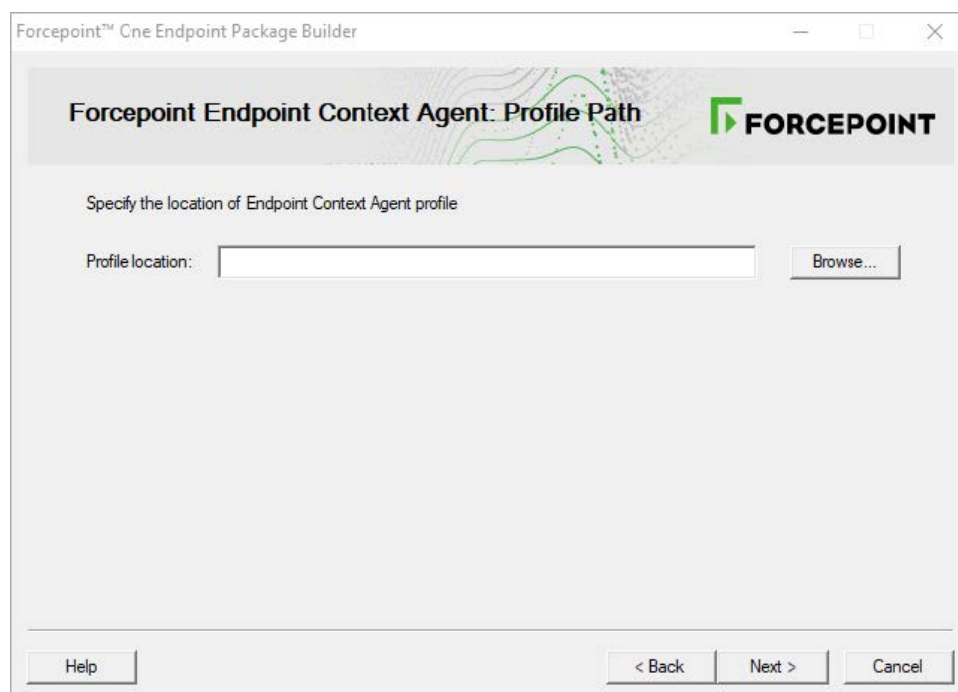
- 9) Indicate whether or not to **Notify users when HTTPS or FTP traffic is blocked**, then, if notifications are enabled, specify how long (in seconds) the message is shown.
Enter and confirm the **Pass phrase** used for communication with the Remote Filtering Server. This must match the pass phrase created when the Remote Filtering Server was installed.
- 10) Click **Next**.
- If you are only creating a Remote Filtering Client package, the **Save Installation Package** screen appears next. Continue with *Global settings*.
 - If you are creating a package with another agent, continue with the relevant section.

Related tasks

[Global settings](#) on page 44

Forcepoint Endpoint Context Agent

If you had selected **Forcepoint Endpoint Context Agent** on the **Select Forcepoint One Endpoint Components** screen, the **Profile Path** screen is displayed after the **Installation Path** and **Firefox Settings** screen:



Steps

- 1) Enter the location where you saved the Forcepoint ECA configuration file (XML file). Either manually enter the folder path to the file or click **Browse** to find the location.
The package builder can accept a configuration file with any filename, not just the `eca_client_yyyymmdd_hhmmss.xml` filename. The configuration file is automatically renamed to `eca.conf` by the package builder when it creates the installation package.
For more information about creating the configuration file, see *Preparing for your Forcepoint Endpoint Context Agent installation*.
- 2) Click **Next**.
 - If you are only creating a Forcepoint ECA package, the **Save Installation Package** screen appears next. Continue with *Global settings*.
 - If you are creating a package with another agent, continue with the relevant section below.

Related tasks

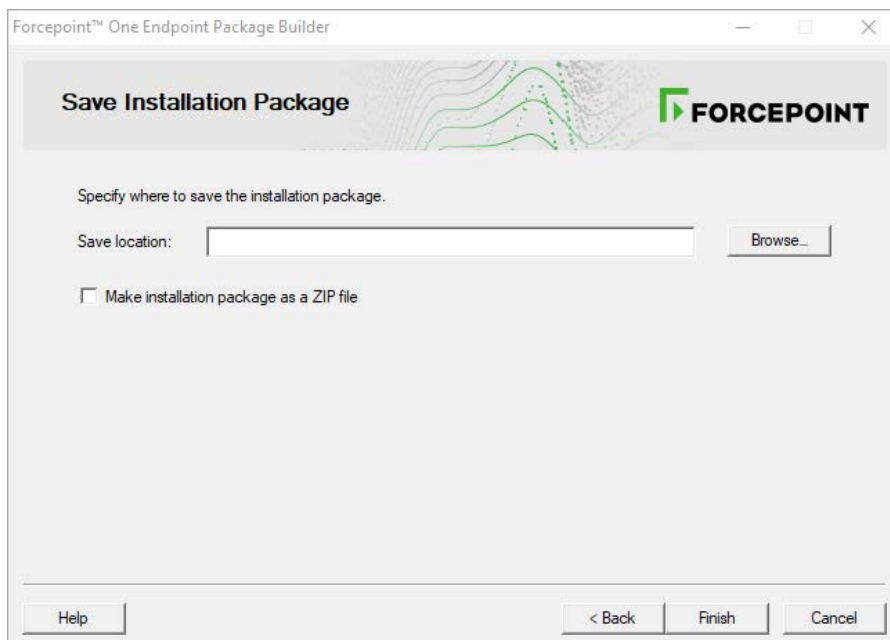
[Global settings](#) on page 44

[Preparing for your Forcepoint Endpoint Context Agent installation](#) on page 20

Global settings

Steps

- 1) When you are done configuring your individual Forcepoint F1E agent selections, the **Save Installation Package** screen is shown. Enter a folder path where the installation package is saved to the local machine.



Either manually enter a path or click **Browse** to find the location.

- 2) Click **Finish**.
If the package is created successfully, a system message is shown.
If the creation of the package fails, an error message is shown. If this happens, contact [Forcepoint Support](#) for assistance.
- 3) Click **OK**.
The packages are created in the designated path configured on the **Save Installation Package** screen. Refer to *Deploying Forcepoint F1E in your Enterprise* for instructions about distributing the package to the endpoint machines.

Related reference

[Deploying Forcepoint F1E in your Enterprise](#) on page 45

Chapter 3

Deploying Forcepoint F1E in your Enterprise

Contents

- [Before you begin](#) on page 45
- [Deploying Forcepoint F1E Outlook Add-in](#) on page 47
- [Windows Installation](#) on page 58
- [macOS Installation](#) on page 66
- [Restarting an endpoint machine after an install or uninstall](#) on page 111
- [Deploying Forcepoint F1E agents and the Neo agent on an endpoint machine](#) on page 112
- [Configuring and managing Forcepoint F1E agents](#) on page 112

This chapter describes how to deploy Forcepoint F1E software on endpoint machines. It covers the following topics:

Related concepts

- [Before you begin](#) on page 45
- [Windows Installation](#) on page 58
- [macOS Installation](#) on page 66
- [Deploying Forcepoint F1E agents and the Neo agent on an endpoint machine](#) on page 112
- [Configuring and managing Forcepoint F1E agents](#) on page 112

Before you begin

- For best practice, start by deploying and testing Forcepoint F1E software on a few local network machines, then increase to a limited number of remote machines before deploying the software throughout your enterprise.
- Check that your endpoint machines meet the minimum system requirements.
- Verify that you have administrator access rights on the endpoint machine. Forcepoint F1E installation requires local administrator rights.
- Exclude the Forcepoint F1E directories from any antivirus software deployed to the endpoint machines. For a full list, see [Excluding Forcepoint files from antivirus scans](#).
- Ensure the Forcepoint F1E installation path is not encrypted by file and folder encryption software. All folders and files within the installation path must be left unencrypted.
- Forcepoint F1E can be installed on an endpoint machine after the disk has been encrypted using full disk encryption.
- If you are deploying Forcepoint DLP endpoint, disable the auto-update feature in the Web Security module of the Forcepoint Security Manager.

- In Windows, ensure that the Remote Desktop Service is not disabled. If disabled, the tray icon might disappear when switching from one user to other.
- For hybrid web deployments, ensure that your user accounts are synchronized with the hybrid service. To verify, log on to the Web Security module of the Forcepoint Security Manager, and select **Main > Status > Hybrid Service**. It is okay if you have not yet used the hybrid service.

Communication Type	Date and Time
Most recent communication by Sync Service	2013-09-20 12:53:32
Directory information sent by Sync Service	✓ 2013-09-19 16:27:00
Reporting information received by Sync Service	✓ 2013-09-20 12:52:41
Reporting information sent to Log Server	✓ 2013-09-20 12:53:32
Policy information sent by Sync Service	✓ 2013-09-19 16:09:51
Account information sent by Sync Service	✓ 2013-09-19 15:58:01

- For Forcepoint Endpoint Context Agent(ECA) deployments, ensure that there are no network address translation (NAT) devices between the Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine and the endpoint machine.

Related concepts

[System requirements](#) on page 13

Disabling automatic updates for Forcepoint Web Security Endpoint

Steps

- 1) Log on to the Web Security module of Forcepoint Security Manager, and go to **Settings > Hybrid Configuration > Hybrid User Identification**.
- 2) Clear **Enable installation and update of Web Endpoint on client machines**.
- 3) Clear **Automatically update endpoint installations when a new version is released**.
- 4) Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.



Note

At the completion of any update, you must restart the Forcepoint F1E software for the updates to take effect.

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) Open the command line, and run the following command 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-ENDPOINTx64.exe
```

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

- 3) Copy your `DCUserConfig.xml` file into this folder.
- 4) Run the following command from the command line to repack the installation package:

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

- 5) Deploy the updated installation package.

Related concepts

[Windows Installation](#) on page 58

Deploying Forcepoint F1E Outlook Add-in

You must install the F1E Outlook Add-in feature to monitor content when new Microsoft Outlook runs on Windows and macOS.



Note

To monitor content via the Outlook Add-in, the Forcepoint F1E v25.09 Windows or macOS agent must be installed on the system.


The F1E agent leverages the Outlook on-send feature to apply an organizations DLP policy to emails that a user is sending on their endpoint using the Outlook Email client. You must install the Forcepoint Outlook Add-in prior to the installation of the Windows or macOS agent on the endpoint.



CAUTION

When using the **Upload and share** option in new Outlook, files are uploaded to OneDrive and shared via a link. This may expose sensitive data if link access is not properly restricted.

You can add the add-in on the account using the xml file. Refer to the table below to download the file.

File name	Description	Download Link
DLPOfficeAddin_no_mac_schedule_	<ul style="list-style-type: none"> On Windows OS, supports outlook classic and new outlook, and Schedule send. On Mac OS, supports outlook classic and new outlook. Schedule send is not supported. 	DLPOfficeAddin_no_mac
DLPOfficeAddin_no_classic_outlook_	<ul style="list-style-type: none"> On Windows OS, supports new outlook, and Schedule send. On Mac OS, supports new outlook, and Schedule send. <div>  <div> Note Classic outlook is not supported </div> </div>	DLPOfficeAddin_no_classic_outlook

Adding custom Add-in in Outlook Desktop Application

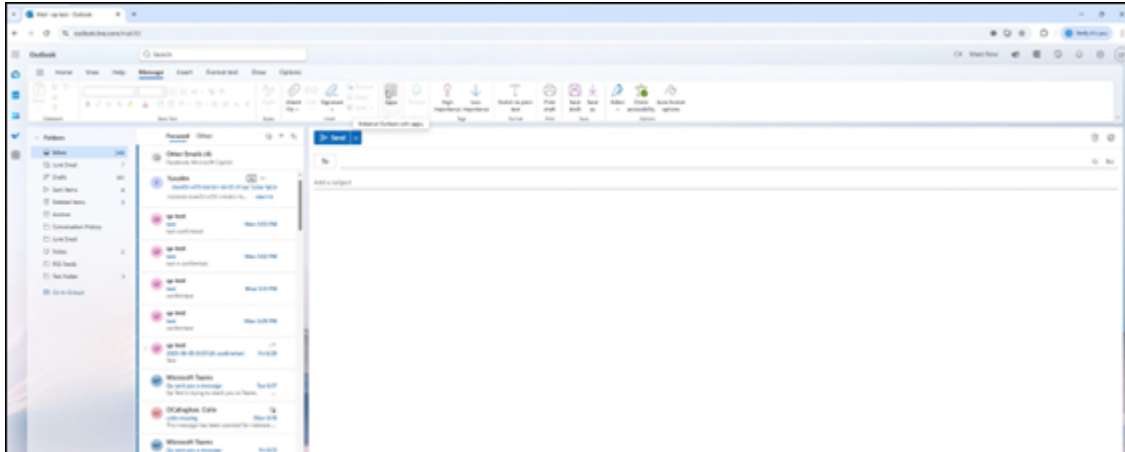
This section outlines the steps required to manually add the add-in to Microsoft Outlook.

You can add the add-in to the Outlook Desktop application using the downloaded xml file.

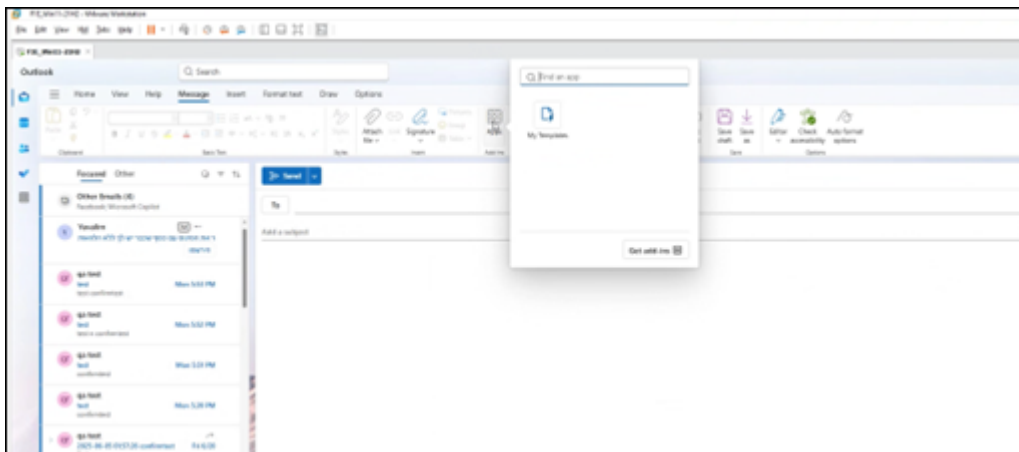
Steps

- 1) Open the new Microsoft Outlook 2016.

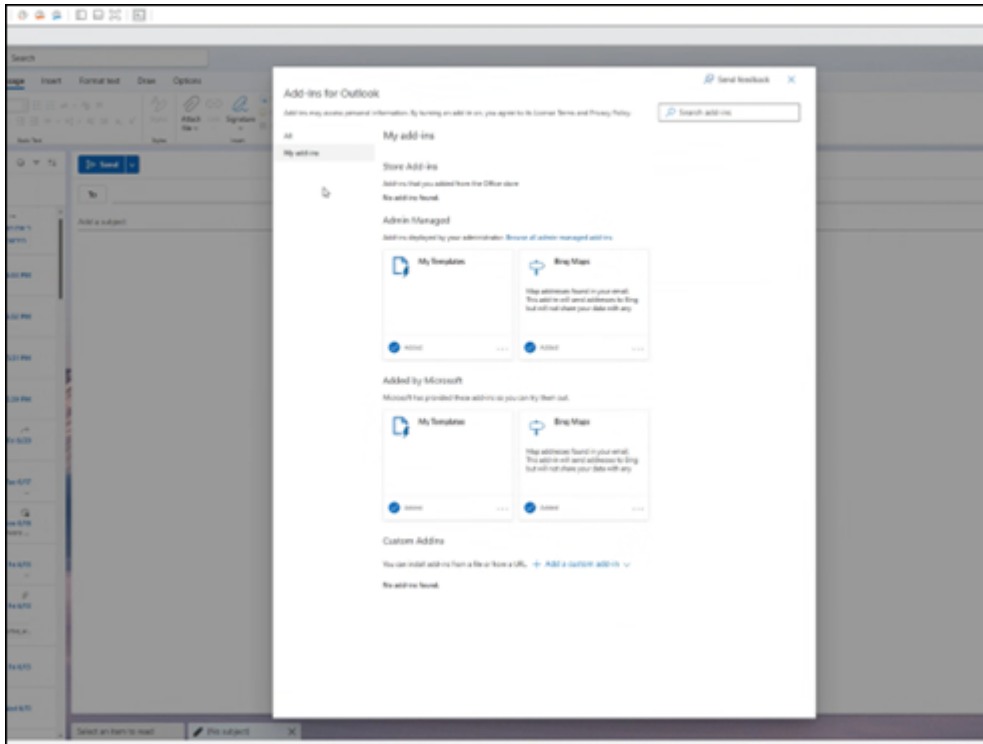
- 2) Go to new Email and then click **Apps**.



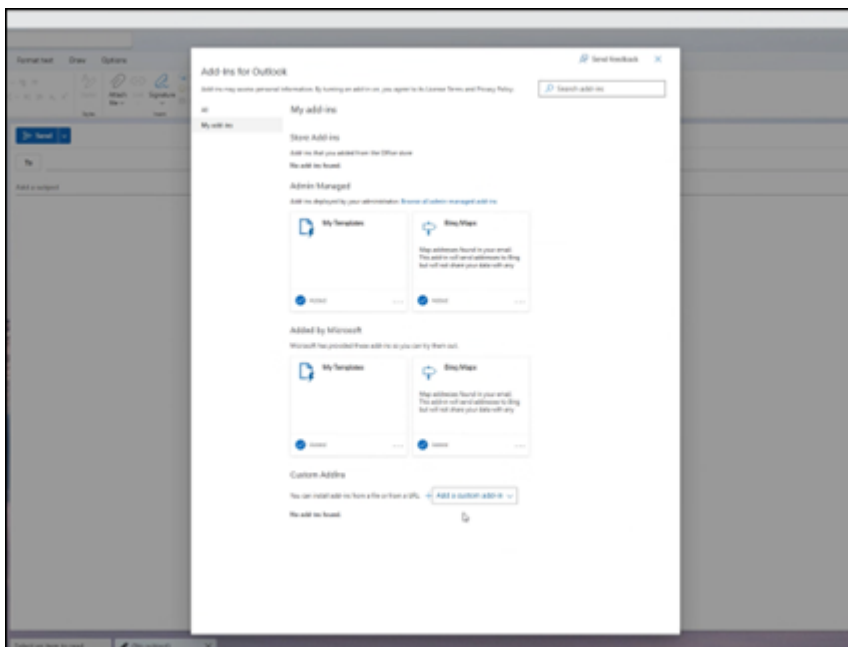
- 3) Click **Get add-ins**.



4) Click **My add-ins**.

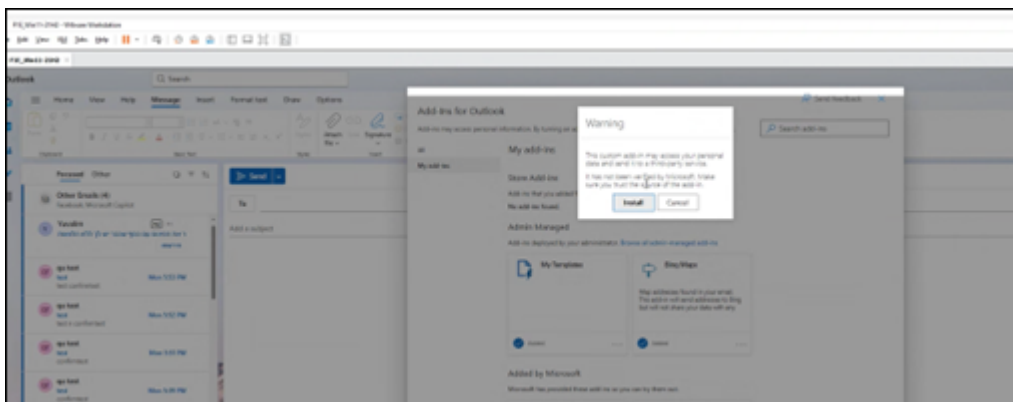


5) Click **Add a custom add-in** and then click **Add from File**.

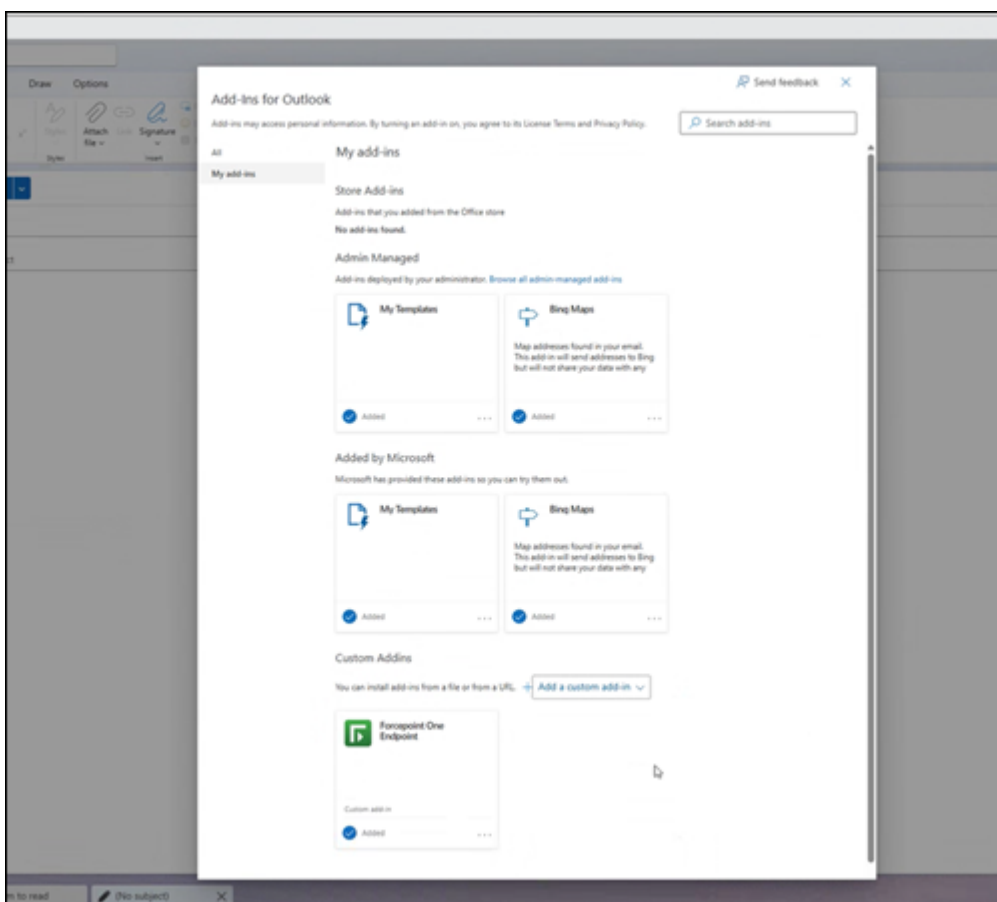


6) Select the downloaded xml file.

7) Click **Install**.



Add-in should be added to the account.



Adding custom Add-in in Outlook Web Application

This section outlines the steps required to manually enable the add-in in Outlook for Web so that it can be used in Outlook Desktop.

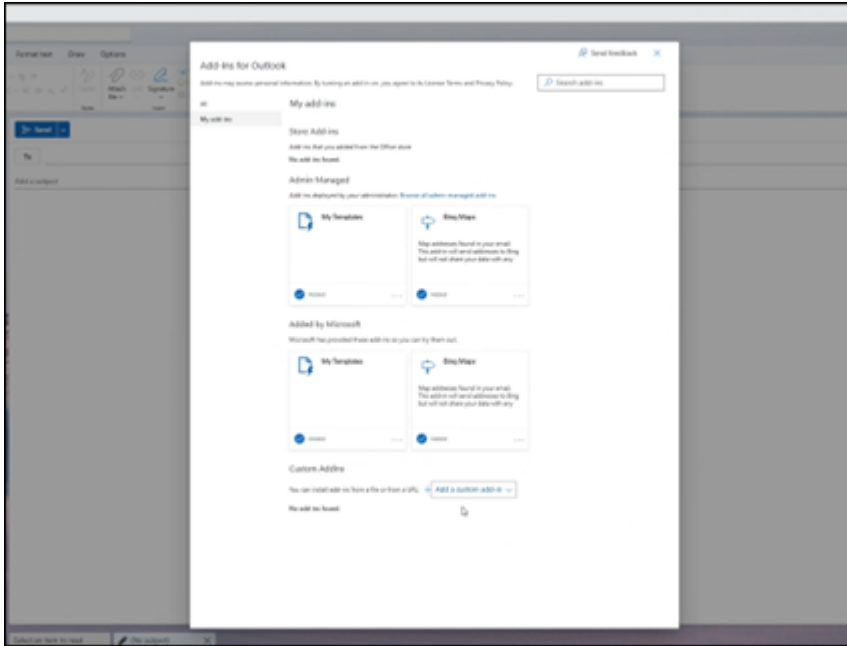
You can add the add-in to the Outlook Web application using the downloaded xml file.

Steps

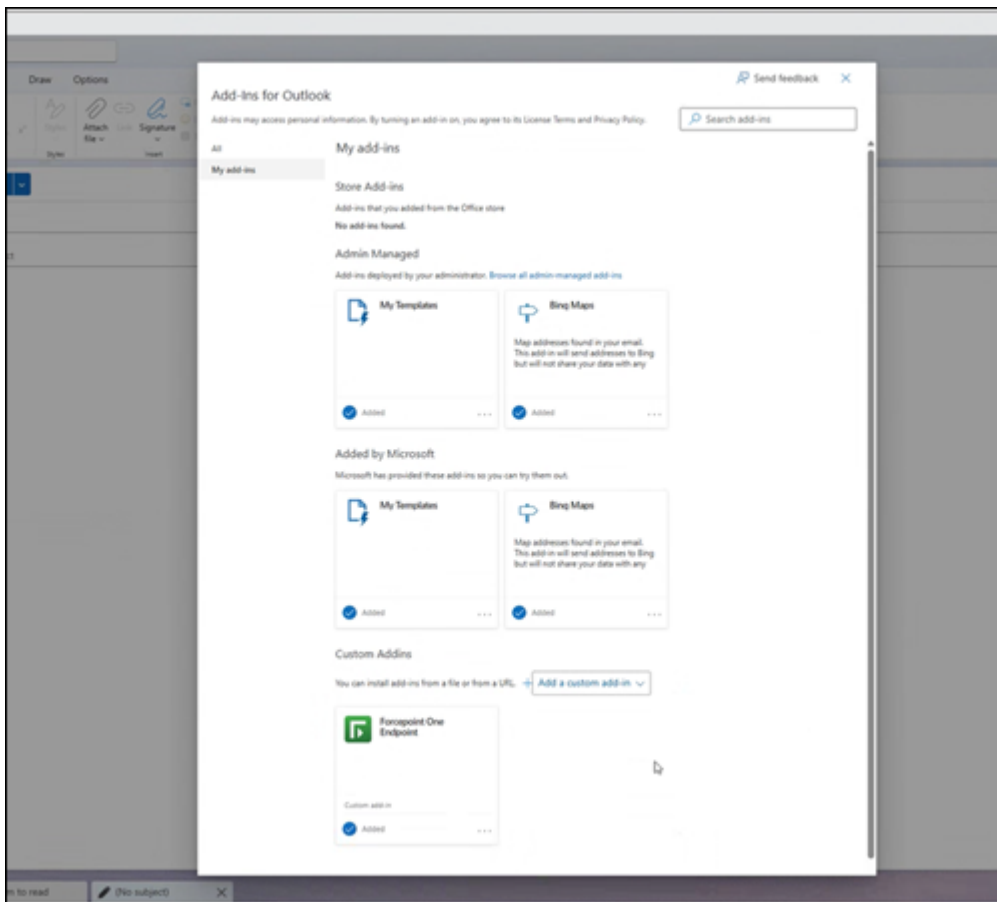
- 1) Navigate to <https://outlook.office.com/mail/> and login using account credentials.
- 2) Once logged in, navigate to <https://outlook.office.com/mail/inclientstore> or <https://outlook.office365.com/owa/?path=/options/manageapps>.

This will bring the user to Add-Ins for Outlook screen.

- 3) Click **Add a custom add-in** and **Add from File**.



- 4) Select the downloaded xml file.
Add-in should be added to the account.



Installing the Add-in using Office 365

You can install the Outlook add-in feature in your Windows or macOS using Microsoft Office 365. You can use the downloaded xml file to install the add-in.



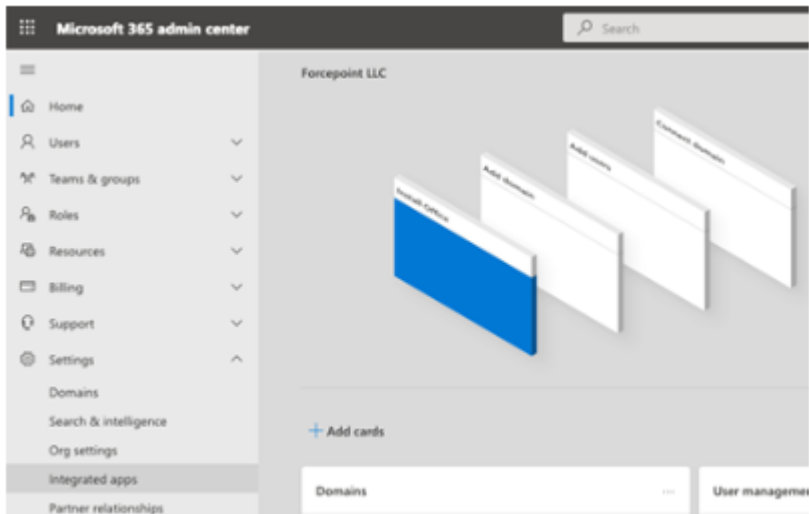
Note

The deployment can take up to six hours and needs to be completed prior to endpoint deployment.

Steps

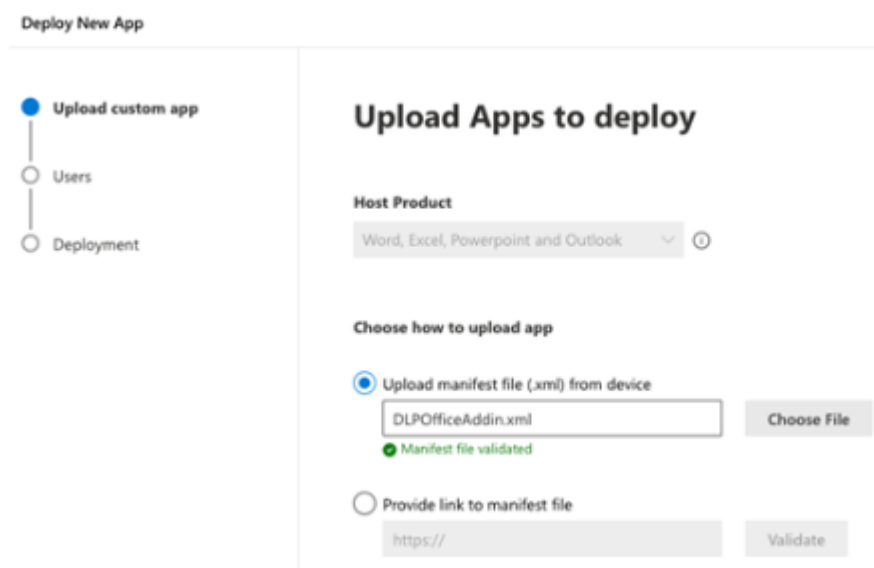
- 1) Open the **Microsoft 365 admin center**.

- 2) In **Settings**, select **Integrated apps**.



You can click **Show All** to see all options.

- 3) In **Upload custom app**, select **Upload manifest file (.xml) from device**, and then choose the xml file.



- 4) Click **Next**.

- 5) Select **Entire organization** or **Specific users/groups** as users, and then click **Next**.

- 6) Accept the permissions requests, and then click **Next**.

- 7) Review and click **Finish** deployment.

- **Note** This step can take up to 6 hours and needs to be completed prior to endpoint deployment.

Deployment completed

Next steps

Test the apps using the following links (if any) to verify that they work as expected.

Forcepoint One Endpoint ● Deployed. It can take up to six hours for the app to appear in Outlook.

Announce this to your users

Studies show that new software is more successfully adopted when users are informed about the software and how to use it. You'll soon receive an announcement email that explains to your users what you deployed and how to get started using the app or solution. Forward this email to your users to improve your adoption rate 2-5x.

[View this deployment](#)

Next Steps

Communication between the Forcepoint agent and the Outlook email client uses HTTPS. Forcepoint recommends creation and use of a specific certificate for use in your environment.

Related tasks

[Creating the Endpoint SSL Identity](#) on page 67

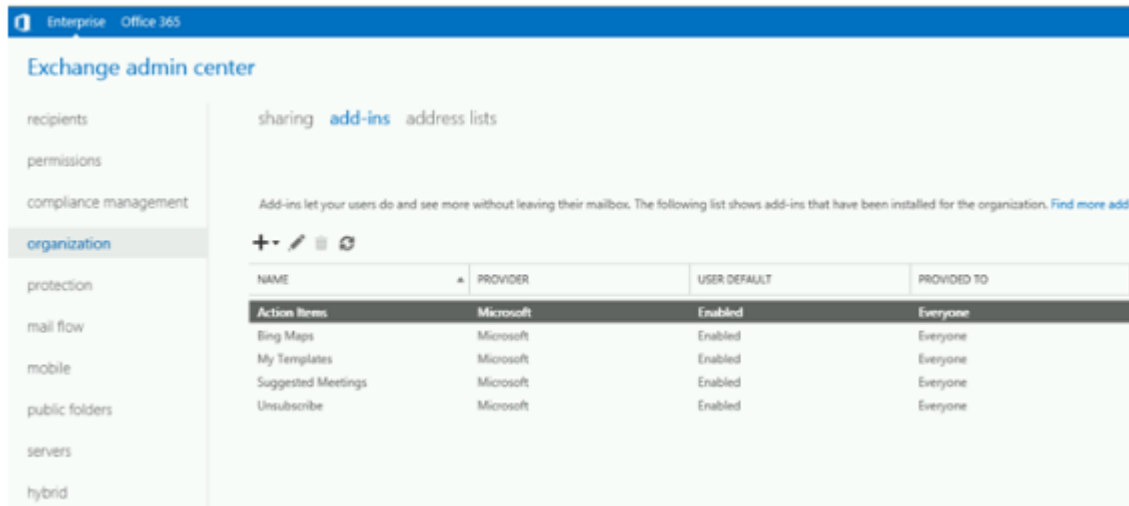
Installing the Add-in using Exchange Server Setup

You can install the Outlook add-in feature in your Windows or macOS using Microsoft Exchange server.

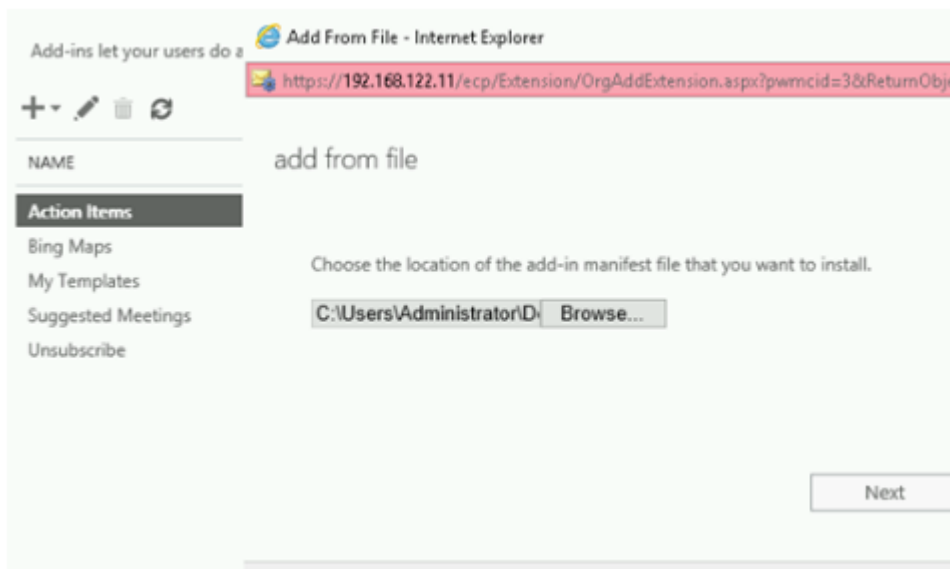
You can use the downloaded xml file to install the add-in.

Steps

- 1) Copy the xml file to the Exchange server.
- 2) Open the **Exchange Center Administration** application.
- 3) Select **organization**, and go to the **add-ins** tab.



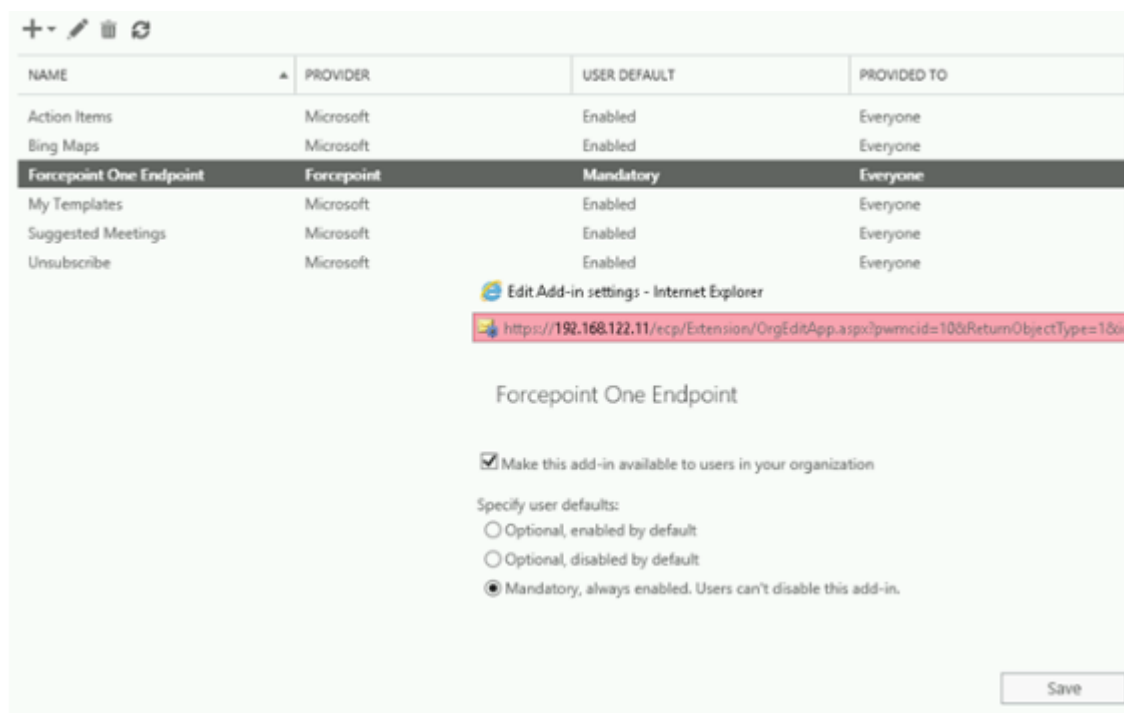
- 4) Click the **+** sign to add a new add-in.
- 5) Select **Add from file** and locate the xml file.



- 6) Click **Next**.
- 7) Set the **Provided to** field to a group that apply specifically to your endpoints or to everyone.

8) Enable **Add-in**.

You can right click to edit **Add-in**, and then specify the user defaults. You can select **Mandatory** to ensure users cannot disable this add-in and bypass DLP inspection.



Next Steps

Communication between the Forcepoint agent and the Outlook email client uses HTTPS. Forcepoint recommends creation and use of a specific certificate for use in your environment.

Related tasks

[Creating the Endpoint SSL Identity on page 67](#)

Compatibility and Other Considerations

The following table (from Microsoft) shows supported client-server combinations for the on-send feature, including the minimum required cumulative update where applicable. Excluded combinations are not supported.

Compatibility

Client	Exchange Online	Exchange 2016 On-Premises (Cumulative Update 6 or Later)	Exchange 2019 On-Premises (Cumulative Update 1 or Later)
Windows: Outlook Client Version 1910 (build 12130.20272) or later	Yes	Yes	Yes
Mac: Build 16.47 or later	Yes	Yes	Yes
Web Browser: Modern Outlook UI	Yes	N/A	N/A

Client	Exchange Online	Exchange 2016 On-Premises (Cumulative Update 6 or Later)	Exchange 2019 On-Premises (Cumulative Update 1 or Later)
Web Browser: Classic Outlook UI	N/A	Yes	Yes

For more information, refer to Microsoft's documentation for [On-Send Supported Clients and Platforms](#).

The Microsoft Outlook add-in is installed into the Outlook account and not the Outlook client. Note the following:

- Only accounts that have the Outlook add-in enabled will have data protection.
- Additional accounts (personal or otherwise) that are added to the Outlook client will not have data protection unless those accounts have an add-in linked.
- Administrators can allow only corporate mailboxes to be added to Outlook accounts by following the instructions in the following Microsoft documentation: [Allow only corporate mailboxes to be added](#).
- Since the add-in is account enabled, it applies to all operating systems for that account. For instance, for a user that has both a macOS and a Windows machine, the add-in is enabled for both of them. However, the endpoint agent has add-in support for macOS and uses injection-based plug-in support on Windows i.e. the Windows agent does not use the add-in.
- There are some Microsoft limits associated with using Outlook add-ins that make use of the On-send function. For more details, see [Outlook On-send Add-ins Limitations](#).

Windows Installation

You can install Forcepoint F1E agents on Windows endpoints.



Important

After deploying Forcepoint DLP Endpoint, you must restart the Forcepoint F1E software to complete the installation process.

There are a few ways to distribute the Forcepoint F1E software on Windows endpoint machines:

- Deploy Forcepoint F1E manually on each endpoint machine.
- Deploy Forcepoint DLP Endpoint to a shared server that hosts Citrix XenApp, Citrix XenDesktop, or Citrix Virtual Apps desktop virtualization software, or deploy Forcepoint ECA to a shared server that hosts Citrix XenDesktop software. This deployment method is similar to the manual deployment, but you deploy the installation package to a network server instead of each endpoint machine. Supported Citrix versions are listed in the [Certified Product Matrix](#).

For more information about specific installation and configuration instructions for Forcepoint DLP endpoint, see [Deploying Forcepoint DLP Endpoint on Citrix XenApp, XenDesktop, and Virtual Apps clients](#).

For more information about deploying software to a Citrix virtual environment, see the [Citrix documentation](#).

- Deploy Forcepoint Endpoint Context Agent (ECA) to a limited set of endpoint machines using the ECA Evaluation deployment option. Forcepoint NGFW 7.0 or later is required to use the ECA Evaluation feature. For more information, see Knowledge Base article [16193](#).
- Deploy Forcepoint F1E using a third-party deployment tool for Windows. Forcepoint F1E can be remotely deployed using your preferred deployment server or distribution system, as long as it accepts an Executable (.exe) or ZIP (.zip) file as the input and can run the installation command remotely.

**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 information

Manual Install on a Windows endpoint machine on page 59

Manual Install on a Windows endpoint machine

Stand-alone Forcepoint DLP Endpoint packages

Windows packages created with the package builder contain a single executable file: `FORCEPOINT-ONE-ENDPOINTx64.exe`. If you are installing Forcepoint DLP endpoint only, you can do the following:

- 1) Copy the executable file to the endpoint machine.
- 2) Double-click the executable file, and step through the installation wizard.
- 3) Restart the endpoint machine to complete the installation.

In virtual desktop (VDI) environments, install the Forcepoint DLP endpoint software as if the endpoint machine were a physical machine, while taking into consideration any additional steps required by the infrastructure for third-party installations.

Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Cloud Security Gateway Portal (Cloud deployments)

ZIP files downloaded from the Forcepoint Cloud Security Gateway Portal (Forcepoint Web Security endpoint packages) contain the `Websense Endpoint.msi` file.

- 1) Copy `Websense Endpoint.msi` to the endpoint machine.
- 2) From the command prompt, run the following command (with the straight quotes around the msi file name) as an administrator:

```
"Websense Endpoint.msi" WSCONTEXT=<token>
```

where `<token>` is the WSCONTEXT string shown in the **GPO code** string on the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web Security module of the Forcepoint Security Manager or the **Web > Endpoint** page in the Forcepoint Cloud Security Gateway portal. For example,

Web > Endpoint

Endpoint

General End User Control Endpoint Bypass

Default Endpoint Policy

Select the default policy for roaming endpoint users who are not already synchronized in your account.

Policy:

Save **Cancel**

Deployment Settings

GPO code: WSCONTEXT=2e5f1ccfe6df33b6f7729483b6c26ef7-0
If you are using a Group Policy Object (GPO) script to deploy the endpoint use this code in your script file. See [Help](#) for further details.

Supply a password that must be used to uninstall the endpoint. This password is stored encrypted for security reasons and can be reset on this page if forgotten.

Set Anti-Tampering Password

Endpoint Client Download

Download the version of endpoint client software you want to install on end-user machines.

Endpoint type: ☒ Direct Connect [?](#)
☐ Proxy Connect [?](#)

Platform:

Available version: [1.5.8.3.3527](#) [Release notes](#) Supported on Windows 7, 8, 8.1, 10

The `WSCONTEXT` string used to identify your organization to the hybrid or cloud service must be included in the command string. Each account has its own `WSCONTEXT` string. Roaming and remote users use this string to connect to your specific account.

Forcepoint Web Security Proxy Connect Endpoint or mixed packages made via the package builder

Windows packages created with the package builder contain a single executable file: `FORCEPOINT-ONE-ENDPOINTx64.exe`.

If you are installing the Forcepoint Proxy Connect Endpoint only, or a mixed installation package containing Forcepoint Proxy Connect Endpoint and one or more other compatible Forcepoint F1E agents (Forcepoint DLP Endpoint or Forcepoint ECA):

- 1) Copy the executable file to the endpoint machine.
- 2) Open the command line and run the following command from the folder containing the installation package: `FORCEPOINT-ONE-ENDPOINT-x64.exe /v"XPSWDPXY=<password> WSCONTEXT=<token>"` where:
 - `<password>` is the anti-tampering password used by the Forcepoint Endpoint software already installed on the endpoint machine (if upgrading) or to be used by the new Forcepoint F1E software. If the password contains a special character, you must type a ^ character before the special character. For more information, see *Guidelines for creating an anti-tampering password*.
 - `<token>` is the WSCONTEXT string shown in the **GPO code** string on the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web Security module of the Forcepoint Security Manager or the **Web > Endpoint** page in the Forcepoint Cloud Security Gateway Portal.

The `WSCONTEXT` string used to identify your organization to the hybrid or cloud service must be included in the command string. Each account has its own `WSCONTEXT` string. Roaming and remote users use this string to connect to your specific account.

All arguments passed via the `/v` parameter must be enclosed in straight quotes, as shown in the example.

You must provide both the XPSWDPXY and WSCONTEXT arguments.

To perform a silent install, add the `/qn` parameter as follows:

```
FORCEPOINT-ONE-ENDPOINT-x64.exe /v"/qn XPSWDPXY=<password> WSCONTEXT=<token>"
```

To perform a silent install that does not prompt the end user to restart the endpoint machine, add the `/norestart` parameter as follows:

```
FORCEPOINT-ONE-ENDPOINT-x64.exe /v"/qn /norestart XPSWDPXY=<password> WSCONTEXT=<token>"
```



Note

You must restart the endpoint machine to finish a Forcepoint DLP endpoint installation. If you perform a silent install without a restart (using the `/norestart` parameter), Forcepoint DLP endpoint may not function as needed until after the endpoint machine is restarted.

The command switches are summarized below:

Function	Switch
Silent install	FORCEPOINT-ONE-ENDPOINT-x64.exe /v"/qn"
Silent install without restart	FORCEPOINT-ONE-ENDPOINT-x64.exe /v"/qn /norestart"
Set WSCONTEXT	FORCEPOINT-ONE-ENDPOINT-x64.exe /v"WSCONTEXT=xxxx"
Set uninstall password	FORCEPOINT-ONE-ENDPOINT-x64.exe /v"XPSWDPXY=xxxx"
Set WSCONTEXT and silent install	FORCEPOINT-ONE-ENDPOINT-x64.exe /v"/qn WSCONTEXT=xxxx"

Related concepts

[Guidelines for creating an anti-tampering password on page 23](#)

Forcepoint Web Security Direct Connect Endpoint or mixed packages made via the package builder

Windows packages created with the package builder contain a single executable file: `FORCEPOINT-ONE-ENDPOINTx64.exe`. Forcepoint Web Security Direct Connect Endpoint packages do not require an installation through the command line, because the `WSCONTEXT` value was provided when the package was created through the package builder.

- 1) Copy the executable file to the endpoint machine.
- 2) Double-click the executable file and step through the installation wizard.

**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.

Related concepts

[Testing your deployment](#) on page 63

Forcepoint Endpoint Context Agent packages made via the package builder

Windows packages created with the package builder contain a single executable file: `FORCEPOINT-ONE-ENDPOINTx64.exe`. To deploy the Forcepoint ECA installation package in your environment, you must complete the following procedures:

- 1) **Authenticate Forcepoint ECA using client certificates**
The Forcepoint NGFW Engine uses a client certificate to authenticate endpoint machines running Forcepoint ECA. In this procedure, you must establish a certificate authority (CA) for Forcepoint ECA, create the client certificate template, then deploy a unique client certificate to each endpoint machine.
- 2) **Configure Forcepoint ECA settings in the Security Management Center (SMC)**
In this procedure, you must configure the initial Forcepoint ECA settings in the SMC to create a configuration file. This configuration file is added to the installation package through the package builder.
- 3) **Deploy Forcepoint ECA to the endpoint machine**
In this procedure, manually install Forcepoint ECA on the endpoint machine.
 - a) Copy the executable file to the endpoint machine.
 - b) Double-click the executable file and step through the installation wizard

Forcepoint ECA Evaluation

Forcepoint ECA can also be deployed to a limited set of endpoint machines using the ECA Evaluation deployment option. This deployment option is beneficial for customers who wish to evaluate Forcepoint ECA without deploying the Forcepoint ECA software enterprise-wide.

With ECA Evaluation, all of the required certificates for communication between endpoint machines and the NGFW Engine are created automatically. After enabling the ECA Evaluation feature, a web app is hosted on the management server. On each endpoint machine, users can browse to the web app, then download and install the Forcepoint ECA software and the necessary certificates. Windows administrator rights are required for installing Forcepoint ECA on the endpoint machine.

For instructions about deploying Forcepoint ECA for evaluation purposes, see Knowledge Base article [16193](#).

**Note**

To use the ECA Evaluation feature, you must have Forcepoint NGFW v7.0 or later deployed in your organization.

Related tasks

[Authenticating Forcepoint ECA using client certificates](#) on page 20

[Configuring Forcepoint Endpoint Context Agent settings in the SMC](#) on page 21

Manual uninstall from a Windows endpoint machine



You can manually uninstall the Forcepoint F1E agent from Windows endpoint.


Steps

- 1) Use the Add or remove programs tool in Windows to uninstall the Forcepoint F1E endpoint. A message appears to confirm that you want to delete the Forcepoint F1E endpoint agent.
- 2) Click **Yes**.
- 3) If you had defined an administrative password, enter the password in the dialog that opens, and then click **OK**.
- 4) To uninstall the Forcepoint DLP endpoint, restart the endpoint machine. The configuration changes are applied only when the endpoint machine has restarted.

Testing your deployment

To confirm that the Forcepoint F1E software is installed and running on an endpoint machine, do the following:

- When Forcepoint DLP endpoint is installed in interactive mode, an icon () is shown on the task bar's notification area (No icon is shown in stealth mode). Right-click the icon, and select **Open Forcepoint DLP Endpoint** to view connection status. Also, if you move your mouse over the icon, a tooltip is shown with the connection status.
You can also verify the status in the Diagnostics Tool. Right-click the Forcepoint icon on the task bar, and select **Open Forcepoint One Endpoint Diagnostics**. The status is shown under the **System information** diagnostics test.
- For Forcepoint Web Security Endpoint deployments:
 - Under **Services** in **Windows Administrative Tools**, verify that the **Forcepoint Websense SaaS Service** is **Running**.
 - Verify the status from the icon () shown on the task bar's notification area. If the icon has a check mark in the lower right corner, the Forcepoint Web Security Endpoint is connected. Also, if you move your mouse over the icon, a tooltip is shown with the connection status.

- Verify the status in the Diagnostics Tool. Right-click the Forcepoint icon on the task, and select **Open Forcepoint One Endpoint Diagnostics**. The status is shown under the **System information** diagnostics test.
- For Windows Forcepoint Web Security Direct Connect Endpoint deployments, ensure that the end users have joined the organization's domain. If the end user has not joined the domain, Forcepoint Web Security Direct Connect Endpoint cannot connect to the disposition server.
To check if the end user is logged on to the domain, open the Diagnostics Tool, and run the System information diagnostics test. If **Logon Domain = No**, the end user has not joined the domain. The Cloud Services diagnostics icon changes to an X and the **Disposition Server Test = Failed**.
- For Forcepoint Endpoint Context Agent (ECA) deployments:
 - Under **Services** in **Windows Administrative Tools**, verify that the **Forcepoint Endpoint Context Agent** service is **Running**.
 - Verify the status from the icon () shown on the task bar's notification area. If the icon has a check mark in the lower right corner, Forcepoint Endpoint Context Agent (ECA) is connected. Also, if you move your mouse over the icon, a tooltip is shown with the connection status.
 - Verify the status in the Diagnostics Tool. Right-click the Forcepoint icon on the task bar and select **Open Forcepoint One Endpoint Diagnostics**. The status is shown under the **System information** diagnostics test.

Mostly, the Forcepoint F1E software installation fails due to permission related issues. An endpoint installation requires local administrator rights.

Troubleshooting a Forcepoint Endpoint Context Agent deployment

If you encounter issues during the Forcepoint Endpoint Context Agent (ECA) installation, review the following checklist, then try to install Forcepoint ECA again.

- Verify that you installed Forcepoint ECA using an account with local administrator rights. Forcepoint ECA installation requires local administrator rights.
- Check the connection between the endpoint machine and Forcepoint NGFW.
- Check the certificates installed in the endpoint machine's certificate stores using mmc.exe and the Certificates snap-in. The certificate issuer (CA certificate) must be configured in the SMC. Verify that the policy on the NGFW Engine is up to date. The endpoint machine receives the network-side CA certificate in the Forcepoint ECA configuration file.
The certificate generated by the SMC is valid from the time it was created in the SMC. If the time on the endpoint machine is different from the time in the SMC, the endpoint machine might not accept the generated certificate. After the endpoint machine's time reaches the certificate's validity start time, the certificate is accepted on the endpoint machine.

The Forcepoint ECA client initiates connections to certificate revocation list (CRL) servers to verify the signatures of the executables that are initiating connections from the endpoint machine. When an executable connects to the network for the first time, the Forcepoint ECA client checks the executable's signature against the CRL.

If the executable has been modified, or if the code signing certificate has been revoked, Forcepoint ECA does not trust the executable fields, such as product name, product version, or signer name, when it tries to match the executable in the Forcepoint NGFW. The executable's signature check status is then logged in the SMC logs as "Failed".

The following list shows common connectivity error messages and troubleshooting steps:

- Error message: **Failed to accept SSL-connection...: SSL error: peer did not return a certificate**
 - Check that the certificate is installed in the certificate store on the endpoint machine.

- Check that the client certificate has the **Client Authentication** Application Policy enabled.
- Check that the issuer of the client certificate on the endpoint machine matches the issuer of the client certificate in the ECA configuration in the SMC.
- Error message: **Failed to accept SSL-connection...: SSL error: sslv3 alert bad certificate**
 - Check the `DebugDump.txt` file in the Forcepoint ECA installation folder on the endpoint machine for the actual error.
 - If the error message is **Verify failure... certificate is not yet valid**, check the time difference between the endpoint machine and the SMC.
- Error message: **Same client connected to adjacent node**
 - If the Forcepoint ECA client disconnects immediately after proceeding to the CONFIGURED connection state and shows the **Same client connected to adjacent node** message in the `DebugDump.txt` file or in the Information Message field in the SMC, ensure that the Forcepoint ECA clients use different certificates. Forcepoint NGFW does not allow two or more connections to share a client certificate. Each Forcepoint ECA client must have a unique client certificate.

Uninstalling Forcepoint F1E from a Windows endpoint machine

You can uninstall Forcepoint F1E software remotely through a deployment server or distribution system.



Note

If you configured an administrative password, you must supply it to uninstall the software.

Uninstalling Forcepoint F1E using a deployment server

If you deployed Forcepoint F1E Endpoint through GPO, you can uninstall the software through the Active Directory Users and Computers snap-in. For more information, see [How to use Group Policy to remotely install software](#).

You can also silently uninstall Forcepoint F1E Endpoint by running the following command (does not apply to stand-alone DLP):

```
msiexec /x {product_code} /qn XPSWDPXY=<password>
```

where:

- `{product_code}` is a unique identifier (GUID) that can be found in the `setup.ini` file of each installation package or the system registry. It is different for each version and bit type.
- `<password>` is the administrator password that you entered when creating the installation package. If the password contains a special character, you must type a ^ character before the special character.

To find the `setup.ini` file, use a file compression tool like WinZip or 7-Zip to extract the contents of the installation package executable.

To silently uninstall Forcepoint F1E Endpoint without a restart, include the `/norestart` parameter as follows:

```
msiexec /x {ProductCode} /qn /XPSWDPXY=<password> /norestart
```

The command switches are summarized below.

Function	Switch
Silent uninstall	<code>msiexec /x {ProductCode} /qn XPSWDPXY=xxxx</code>
Silent uninstall without restart	<code>msiexec /x {ProductCode} /qn XPSWDPXY=xxxx/ norestart</code>

Related concepts

[Guidelines for creating an anti-tampering password](#) on page 23

Uninstalling Forcepoint F1E using a distribution system

If you used the Microsoft SMS distribution system to create the Forcepoint F1E installation packages, you can modify the packages and use them to uninstall the software. If you did not create a package for deploying Forcepoint F1E, you must create a new package for uninstallation.

For more information about creating SMS installation packages, see [Creating Software Installation Packages with SMS Installer](#).

After deploying the package, Forcepoint F1E is uninstalled from the defined list of endpoint machines.

macOS Installation

You can install Forcepoint F1E agents on macOS endpoints.

There are a few ways to distribute the Forcepoint F1E software on mac endpoint machines:

- Manually on each endpoint machine
- Using Remote Desktop
- Automatically using mobile device management (MDM) software, such as Jamf

**Note**

If you are downgrading to an older version of F1E, you must uninstall the latest version from your system, and then install the desired version.

Related concepts

[Manual Install](#) on page 71

Related tasks

[Installing the agent using Jamf](#) on page 83

Creating the Endpoint SSL Identity

To enable secure communication between the Forcepoint F1E agent and components like the Outlook add-in, browser extension, Inline Proxy, and macOS-based Direct Connect or Proxy Connect installations, the Endpoint must be assigned an SSL identity, and the client machine must trust that identity.

Before you begin

You must have OpenSSL installed on your machine.

Forcepoint recommends to create a self-signed certificate that can be bundled with the Endpoint installation package along with the private key used for generating the certificate. This document explains how to generate this certificate using OpenSSL.



Note

You can follow the steps in this procedure only if you want to create your own SSL identity and do not want to use the default one provided with the installer. For a full manual installation, the localhost (`server.pem`) certificate needs to be added and trusted manually in the Keychain app. If you use Jamf and the default certificates and do not want to create a unique SSL Identity, you can place the localhost (`server.pem`) certificate in Jamf to avoid manually trusting the certificate in Keychain. This (`server.pem`) certificate is located at "`\Library\Application Support\WebSense Endpoint\DLP\www\certs`" on macOS after the agent is installed.

Creation of an SSL Identity for your endpoints with OpenSSL uses a configuration file.

Steps

- 1) Open the configuration file template.

```
[ req ]
distinguished_name = req_distinguished_name
req_extensions      = v3_req
x509_extensions     = v3_req
prompt              = no
[ req_distinguished_name ]
C                   = <Country>
ST                  = <State or Province>
L                   = <City>
O                   = <Organization>
OU                  = <Organizational Unit>
CN                  = localhost
emailAddress        = <Email>

[v3_req]

subjectKeyIdentifier = hash
basicConstraints     = critical,CA:false
subjectAltName       = DNS:localhost
keyUsage             = critical,digitalSignature,keyEncipherment
```

See sample below:

```
1 [ req ]
2
3 distinguished_name = req_distinguished_name
4 req_extensions= v3_req
5 x509_extensions= v3_req
6 prompt= no
7
8 [ req_distinguished_name ]
9 C= IE
10 ST= Cork
11 L= Cork
12 O= Forcepoint
13 OU= IT
14 CN= localhost
15 emailAddress= first.name@email.com
16
17 [v3_req]
18
19 subjectKeyIdentifier = hash
20 basicConstraints = critical,CA:false
21 subjectAltName = DNS:localhost
22 keyUsage = critical,digitalSignature,keyEncipherment
```

- 2) Replace the values in angle brackets (<>) with the appropriate information for your organization:
 - Be sure to remove all the angle brackets from the document.
 - Country name can only have a maximum of two characters entered.
 - Values not in angle brackets are defaults and can be left unchanged.
 - The CN must be entered as `localhost` and the `subjectAltName` must be entered as `DNS:localhost`.
- 3) Once complete, save the file as `localhost.config` in a directory of your choice.
- 4) Open a terminal application and `cd` to the directory you saved the `localhost.config` file.
- 5) Run the following command from the same directory to create the key files:

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out server.pem -sha256 -config localhost.config -days 10950 -nodes
```

The command creates the following files:

 - `key.pem`: Private key for the SSL identity. This file is deployed to the endpoint clients.
 - `server.pem`: Self-signed certificate for the SSL identity. This file is deployed to the endpoint clients.
- 6) Run the Websense Endpoint Package Builder on the management server and create new MAC Endpoint installation package.
- 7) Unzip the new mac Endpoint Installer `FORCEPOINT-ONE-ENDPOINT-Mac.zip`.
- 8) To place both PEM files in the same directory of the `WebsenseEndpoint.pkg` file, copy `server.pem` and `key.pem` into the newly created Endpoint Mac Installer in `directory \FORCEPOINT-ONE-ENDPOINT-Mac \EndpointInstaller\`.
- 9) Zip folder back up again.
- 10) Install the new package on the Mac clients.
- 11) Optional: If you plan to install the agent via Jamf, then you must convert the certificate to its binary encoded DER format.

The `server.pem` and `key.pem` should still be placed in the installer package, however, the converted `server.der` should only be used in JAMF policy and NOT be placed in the installer package.

Related concepts

Converting the `server.pem` file to `.der` format on page 85

Creating the Endpoint SSL Identity using custom certificate

You can use custom or third party signed certificate for generating the endpoint ssl identity files.

Steps

- 1) To generate a new key in .pem format and Certificate Signing Request (CSR) of the `localhost.config` file, generate the following request in the OpenSSL at the terminal.

```
openssl req -newkey rsa:4096 -keyout key.pem -out server.csr -config localhost.config -sha256 -nodes
```

- 2) Sign the CSR using third party certificate authority (CA).

You can use **Web Server** default template to sign in Base 64 encoded format.

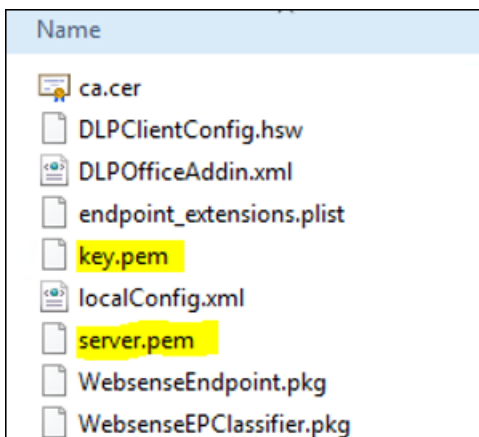
- 3) Convert the .cer file to .pem by running the command: `openssl x509 -in certnew.cer -out server.pem`. `Server.pem` and `key.pem` files are generated.

- 4) Optional: To review the certificate before re-packaging them into the installer, do the following:

- a) Run the command: `openssl x509 -in server.pem -text -noout`
- b) Ensure all the specifications defined in the config file being present in the certificate as below:
 - Signature Algorithm: **sha256WithRSAEncryption**
 - RSA Public-Key **4096** bit
 - X509v3 extensions:
 - X509v3 Key Usage: critical
 - **Digital Signature, Key Encipherment**
 - X509v3 Subject Alternative Name: **DNS:localhost**

- 5) Add the `key.pem` and `server.pem` files into extracted Endpoint installer path below, and extract to zip (FORCEPOINT-ONE-ENDPOINT-Mac.zip)

■ `\FORCEPOINT-ONE-ENDPOINT-Mac\EndpointInstaller\`



Note

You can perform a manual installation of the Endpoint on a test MAC machine before Jamf packaging.

Manual Install

You can install the Forcepoint F1E Endpoint agent on macOS.

The install process is broken into two steps – an initial agent install followed by trusting the SSL identity for your endpoint. The second step is only required if you intend to monitor email on the endpoint and if your email client is Microsoft Outlook.



Note

Forcepoint recommends to deploy the agent using distributions services such as Jamf for production roll outs.

Following are the requirements for agent installation:

- Administrator credentials on the endpoint machine.
- For the DLP installations, ensure the following:
 - If you intend to monitor email on the endpoint and if your email client is Microsoft Outlook then you must first deploy the Forcepoint Outlook Add-in.
 - You must create the SSL Identity, and generate the following:
 - `key.pem`: Private key for the SSL identity.
 - `server.pem`: Self-signed certificate for the SSL identity.

Related concepts

Deploying Forcepoint F1E Outlook Add in on macOS

Related tasks

Creating the Endpoint SSL Identity on page 67

Initial agent install on page 72

Trusting the SSL Identity and deploying the certificate on page 81

Creating the installation package from the package builder on page 26

Initial agent install

You can install the Forcepoint F1E agent manually in your macOS.

Steps

- 1) From the mac packages, copy `FORCEPOINT-ONEENDPOINT-Mac.zip` to the endpoint machine, then double-click the file to unzip the installation package.

macOS automatically creates a directory named `EndpointInstaller`, which contains a file called `WebsenseEndpoint.pkg` and the `generate_root_ca` tool.

**Note**

You may need to modify the `generate_root_ca` permissions so you can double click the `generate_root_ca` as an executable file. To do this, open the folder where the `generate_root_ca` is located and run `chmod 777 generate_root_ca` in the terminal.

- 2) To run the `generate_root_ca` tool, open the folder where the `generate_root_ca` is located and run `generate_root_ca` in the terminal.

The `_ca.cer` certificate and the `fpnpd.dat` file generates.

**Note**

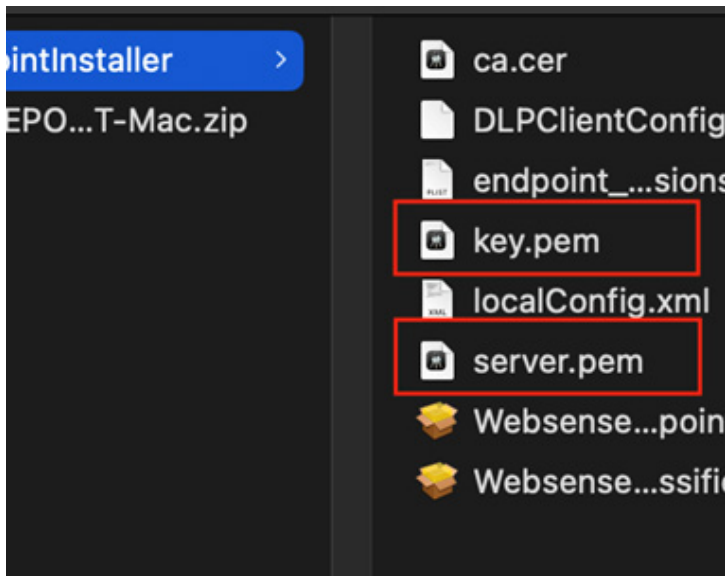
After running the `generate_root_ca` tool, the installer folder will have two certificates, `ca.cer` and `_ca.cer` . When you run the installer, the certificates are picked and installed. You must manually trust the `_ca.cer` certificate after opening the keychain.

- 3) Add the `_ca.cer` certificate file into the keychain and trust it.

**Note**

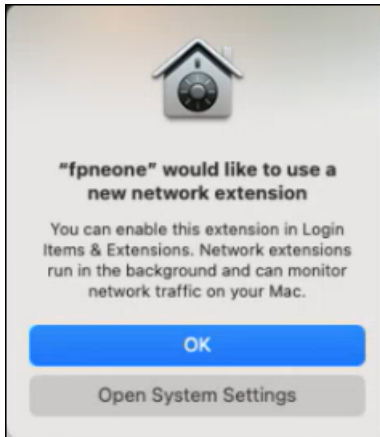
If you encounter certificate issues, you should remove and re-trust the root CA. Begin by opening keychain, locate the FP root CA certificate and remove it. Restart the device to apply the changes and after restart, open the key chain and trust the certificate again.

- 4) If you are deploying a Forcepoint DLP Endpoint package, add the private key file `key.pem` and the certificate file `server.pem` to the `EndpointInstaller` folder.



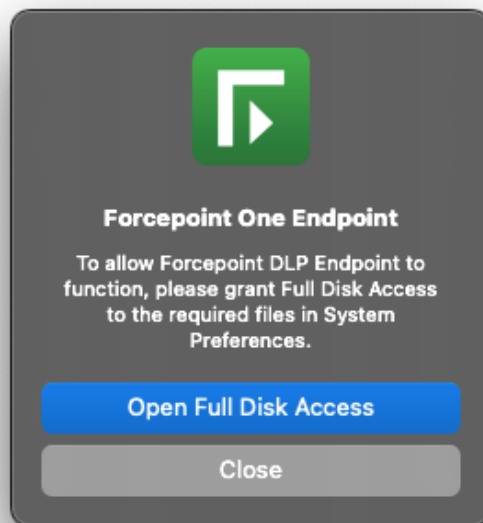
- 5) To start the installation process, double-click `WebsenseEndpoint.pkg`.
- 6) Click **Continue**, and agree to the license agreement.
- 7) Click **Install**.

- 8) To install the software, enter a user name and password for a user with administrator rights. A message appears stating to use a new network extension.



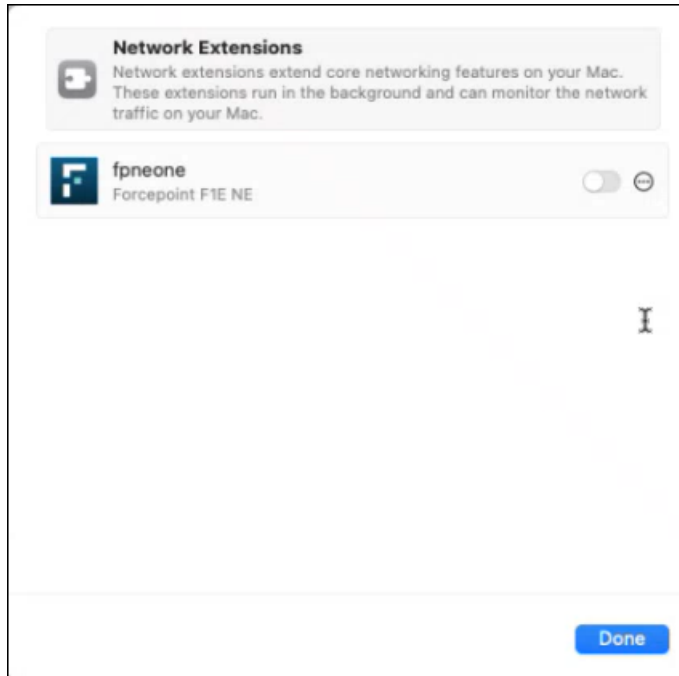
Note

If you are installing Forcepoint DLP Endpoint v21.12 or later on macOS 13 (Ventura) or macOS 14 (Sonoma), message appears for you to enable full disk access (FDA) for four new processes. (The instructions here are explained with reference to macOS 15 Sequoia. Follow the similar instructions for other operating systems).



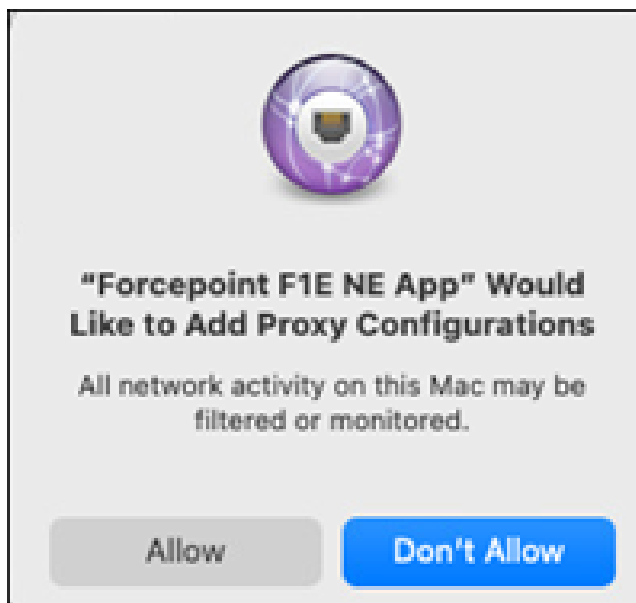
- 9) To install the system extensions, do the following:
- a) Click **Open System Settings** or navigate to **General > Login Items & Extensions > Network Extensions**.

- b) Turn on **fpneone**.



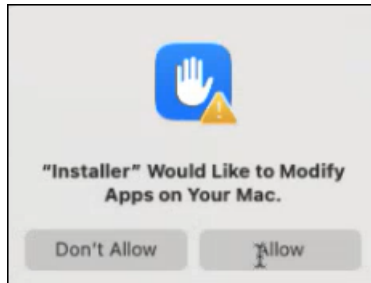
The **System Extensions** window opens.

- c) Enter password, and then click **OK**.
A message appears stating that the Forcepoint F1E NE App would like to add proxy configurations.
- d) Click **Allow**.

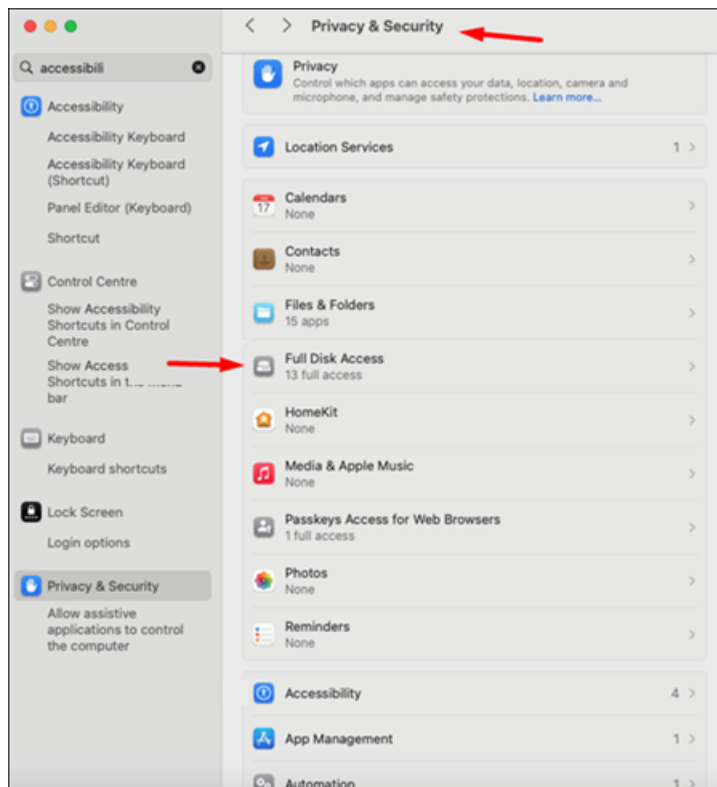


- e) Click **Done**.

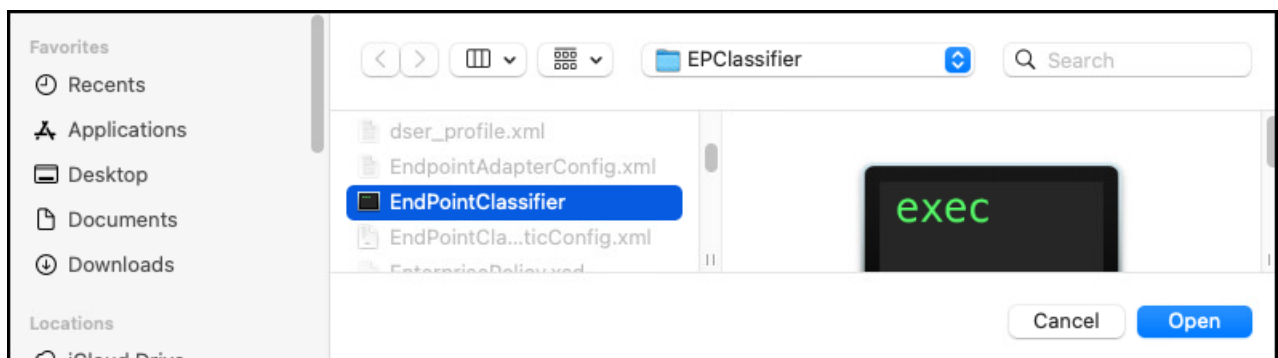
- f) To allow the installer to modify the applications on your Mac, click **Allow**.




- 10) To grant Full Disk Access(FDA) access, navigate to **Privacy & Security > Full Disk Access**, and do the following.



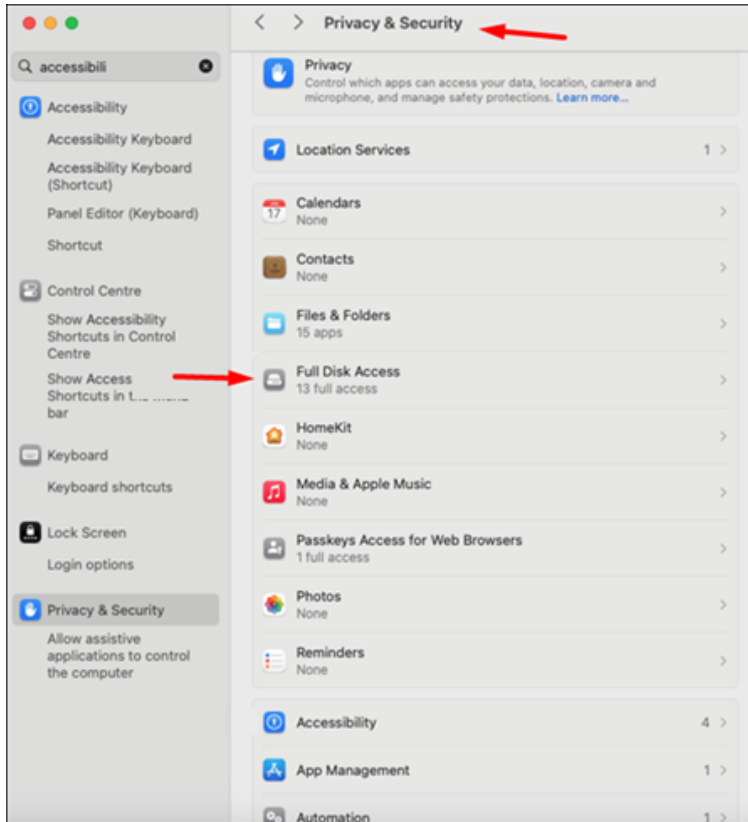
- a) Click the **+** button, and navigate to **Library > Application Support > Websense Endpoint > DLP**, select `wsdlpd`, and then click **Open**.



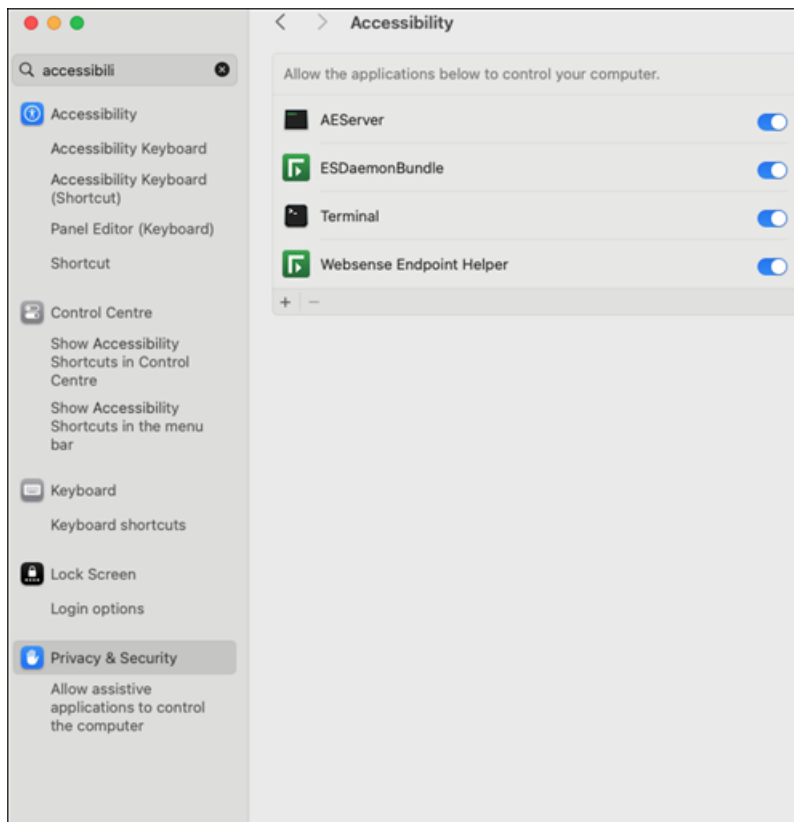
Verify that `wsdlpd` is included in the list and selected.


- b) Click the  button and navigate to **Library > Application Support > Websense Endpoint > EPClassifier**, select `EndPointClassifier`, and then click **Open**.
Verify that `EndPointClassifier` is included in the list and selected.

- 11) To grant accessibility, navigate to **Privacy & Security > Accessibility**, and do the following.



- a) Turn on **ESDaemonBundle**, **Websense Endpoint Helper**, and **AESEServer**.



- b) To add AEServer in **Privacy & Security > Accessibility**, click the  button and navigate to **System > Library > Frameworks > CoreServices.framework > Versions > A > Frameworks > AE.framework > Versions > A > Support > AEServer**.
- c) Close the **Privacy & Security** window.

**Note**

If you are deploying Forcepoint DLP Endpoint using Jamf, you can enable FDA for these processes using a configuration file.

Related concepts

Enabling full disk access on macOS on page 79

Related tasks

Creating the Endpoint SSL Identity on page 67

Installing the agent using Jamf on page 83

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*.

Related tasks

Initial agent install on page 72

Installing the agent using Jamf on page 83

Enabling web file uploads analysis

Enabling web file uploads analysis is required to detect file uploads on the Web channel.

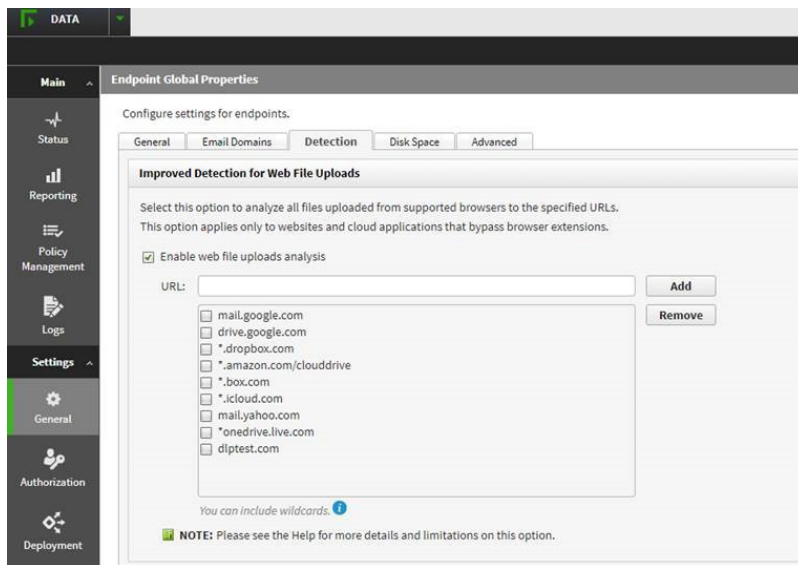


Note

This feature is no longer required when using a Manifest V3 browser extension or an inline proxy for web channel inspection.

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) In **URL**, 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.

Trusting the SSL Identity and deploying the certificate

To enable secure communication with your Outlook Email client, the Endpoint must be given an SSL identity, and the client machine must be set up to trust that identity.

Before you begin

You must create the Endpoint SSL Identity.

This step is only required if you intend to monitor email on the endpoint and if your email client is Microsoft Outlook.

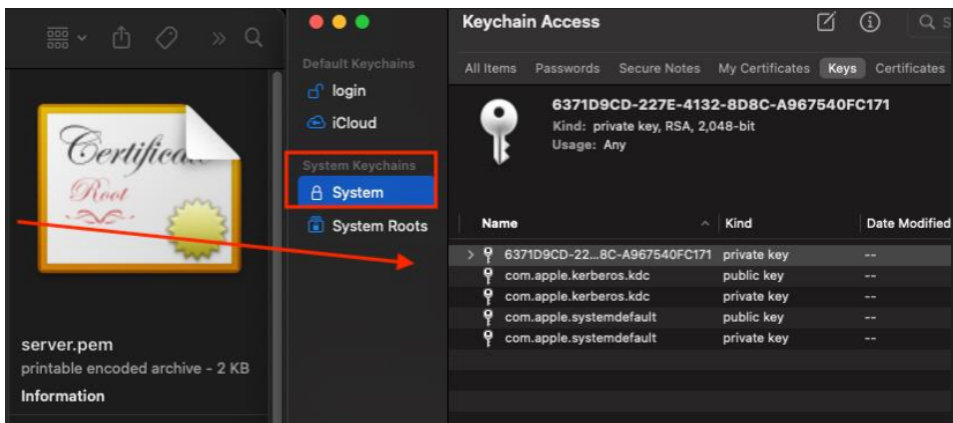


Note

You can also use the mobile device management (MDM) methods such as Jamf for deployment of SSL certificates in your mac Endpoints.

Steps

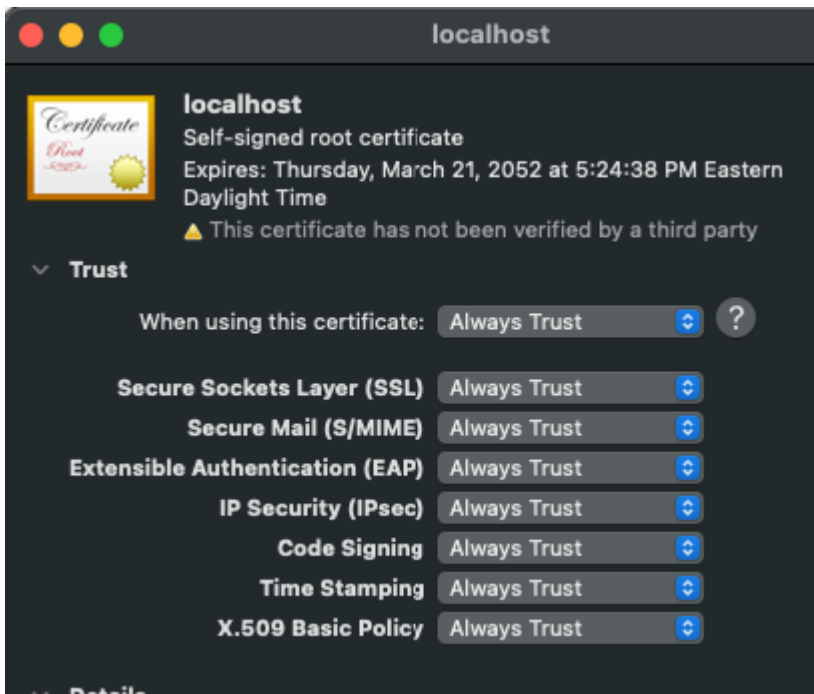
- 1) Open the installation folder which has the `server.pem` file.
- 2) Double click the `server.pem` file.
The macOS **Keychain Access** application opens.
- 3) Select the **Keys** tab in **System**, and drag the `server.pem` file in to add it.



A new certificate `localhost` is created in **Certificates**.

- 4) In **Certificates**, click `localhost` to open the Trust section.

- 5) To ensure that your local system always trusts the certificate, in **When using this certificate**, select **Always Trust**.



- 6) To save the settings, close the windows.
The certificate now shows as trusted for all users in your **Keychain Access** application.

Related tasks

Trusting the SSL Identity using Jamf and deploying the certificate on page 85

Testing your deployment

You can confirm that the Forcepoint F1E software is installed and running on a mac endpoint machine by the following ways:

- Forcepoint F1E files are installed in the **Library > Application Support > Websense Endpoint** directory.
- When Forcepoint DLP Endpoint is installed and running in interactive mode, an icon (🛡️) displays on the menu bar's status menu. You can click the icon for status information. (No icon is shown in stealth mode).

To check whether the Forcepoint F1E software is running, you can open **Activity Monitor**, and select **All Processes** in **View**. The process "wspxyd", "wsdc", "wsdlpd" or "wsrfd" should be running depending on which Forcepoint F1E product is installed.

If you are using the Firefox browser, and the Forcepoint F1E Firefox extension is not installed, you must complete one of the following actions:


- Stop and start the service from the command line: `wepsvc --stop && wepsvc --start`
- Restart the endpoint machine.
On relaunching Firefox, the Firefox extension will be installed and visible in the list of extensions.

Manual Uninstall

Manually uninstall the agent from your macOS endpoints.

You can use the **System Preferences** or **System Settings** window to uninstall the Forcepoint F1E agent.

Steps

- 1) Open **System Preferences** or **System Settings**.
- 2) Click the Forcepoint F1E agent  icon.
- 3) Click **Uninstall Endpoint**.
- 4) Enter the local administrator password.
- 5) Click **OK**.
- 6) If you created an anti-tampering password to block attempts to uninstall or modify Forcepoint F1E software, enter that password.



Important

- Depending on the Forcepoint F1E agent installed, you may need to enter the anti-tampering password before entering the local administrator password.
- Carefully read each prompt before entering the password to ensure you are entering the correct password.

- 7) To uninstall the Forcepoint F1E software, click **OK**.
A confirmation message appears when Forcepoint F1E Endpoint is successfully uninstalled.
- 8) To uninstall Forcepoint F1E Endpoint remotely from a Mac endpoint machine, run the following command line option with Apple Remote Desktop:

```
/usr/local/sbin/wepsvc --uninstall [--password pwd]
```


If the password contains a special character, enclose the password in single quotation marks.

Installing the agent using Jamf

Forcepoint recommends to install the agent using Jamf installation method.

While deploying the agent configuration profile using Jamf, you can automatically obtain the necessary permissions and accessibility to the agent that avoids complicated administrator or user confirmation dialogs. To install the agent using Jamf, do the following:

Steps

- 1) Create the endpoint SSL identity.
- 2) Create the endpoint package.

- 3) From the mac packages, copy `FORCEPOINT-ONEENDPOINT-Mac.zip` to the endpoint machine, then double-click the file to unzip the installation package.

macOS automatically creates a directory named `EndpointInstaller`, which contains a file called `WebsenseEndpoint.pkg` and the `generate_root_ca` tool.



Note

You may need to modify the `generate_root_ca` permissions so you can double click the `generate_root_ca` as an executable file. To do this, open the folder where the `generate_root_ca` is located and run `chmod 777 generate_root_ca` in the terminal.

- 4) To run the `generate_root_ca` tool, open the folder where the `generate_root_ca` is located and run `generate_root_ca` in the terminal.

The `_ca.cer` certificate and the `fpnpd.dat` file generates in the installer folder.



Note

With `_ca.cer` being deployed by Jamf, the `fpnpd.dat` file must be included in the installer before publishing the package in Jamf.

- 5) Convert the `server.pem` file to the `.der` format using openssl command.
- 6) Deploy the `server.der` certificate (`.der` files) through Jamf to all the endpoints.
- 7) Deploy the following through Jamf:
 - The `_ca.cer` certificate.
 - Privacy Preferences Policy Control (pppc) profile (for enabling FDA & fpneone process).
 - Content filter configuration.
 - Outlook add-in.
 - Chrome extension.
 - Firefox extension. This is built-in to the installer package for deployment.
- 8) Deploy the endpoint package through Jamf.

Related concepts

Converting the `server.pem` file to `.der` format on page 85

Related tasks

Creating the Endpoint SSL Identity on page 67

Creating the installation package from the package builder on page 26

Trusting the SSL Identity using Jamf and deploying the certificate on page 85

Deploying Privacy Preferences Policy Control (pppc) profile on page 89

Deploying Chrome extension on page 103

Deploying Firefox extension on page 104

Configuring content filters on page 96

Deploying the endpoint package through Jamf on page 104

Deploying the Agent's SSL Identity

To enable secure communication between the Forcepoint F1E agent and components like the Outlook add-in, browser extension, Inline Proxy, and macOS-based Direct Connect or Proxy Connect installations, the Endpoint must be assigned an SSL identity, and the client machine must trust that identity and deploy the certificates.

Follow the instructions to create the SSL identity and deploy the certificates through Jamf.

Related tasks

[Creating the Endpoint SSL Identity](#) on page 67

[Trusting the SSL Identity using Jamf and deploying the certificate](#) on page 85

Converting the server.pem file to .der format

You can use the Open SSL command to convert the server.pem file to .der format.

Jamf does not support the PEM format, so while using Open SSL we must run the following command:

```
openssl x509 -in server.pem -out server.der -outform DER
```

Trusting the SSL Identity using Jamf and deploying the certificate

While installing the Forcepoint F1E agent using Jamf, you must set up the client machine to trust the SSL identity so that the agent can securely communicate with the Outlook Email client.

Before you begin

You must do the following:

- Complete the steps to create the SSL identity and you have the `server.pem` file.
- Convert server.pem file to .der format.

To trust the SSL identity and deploy the certificate with Jamf, do the following:

Steps

- 1) Create the agent configuration file in Jamf Pro to hold the endpoints SSL Identity.
 - a) On the **Computers** tab, select **Configuration Profiles**.
 - b) Create the new profile and give it a name (or alternatively use an existing profile).
 - c) Select certificate, give the certificate a name, and then select **Upload**.
 - d) Upload the `server.der` file as the certificate.
 - e) Save the certificate.
 - f) Save the configuration profile.

- 2) Set the profile scope to be delivered to all macOS endpoint machines.
 - a) On the **Computers** tab, select **Configuration Profiles**, then select the SSL Identity configuration profile created in step 1.
 - b) On the **Scope** tab, select **All Computers** and **All Users**. Alternatively, specify certain individuals or groups to receive this profile
 - c) Click **Save**.



Note

Include the PEM files with the Forcepoint DLP macOS F1E package (whether within the installer ZIP archive or pushed out in addition to it so that they are extracted to the same location), and re-install the endpoint for the communication to be successful.

Deploying the `_ca.cer` certificate

For macOS endpoint installations, you must deploy `_ca.cer` certificate as the single global certificate to decrypt traffic.

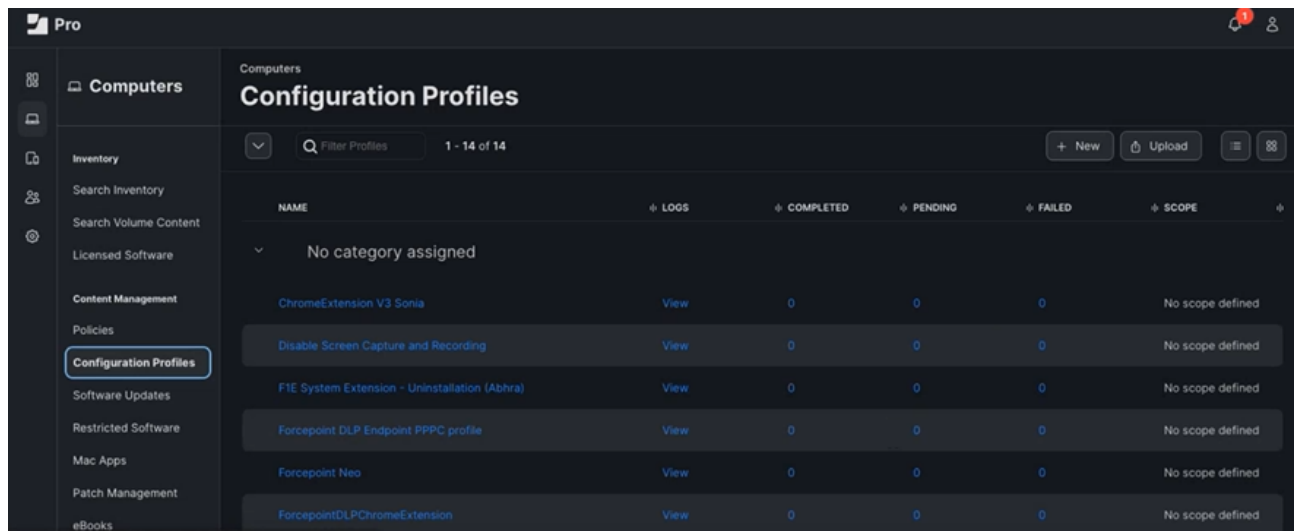
Before you begin

You must run the `generate_root_ca` tool, extracted from the `FORCEPOINT-ONEENDPOINT-Mac.zip` installer to generate the `_ca.cer` file.

Follow the below steps to deploy the certificate using Jamf:

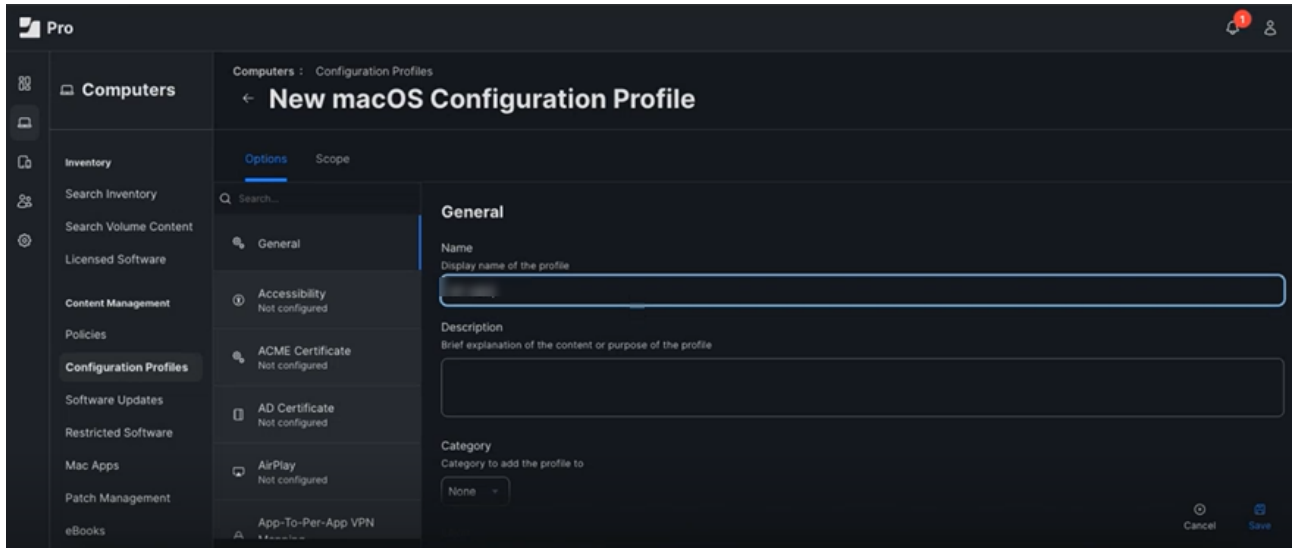
Steps

- 1) Open Jamf Pro, enter the administrator name and password, and then click **Log in**.
- 2) On the **Computers** tab, select **Configuration Profiles**.

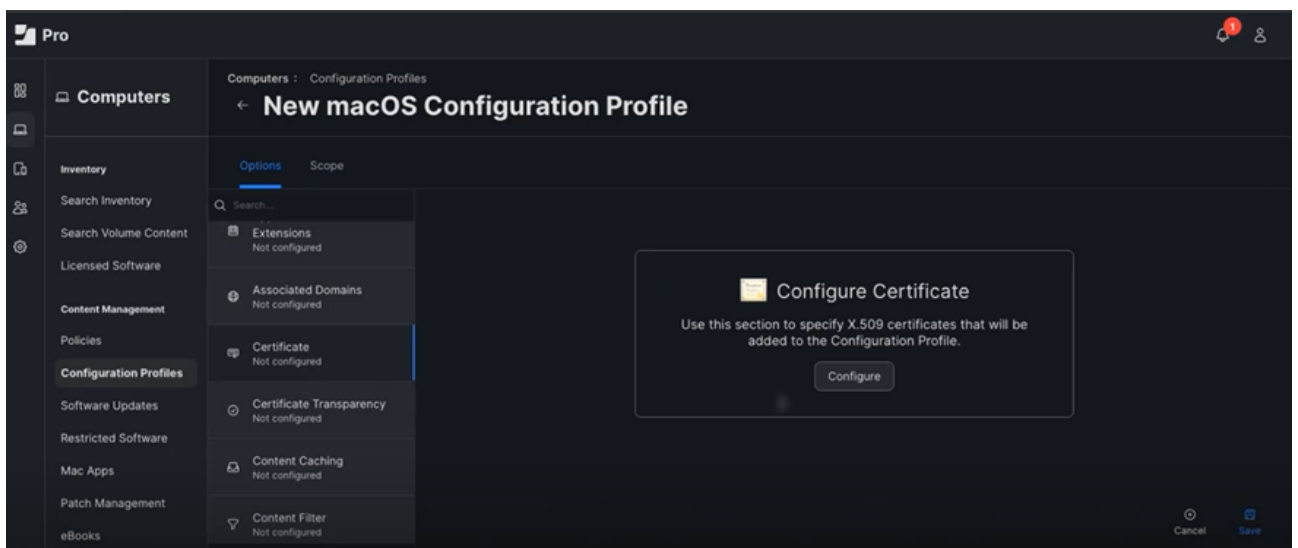


- 3) Click **New**.

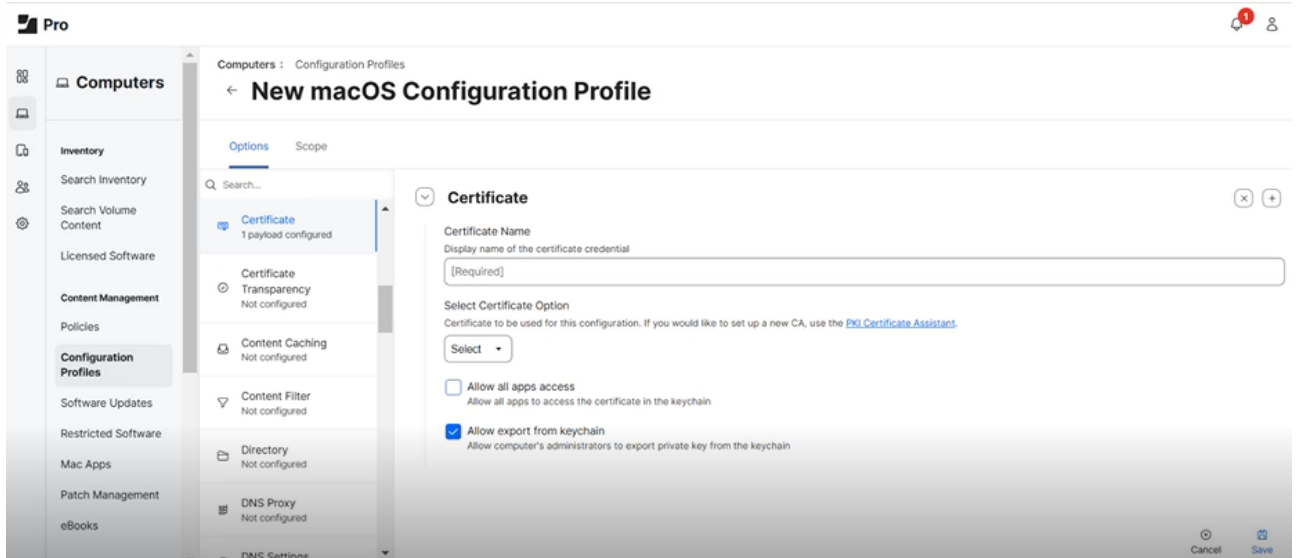
- 4) In **General**, enter the name for your configuration profile.



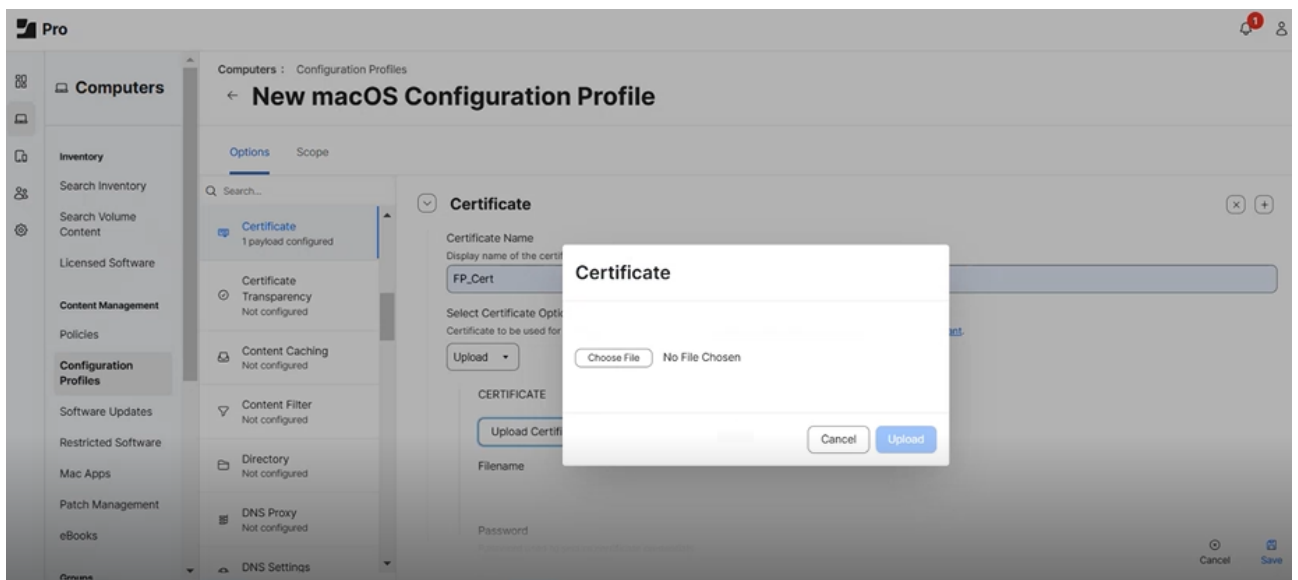
- 5) In **Certificate**, click **Configure** in **Configure Certificate**.



- 6) In the **Certificate** pane, enter the certificate name.



- 7) In **Select Certificate Option**, select **Upload**.



- 8) Click **Choose File** and select the `_ca.cer` file.
- 9) Click **Upload**.
- 10) Click **Save**.
The configuration profile is pushed to the endpoint.

Deploying Privacy Preferences Policy Control (pppc) profile

You must deploy a Privacy Preferences Policy Control (PPPC) profile to automatically enable Full Disk Access (FDA) and the fpneone process.

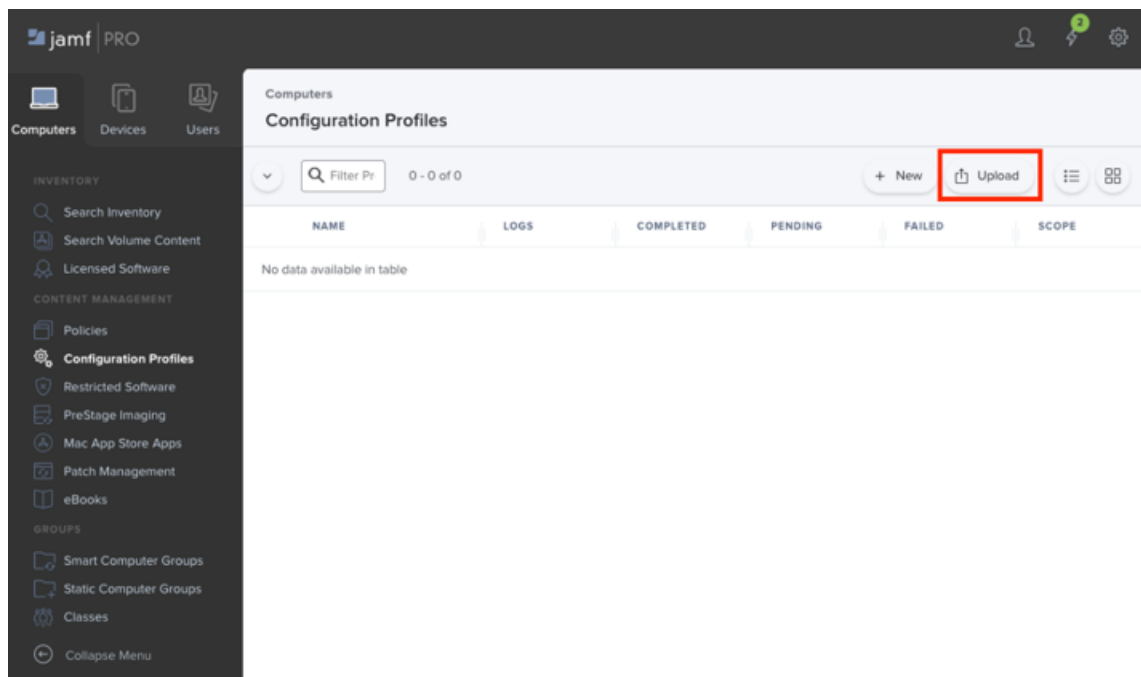
Before you begin

Download the agent configuration profile `Forcepoint DLP Endpoint PPC profile.mobileconfig` [here](#).

Deploying the attached PPC profile will configure Full Disk Access (FDA) for files required for Forcepoint DLP Endpoint to function and enables the fpneone process in **System Preferences**.

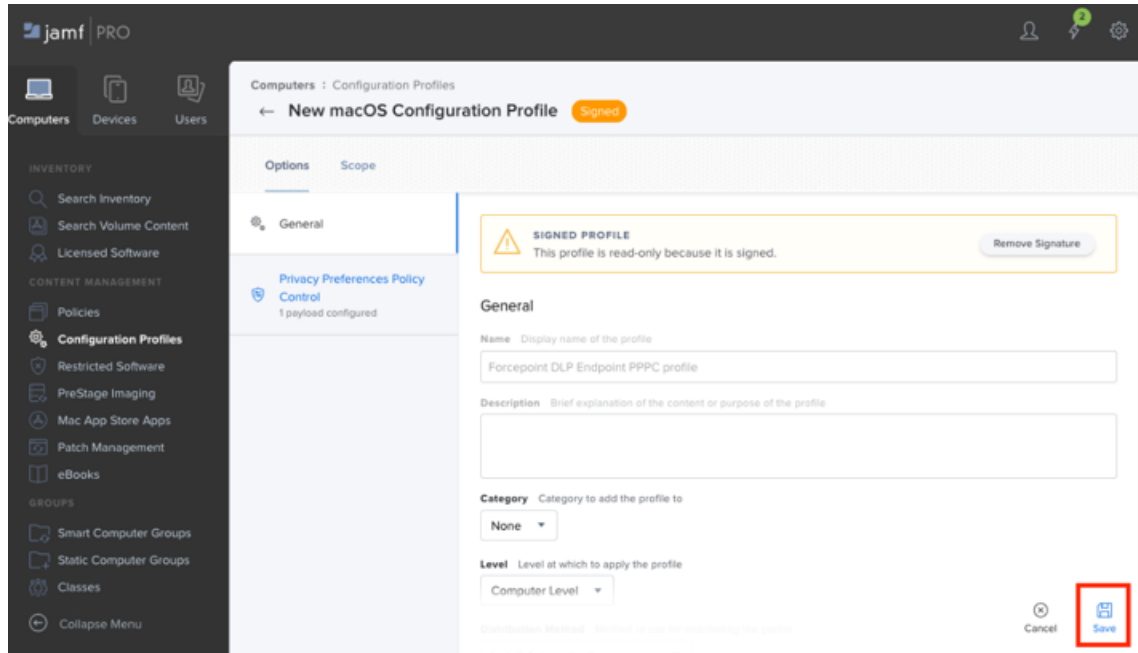
Steps

- 1) Open Jamf Pro, enter the administrator name and password, and then click **Log in**.
- 2) On the **Computers** tab, select **Configuration Profiles**, then click **Upload**.

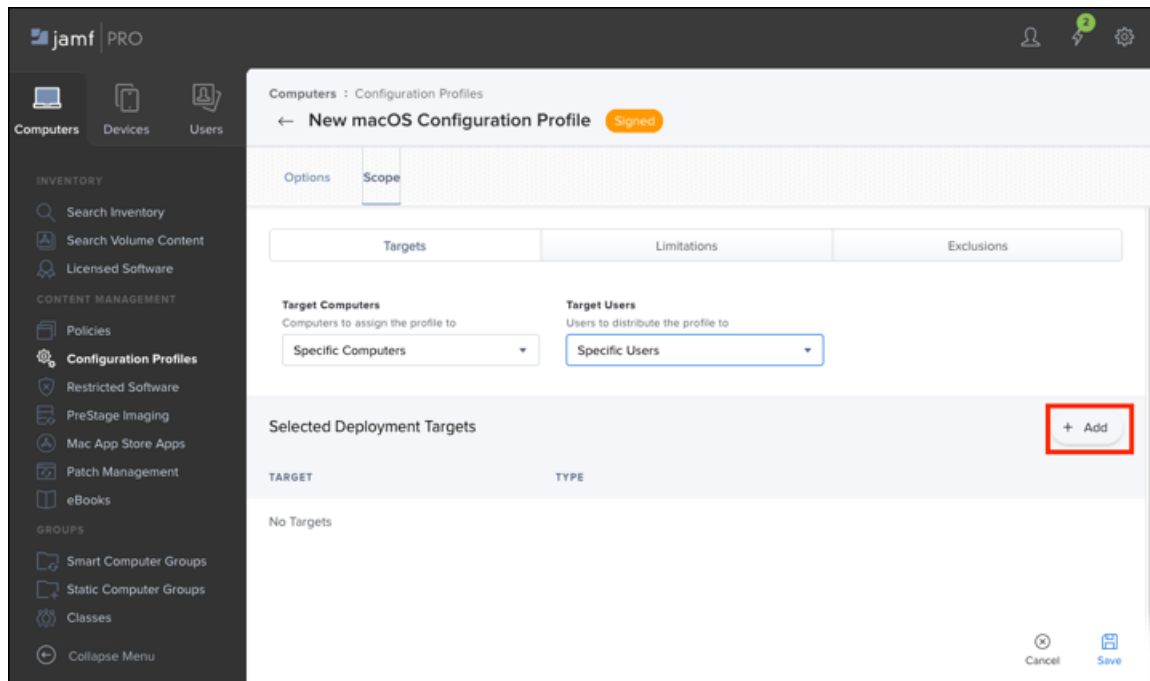


- 3) To import the agent configuration profile file `Forcepoint DLP Endpoint PPC profile.mobileconfig` into Jamf Pro, click **Upload**.

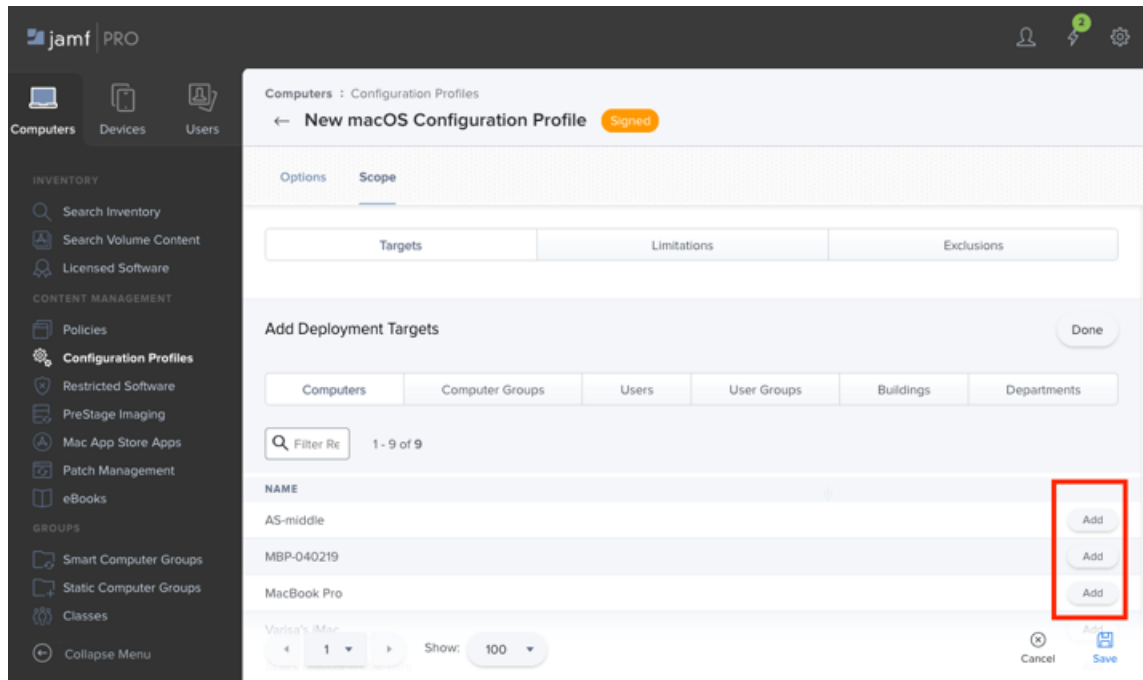
- 4) Select the Forcepoint DLP Endpoint PPC profile.mobileconfig file, and then click **Save**.



- 5) After the file has been uploaded successfully, select the **Scope** tab, and click **Add** to add one or more enrolled targets (i.e. endpoint machines) to use this policy.

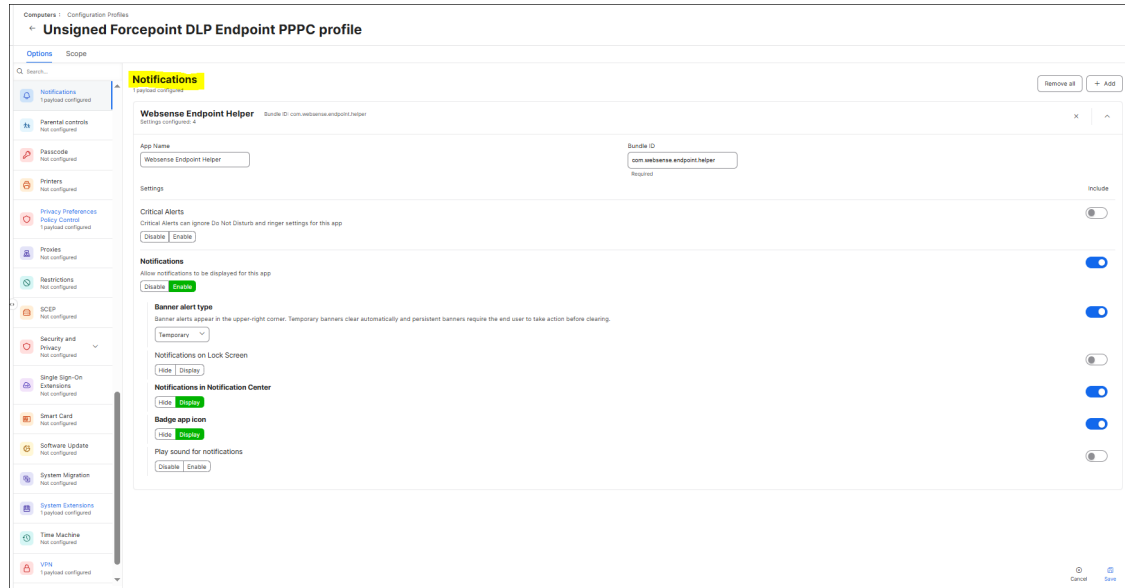


- 6) On the **Add Deployment Targets** screen, click **Add** next to each target machine to enroll in the policy.



- 7) To force the Forcepoint F1E to run in the background, add the team identifier in the profile.
- 8) After all targets have been added to the policy, click **Save**.
- 9) Return to the **Configuration Profiles** screen and verify that the policy is listed as **Completed** for the enrolled targets.
If any targets display a **Pending** status, you must log out of the target and then log in again until the status displays as **Completed**.
- 10) To ensure all notifications are displayed in the macOS Notification Center, follow the below steps:
- In **Options**, search for and select **Notifications**.
 - Under **Allow notifications to be displayed for this app**, turn on the **Enable** toggle.

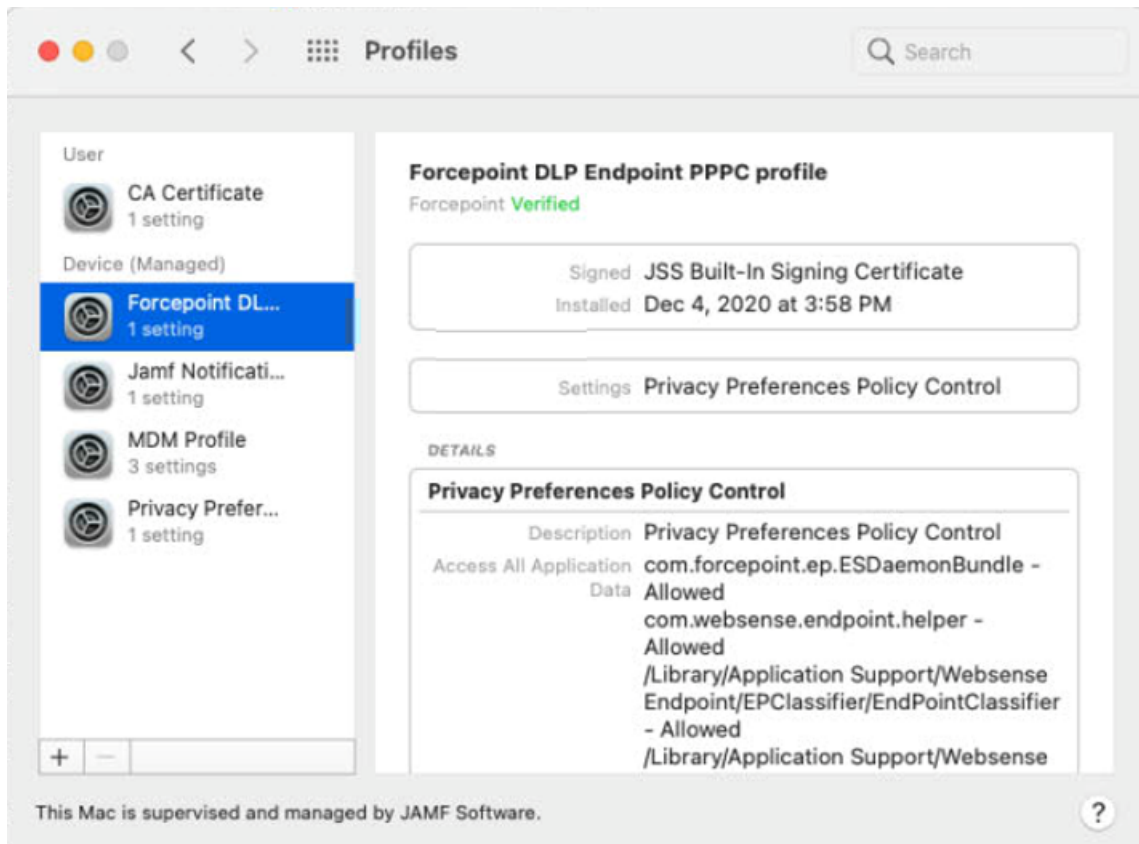
c) Under **Notifications in Notification Center** and **Badge app icon**, turn on the **Display** toggles.



Note

Starting from 25.09, block notifications will appear in the macOS Notification Center.

- 11) To verify that the profile has been loaded successfully on the target machine, do the following:
- Open the **Profiles** preference page within the macOS System Settings under Privacy and Security. If the profile loaded successfully on the machine, then the **Forcepoint DLP Endpoint PPC** profile policy is present.



Related tasks

Forcing the allowance for Forcepoint F1E agent to run in the background on page 93

Forcing the allowance for Forcepoint F1E agent to run in the background

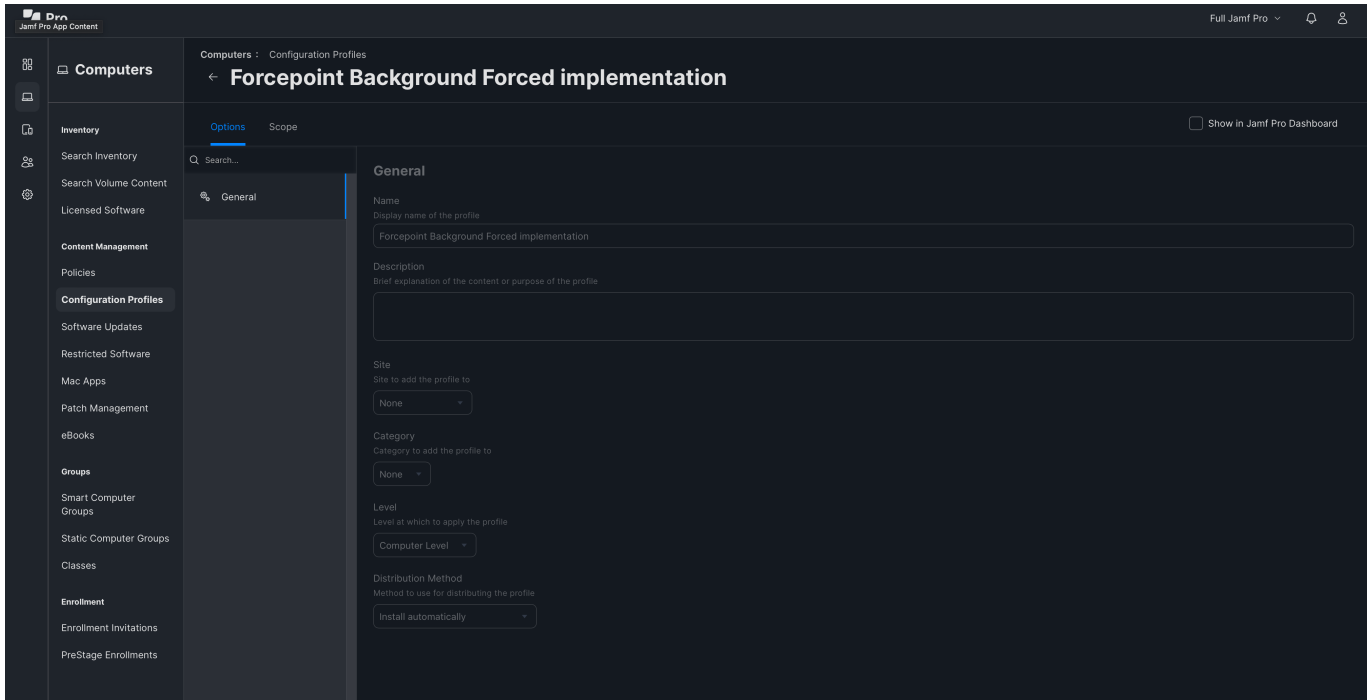
To ensure the Forcepoint F1E agent runs in the background, is forced and cannot be manually disabled by end users, you must add the **Team Identifier** to the **Managed Login Items** section of your pppc profile.

If the Forcepoint F1E agent is disabled in **System Preferences > General > Login Items > Allow in the Background**, the agent fails to run after a system restart. Using Jamf, you can configure the profile, and force the switch to enable the Forcepoint F1E agent.

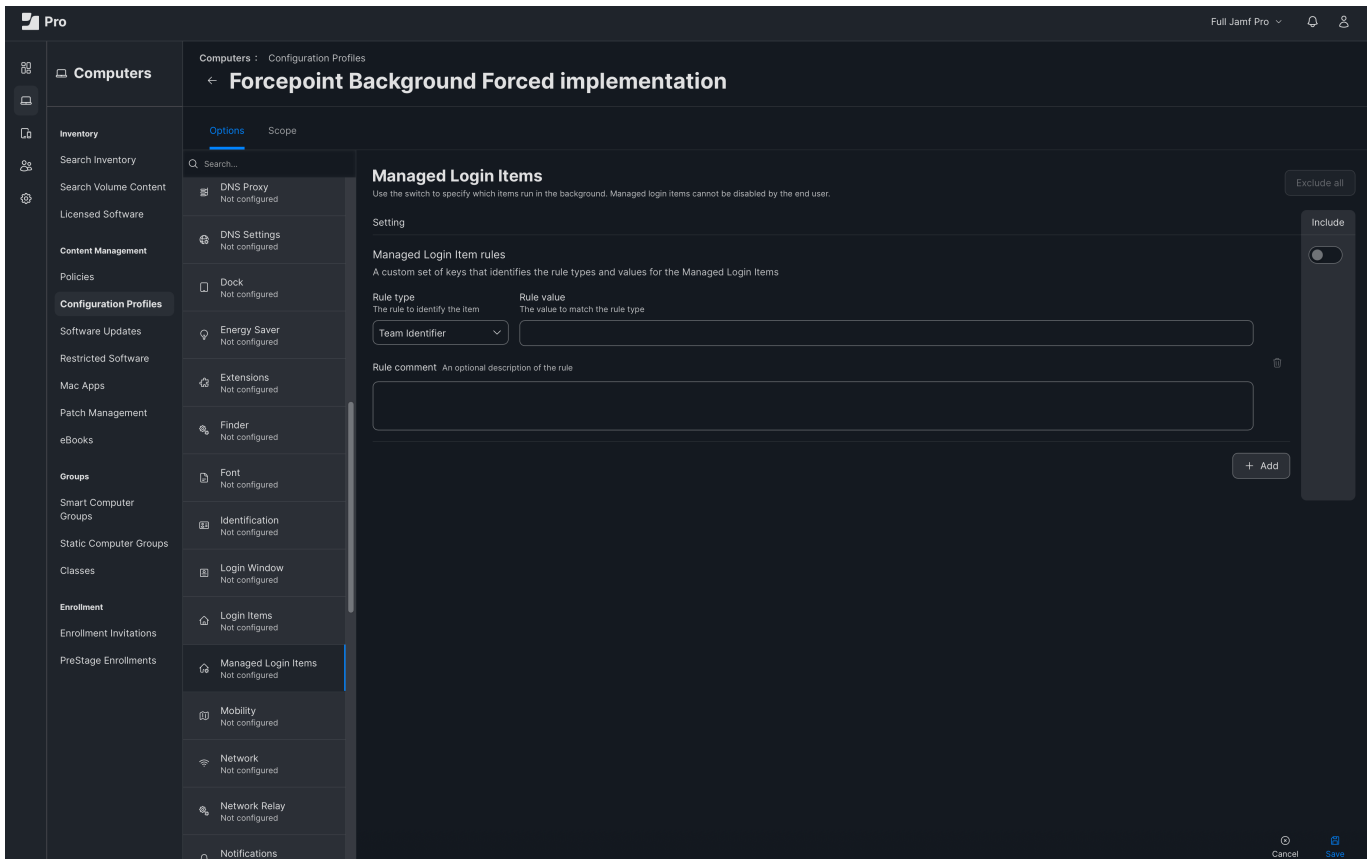
Steps

- 1) Open Jamf Pro, enter the administrator name and password, and then click **Log in**.
- 2) On the **Computers** tab, select **Configuration Profiles**.

3) Create a new profile and enter the appropriate name.



4) In the sidebar, locate and select the **Managed Login Items** section. The **Managed Login Items** section opens.

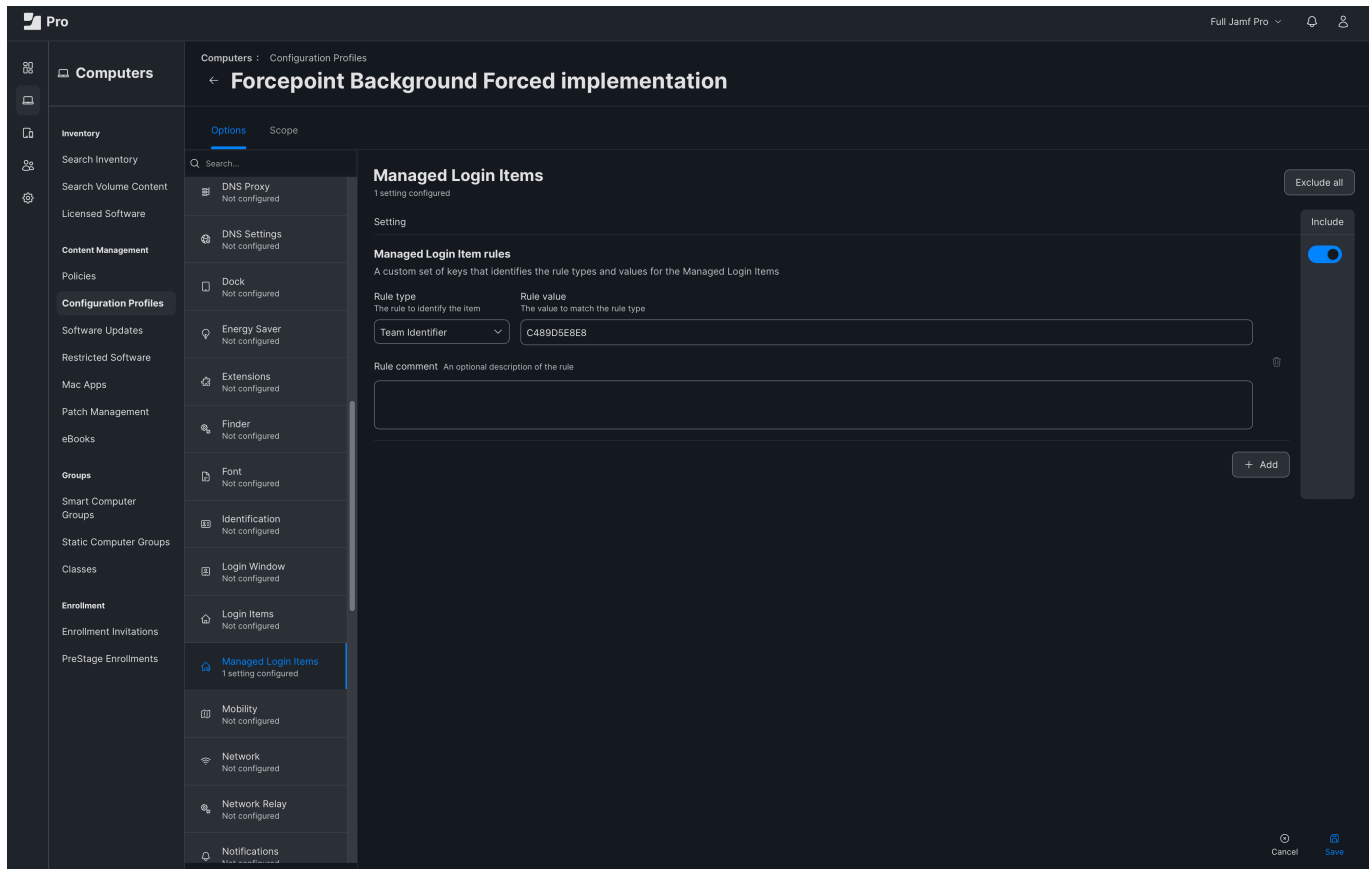


5) Turn on **Include**.

6) In **Rule Type**, select **Team Identifier**.

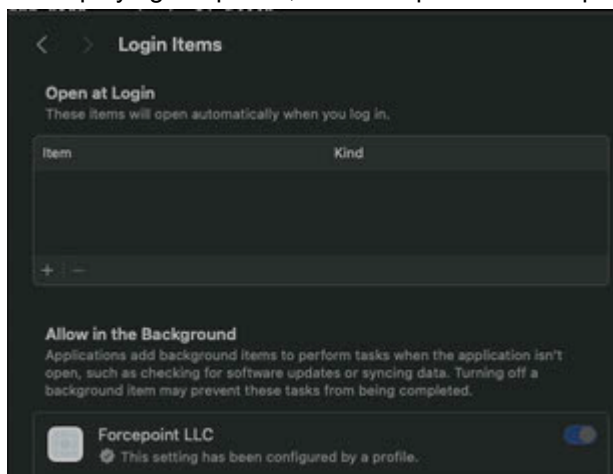
7) In **Rule Value**, enter the F1E team identifier ID as **C489D5E8E8**.

You can also copy the team identifier ID from the **System Extensions** tab, and then paste it in **Rule Value**.



8) Click **Save**.

On deploying the profile, the Forcepoint F1E endpoint switch is enabled in **Allow in the Background**.



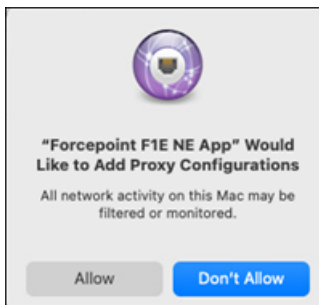
Configuring content filters

You can use content filters to configure application access prior to performing F1E upgrades and allow for silent installations.

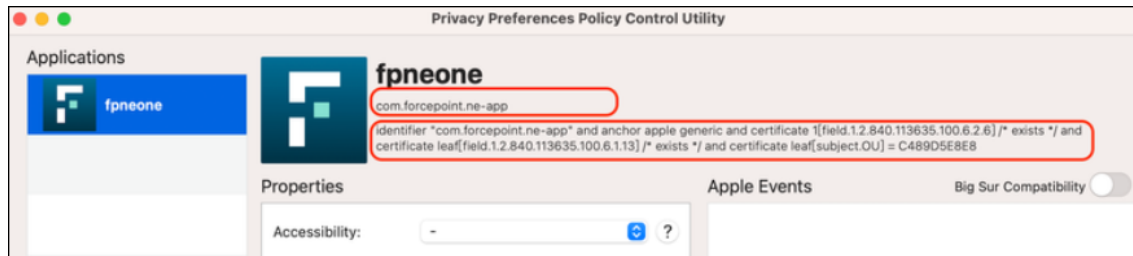
In order to suppress any dialogs related to the **fpneone** process on F1E v22.12 and later (for example, dialogs such as "Forcepoint F1E NE App" Would Like to Add Proxy Configurations"), Forcepoint recommends that you perform the following prior to an upgrade of F1E:

Steps

- 1) In the Jamf Pro server, on the **Privacy Preferences Policy Control** tab, define the following component for application access:
 - a) **Identifier:** com.forcepoint.ne-app
 - b) **Identifier Type:** Bundle ID
 - c) **Code Requirement:** identifier "com.forcepoint.ne-app" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "C489D5E8E8"
- 2) Allow access and then push out the policy.



- 3) To deploy a profile to the endpoint by configuring the Content Filter payload and adding the proxy configurations automatically, do the following:
 - a) Open the Privacy Preferences Policy Control (PPPC) Utility in Jamf and identify the app **Identifier** and its **Code** information.
 For example, in the below screenshot, the identifier is "com.forcepoint.ne-app" and the code is "identifier "com.forcepoint.ne-app" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = C489D5E8E8".



- b) Create a new profile or to edit an existing PPPC/KEXT profile in Jamf Pro, select **Configuration Profiles** in **Computers**, and choose the **Forcepoint DLP Endpoint PPPC profile.mobileconfig** file.

- c) In **Options**, select **Content Filter**.

Computers : Configuration Profiles

← **Forcepoint DLP Endpoint PPPC profile**

Options Scope ☐ Show in Jamf Pro Dashboard

Search...

General

Certificate
1 payload configured

Content Filter
Settings configured: 6

Privacy Preferences
Policy Control
1 payload configured

System Extensions
1 payload configured

VPN
1 payload configured

Content Filter
Settings configured: 6

Filter Name
Display name of the filter in the app and on the device
Forcepoint F1E

Identifier
Identifier for the filter plug-in
com.forcepoint.ne-app

Organization
Organization for the filter plug-in
Forcepoint LLC

Filter Order
Specify the order in which traffic is filtered. Filters with a grade of firewall see network traffic before filters with a grade of inspector.
Firewall

Socket Filter
Specify filtering of socket traffic
Enabled

Socket Filter Bundle Identifier Bundle identifier of the socket filter provider system extension
com.forcepoint.ne-app

Socket Filter Designated Requirement Designated requirement of the socket filter provider system extension
identifier "com.forcepoint.ne-app" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = C489D5E8E8

Network Filter
Specify filtering of network packets
Enabled

Network Filter Bundle Identifier Bundle identifier of the network filter provider system extension
com.forcepoint.ne-app

Network Filter Designated Requirement Designated requirement of the network filter provider system extension
identifier "com.forcepoint.ne-app" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = C489D5E8E8

- d) In **Identifier**, enter the app Identifier name.
- e) Ensure **Socket Filter** is enabled, and enter the identifier name in the **Socket Filter Bundle Identifier** field and the code value in the **Socket Filter Designated Requirement** field.
- f) Ensure **Network Filter** is enabled, and enter the identifier name in the **Network Filter Bundle Identifier** field and the code value in the **Network Filter Designated Requirement** field.
- A new proxy setting is added and enabled, and no dialog appears during the installation.

Manually creating the MDM profile

You can manually create the mobile device management (MDM) profile if you have issues importing the MDM profile provided by Forcepoint.

In order to suppress any dialogs related to the "fpneone" and "Forcepoint Neo NE App" processes, you can manually create the MDM profile. Do the following prior to upgrade:

Steps

- 1) Log in to the Jamf Pro server.

- 2) On the **Computers** tab, select **Configuration Profiles**, and then click **New**.

NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
No category assigned					
Disable Screen Capture and Recording	View	0	0	0	No scope defined
F1E System Extension - Uninstallation (Alpha)	View	2	0	0	2 computers
Forcepoint DLP Endpoint PPPC profile	View	1	0	0	1 computer
Forcepoint Neo	View	2	0	0	2 computers
ForcepointDLPChromeExtension	View	0	0	0	No scope defined
ForcepointDLPChromeExtension (DKG ID)	View	0	0	0	No scope defined
ForcepointDLPFirefoxExtension	View	0	0	0	No scope defined
Outlook Add-in	View	0	0	0	No scope defined
Unsigned Forcepoint DLP Endpoint PPPC profile	View	2	1	0	3 computers

- 3) To create a new configuration profile, provide the required details under **General**.

General

Name Display name of the profile

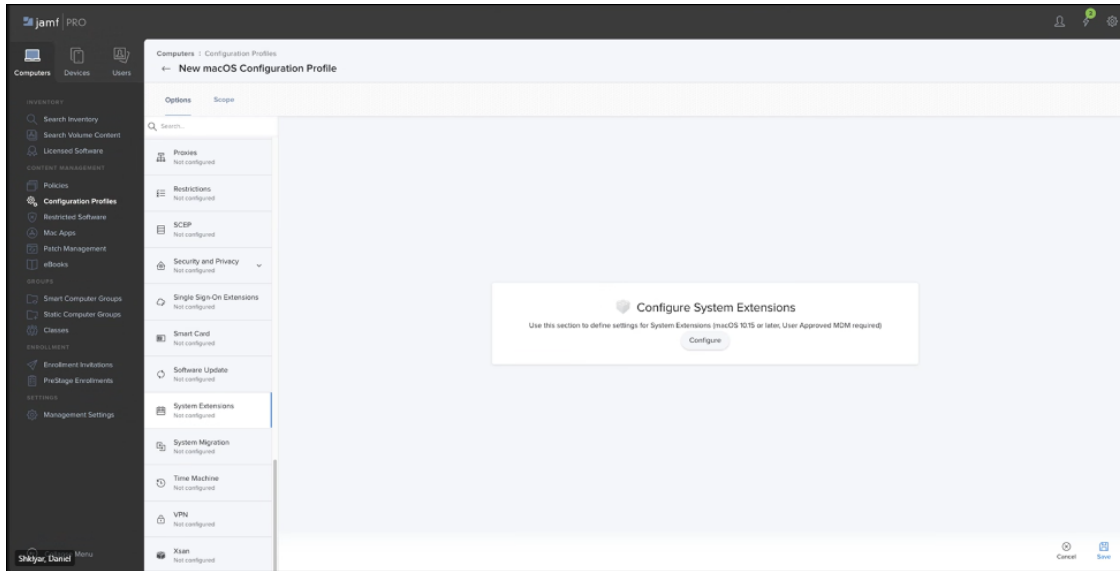
Description Brief explanation of the content or purpose of the profile

Category Category to add the profile to

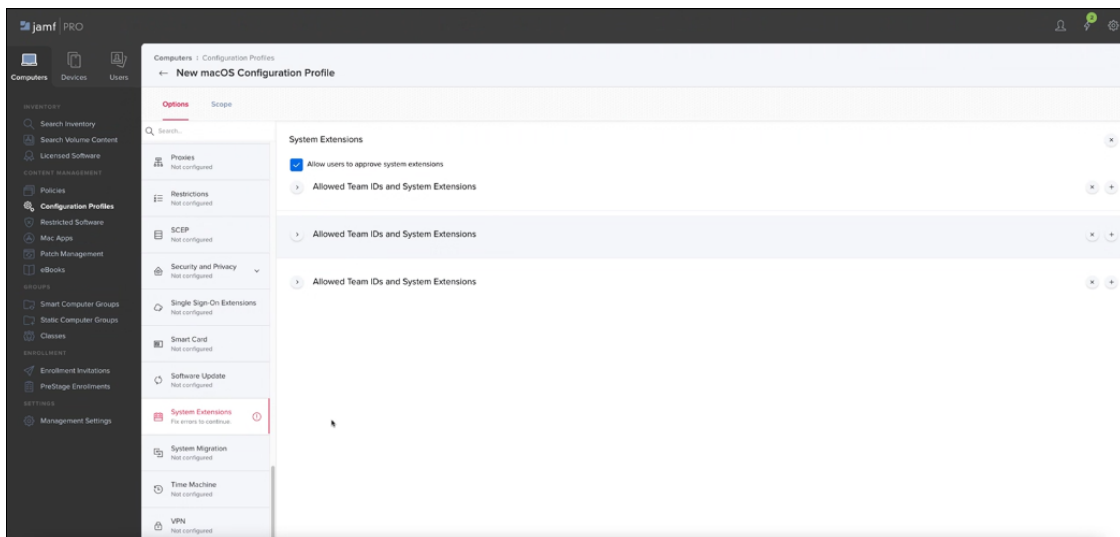
Level Level at which to apply the profile

Distribution Method Method to use for distributing the profile

4) Under **System Extensions**, click **Configure**.



5) Add three System Extension objects, using the **+** button.

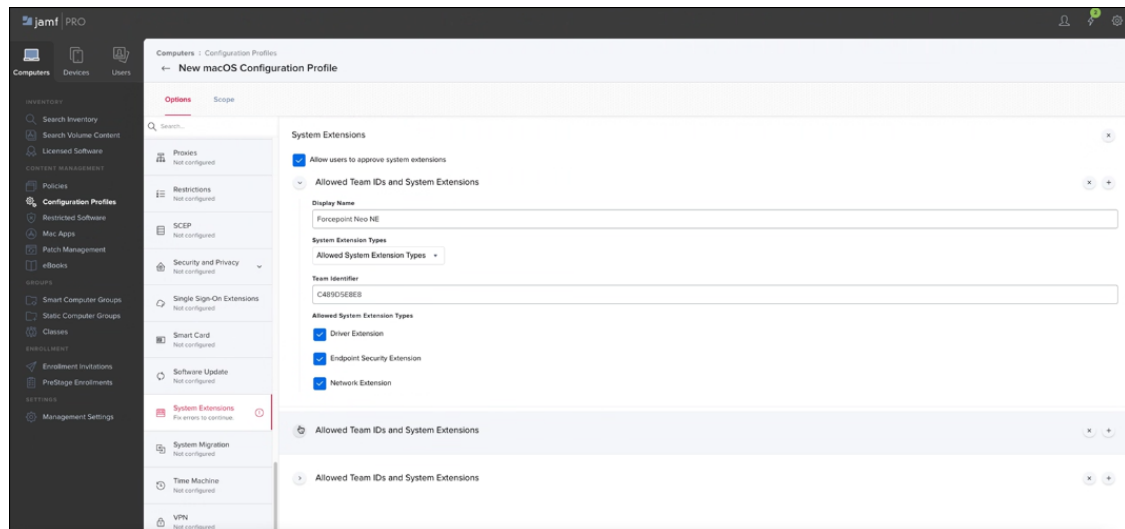


6) Modify the first extension as the following:


- a) In **Display name**, enter Forcepoint Neo NE.
- b) In **System Extension Type**, enter Allowed System Extensions.
- c) In **Team Identifier**, enter C489D5E8E8.

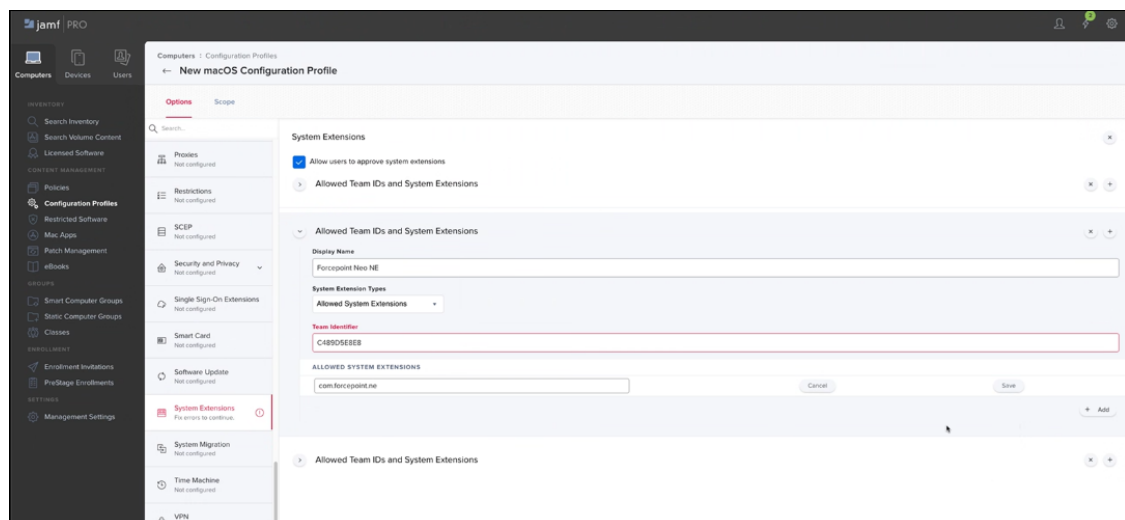
d) Under the **Allowed System Extension Types**, select the below options.

- **Driver Extension**
- **Endpoint Security Extension**
- **Network Extension**




7) Modify the second extension as the following:

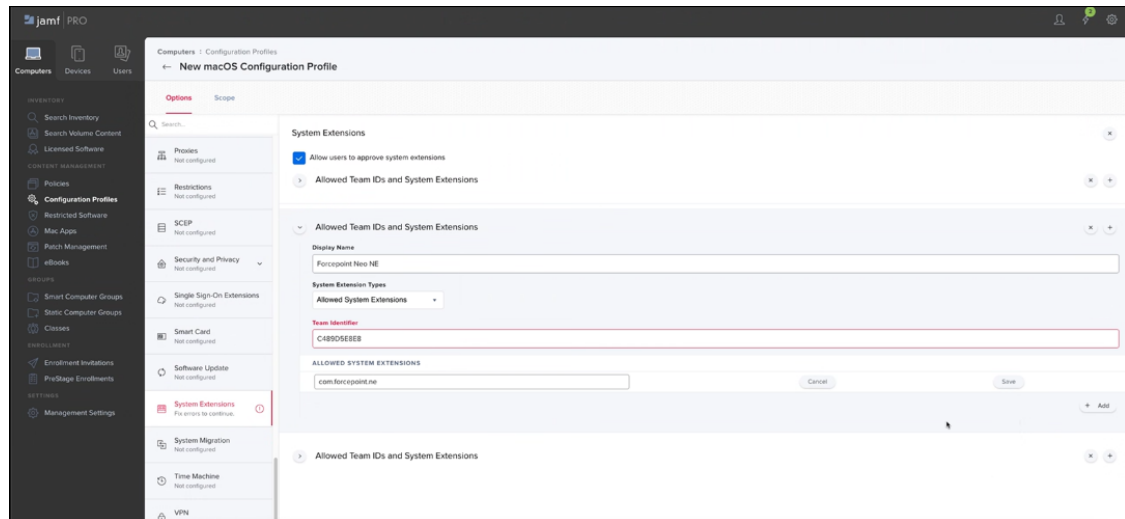
- a) In **Display name**, enter Forcepoint Neo NE.
- b) In **System Extension Type**, enter Allowed System Extensions.
- c) In **Team Identifier**, enter C489D5E8E8.
- d) Click the  button for this object, and enter the value: com.forcepoint.ne.



8) Modify the third extension as the following:

- a) In **Display name**, enter Forcepoint Neo NE.

- b) In **System Extension Type**, enter Removable System Extensions.
- c) In **Team Identifier**, enter C489D5E8E8.
- d) Click the  button for this object, and enter the value: com.forcepoint.ne.



- 9) In **VPN**, click **Configure**.
- 10) Enter the following values:
 - **Connection name**: Forcepoint Neo
 - **VPN Type**: VPN
 - **Connection Type**: Custom SSL
 - **Identifier**: com.forcepoint.ne-app
 - **Server**: Forcepoint Neo
 - **Provider Bundle Identifier**: com.forcepoint.ne
 - **Provider Type**: App-proxyEnable

11) Select the following fields:

- **Include All Networks**
- **Exclude Local Networks**
- **Enable VPN on Demand**
- **Prohibit users from disabling on-demand VPN settings**

Computers : Configuration Profiles

← Unsigned Forcepoint DLP Endpoint PPC profile

Options Scope

Search...

Log in Items
Not configured

Log in Window
Not configured

Managed Log in Items
Not configured

Mobility
Not configured

Network
Not configured

Notifications
Not configured

Parental Controls
Not configured

Password
Not configured

Printing
Not configured

Privacy Preferences
Policy Control
1 payload configured

Proxies
Not configured

Restrictions
Not configured

SCEP
Not configured

Security and Privacy
Not configured

Single Sign-On
Extensions
Not configured

Smart Card
Not configured

Software Update
Not configured

System Extensions
1 payload configured

System Migration
Not configured

Time Machine
Not configured

VPN
1 payload configured

Xsan
Not configured

VPN

Connection Name Display name of the connection (displayed on the device)
Forcepoint Neo

VPN Type The type of VPN connection to configure
VPN

Connection Type The type of connection enabled by this policy
Custom SSL

Identifier Identifier for the custom SSL VPN
com.forcepoint.ne-app

Server Hostname or IP address for server
Forcepoint Neo

Account User account for authenticating the connection

Provider Bundle Identifier Bundle identifier for the selected VPN provider
com.forcepoint.ne

Custom Data Keys and string values for custom data
KEY

User Authentication Authentication type for the connection
Password

Password Password for authenticating the connection

Verify Password

Provider Type Type of tunnel for network traffic
App-proxy

☒ **Include All Networks** Routes all traffic through the VPN

☒ **Exclude Local Networks** Routes all local network traffic outside the VPN

Provider Designated Requirement

☒ **Enable VPN on Demand** Domain and host names that will establish a VPN

☒ **Prohibit users from disabling on-demand VPN settings**

Idle Timer The length of time to wait before disconnecting a VPN connection
Do not disconnect

Proxy Setup Configures proxies to be used with this VPN connection
None

Deploying extensions

You can automatically deploy the extensions on the endpoint machines to ensure consistent extension configuration across devices.

Before you deploy the extensions using Jamf, note the following limitation for Forcepoint F1E installations on macOS:

- If the browser extension is installed through Jamf, it cannot be disabled through the **Endpoint Profiles** setting in Forcepoint DLP on the Forcepoint Security Manager. Endpoint Profiles can still be used to configure whether the extension runs in Enabled (blocking) mode or Monitoring only mode.

If you are managing any endpoint machines that are running macOS 10.15 (Catalina) or lower, you need to disable the automatic installation of the browser extension by the Forcepoint F1E installer package, because this may override the policy pushed to your endpoint machines by Jamf.

Deploying Chrome extension

You can deploy Chrome extensions to manage extensions alongside the F1E Endpoint agent installation.

To deploy the Chrome extension for Forcepoint DLP Endpoint using Jamf, do the following:

Steps

- 1) Download the `ProfileToDeployChromeExtension.mobileconfig` file from [here](#).
- 2) Sign in to your Jamf Pro server administration portal.
- 3) In the Jamf Pro server administration portal, navigate to **Computers > Content Management > Configuration profiles**, and then click **Upload**.
- 4) Upload `ProfileToDeployChromeExtension.mobileconfig`.
- 5) After the mobileconfig file is uploaded successfully, select the **Scope** tab, then click **Add** to add one or more enrolled target (such as an endpoint machine) to use this policy.
- 6) After you add the targets, return to the **Configuration Profiles** screen and verify that the policy is listed as **Pending** for the enrolled targets.
- 7) On each target, log out, and then log in again.
After the target has logged in again, the **Configuration Profile** screen shows that the policy is listed as **Completed**.
- 8) To verify, open the **Profiles** preference page in the **Settings** application on the target.
If the profile loads successfully on the target, the policy appears.



See [Disable/Enable Chrome Extension in DLP Endpoint \(Windows and macOS\)](#) for steps to disable the automatic installation of the Forcepoint Chrome Extension.

For information on deploying the Chrome extension for Forcepoint DLP Endpoint using Intune, see [Deploying the Forcepoint Chrome Extension Using Intune](#).

Deploying Firefox extension

The Firefox extension is built-in to the installer package for deployment.

Deploying the endpoint package through Jamf

You can automatically deploy endpoint packages using Jamf.

Steps

- 1) Once the package is built with the Forcepoint Package builder, upload the file using Casper admin. For information, see the [Jamf Pro Administrator's Guide](#) for the version in use.
- 2) Create a policy to deploy the ZIP archive, ideally with a smart or static group.

- 3) Make a second policy that looks for the package already installed that runs a bash script to run the installer with the sudo prefix:

```
sudo unzip ./FORCEPOINT-ONE-ENDPOINT-Mac.zip
```

```
sudo installer -package ./EndpointInstaller/WebsenseEndpoint.pkg -target /
```



Note

Update the paths or file names as needed.

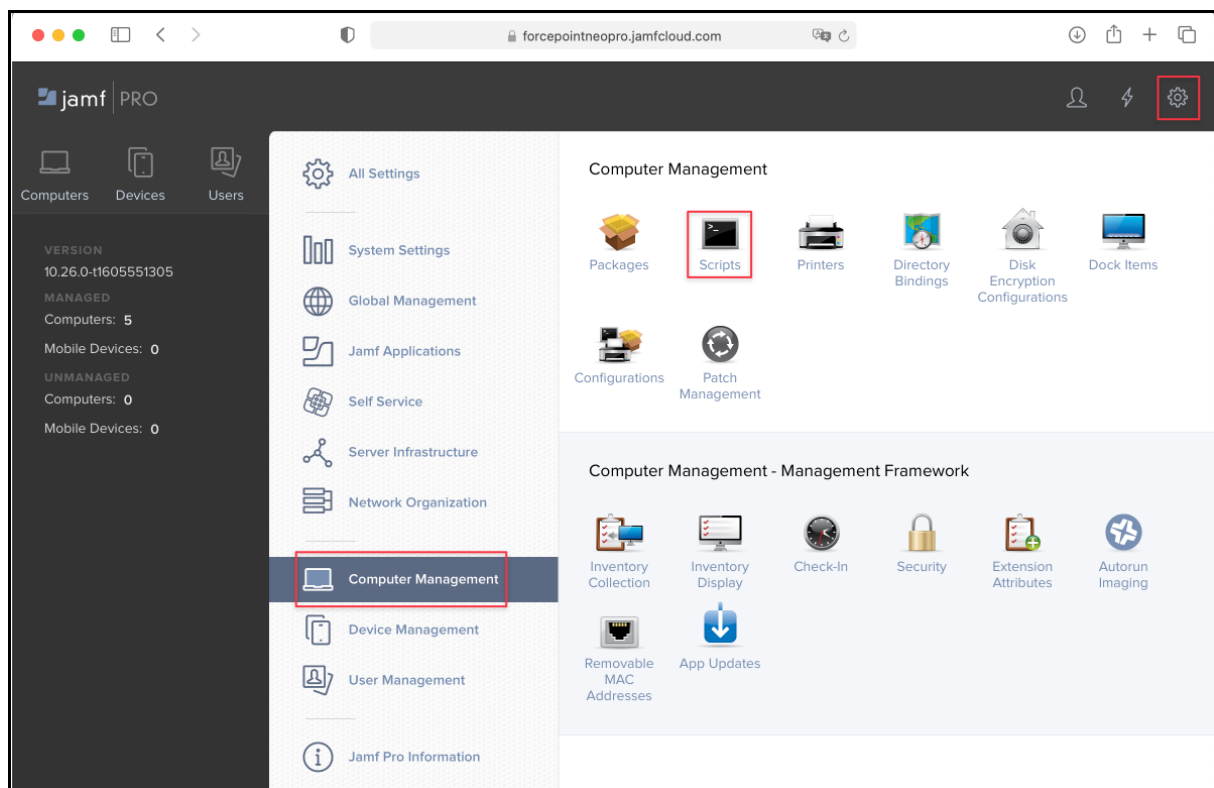
`WebsenseEndpoint.pkg` (not `WebsenseEPClassifier.pkg`) contains the installer and will call on the other files from the zip, so run the command inside the directory where the zip has been extracted.

Uninstalling the agent using Jamf

You can use jamf to automatically uninstall the Forcepoint F1E agent on your endpoint machines. Create a Jamf policy to uninstall the agent from your endpoint machines.

Steps

- 1) Sign in to Jamf Pro and go to **Computers > Settings**.
- 2) Open **Computer Management > Scripts**, then click **New**.



- 3) Under **Display Name**, enter the script name. For example, `uninstall_F1E.sh`.

The screenshot shows the Jamf Pro web interface in a browser window. The address bar shows `forcepointneo.jamfcloud.com`. The left sidebar contains the Jamf Pro logo and navigation icons for Computers, Devices, and Users. The main content area is titled 'Settings : Computer Management > Scripts' and shows the configuration for a script named 'run_uninstall_app.sh'. The 'General' tab is selected, showing fields for 'Display Name' (set to 'run_uninstall_app.sh'), 'Category' (set to 'None'), 'Information' (a large text area), and 'Notes' (a large text area). At the bottom right, there are 'Cancel' and 'Save' buttons.

jamf PRO

Full Jamf Pro

Computers Devices Users

VERSION
10.26.0-t1605551305

MANAGED
Computers: 28
Mobile Devices: 0

UNMANAGED
Computers: 3
Mobile Devices: 0

Settings : Computer Management > Scripts

← run_uninstall_app.sh

General Script Options Limitations

Display Name Display name for the script

run_uninstall_app.sh

Category Category to add the script to

None

Information Information to display to the administrator when the script is run

Notes Notes to display about the script (e.g., who created it and when it was created)

Cancel Save

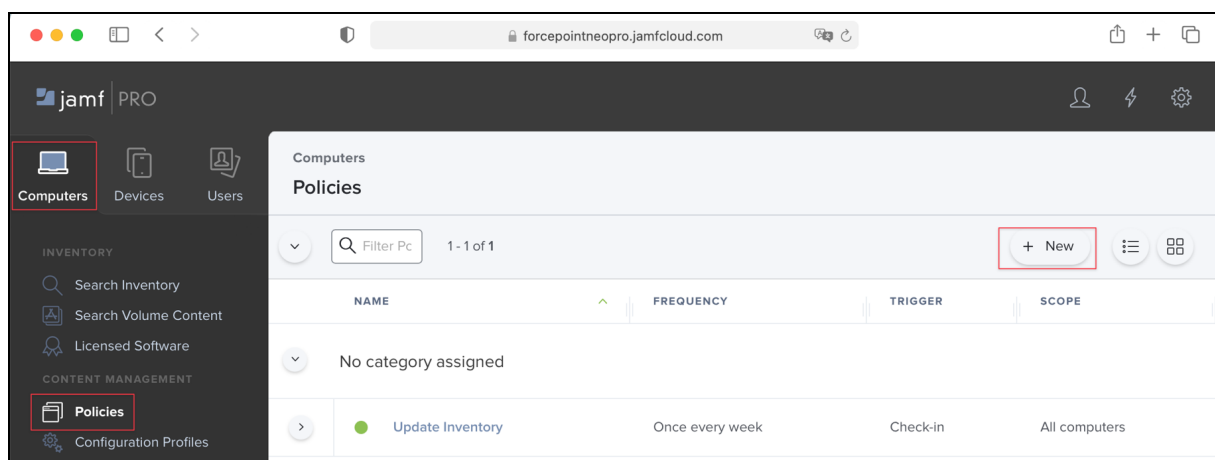
- 4) On the **Script** tab, login as root and enter the script attached [here](#).

```

1  #!/bin/bash
2
3  # Script written by Sebastian Santos in January 2019
4  # Note: Please do not remove the author's name from this script.
5  # Updated by sebastian santos Script cember 8 2023
6  # Check for root privileges
7  if [ "$EUID" -ne 0 ]; then
8      echo "Please run as root."
9      exit 1
10 fi
11
12 # Log file path
13 logFilePath="/var/log/F1EDLP.log"
14
15 # Check if Forcepoint DLP Endpoint is installed
16 if [ -d "/Applications/Forcepoint DLP Endpoint.app" ]; then
17     # Get the installed version
18     AppVersion=$(/usr/bin/defaults read "/Applications/Forcepoint DLP Endpoint.app/Contents/Info.plist" CFBundleShortVersionString)
19
20     # Check if the version is one of the specified versions
21     #if [[ $AppVersion == "23.04.0377" || $AppVersion == "23.10.0385" || $AppVersion == "23.11" ]]; then #Make sure you add the full version pf DLP you are trying to uninstall
22         # Uninstall if version matches
23         # password="forcepoint" # Adjust the password as needed
24         # echo "Uninstalling DLP version $AppVersion"
25     #else
26         # Uninstall if version doesn't match
27         # password="forcepoint" # Adjust the password as needed
28         # echo "Uninstalling older version of DLP"
29     #fi
30     password="forcepoint"
31     # Perform the uninstallation
32     if echo "$password" | sudo -S /usr/local/sbin/wepsvc --uninstall --password "$password"; then
33         echo "$(date '+%Y-%m-%d %H:%M:%S') - Uninstalled DLP version $AppVersion" >> "$logFilePath"
34     else
35         echo "Failed to uninstall DLP version $AppVersion"
36         exit 1
37     fi
38 else
39     # If Forcepoint DLP Endpoint is not installed
40     echo "Forcepoint DLP Endpoint is not installed"
41 fi
42
43 # Display a pop-up window notifying the user about the upcoming restart
44 osascript -e 'display dialog "F1E was uninstalled successfully" buttons {"OK"} default button "OK" with title "Uninstall"'
45
46
47 exit 0

```

- 5) Click **Save**.
- 6) Open **Computers > Policies**, then click **New**.

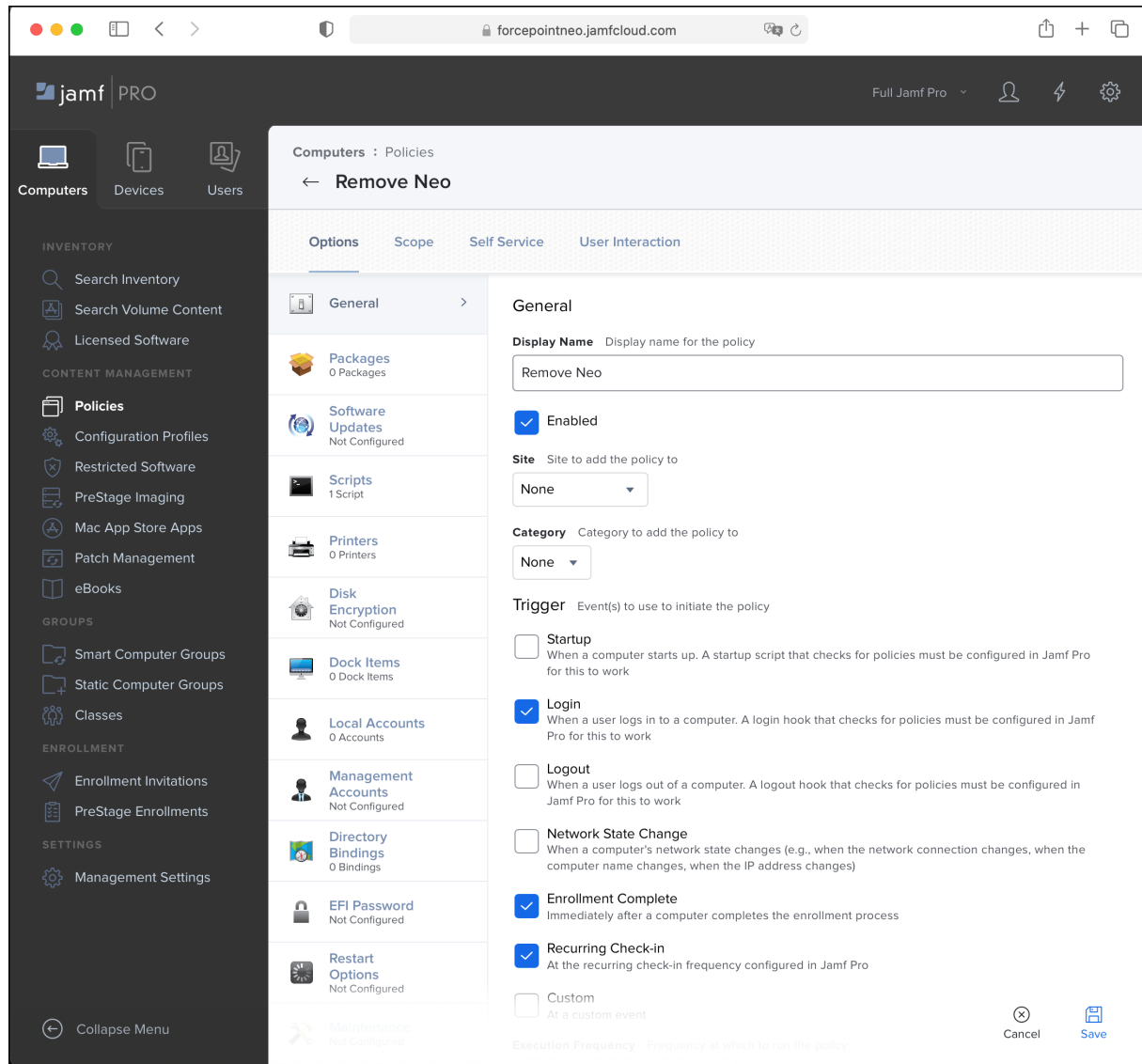


- 7) Enter the following details:

a) **Display Name:** Remove F1E

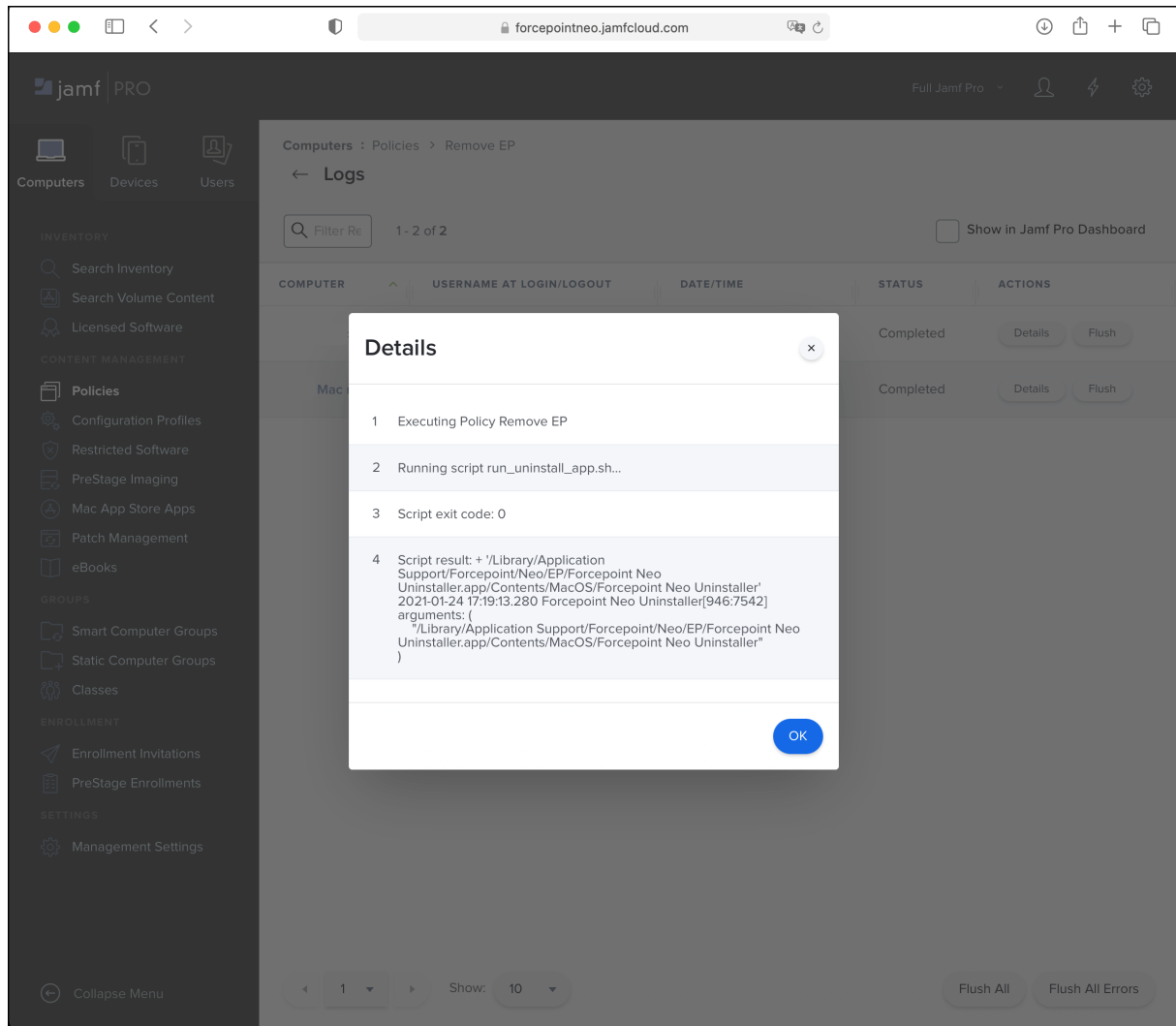
b) Select the **Enabled** check box

c) Under **Trigger**, select **Login**, **Enrollment Complete**, and **Recurring Check-in**.



8) On the **Scripts** tab, click **Configure Scripts** and add the script created above.

9) On the **Scope** tab, select **All Computers** and **All Users**.



Note

Alternatively, use this tab to specify certain individuals or groups from which to uninstall the agent.

10) Click **Save**.

11) Click **Logs** to verify the uninstallation.



Note

To troubleshoot uninstall issues on endpoints, open the `/Library/Logs/com.forcepoint.neo/uninstall/uninstall.log` file.

Silently upgrading Forcepoint F1E using MDM

You can silently upgrade Forcepoint F1E endpoint installation using mobile device management (MDM).

If FSM 10 was installed before F1E v23.11 release, switching to Network Proxy mode requires a manual minor update of the profile on the FSM site. After v23.11 F1E clients are upgraded on the endpoints, a simple modification, for example, profile description adjustment is adequate to increment the profile version.

If FSM 10 is upgraded concurrently with the F1E v23.11 release, ensure that the profile is configured to be in Browser Extensions mode until the F1E clients are updated to v23.11. Once v23.11 is installed on the endpoints, the FSM profile should be changed to Network Proxy mode.

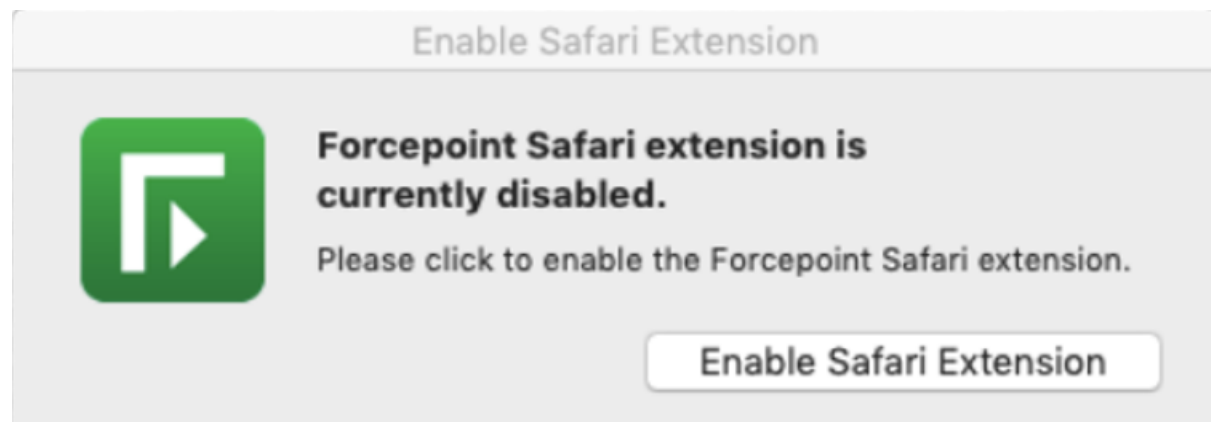
Steps

- 1) On FSM 10 or later, setup your profile to be in browser extensions mode.
- 2) Upgrade to latest F1E version with latest classifier using MDM for silent install.
- 3) Switch Web Traffic Detection Mode to Inline Proxy.
- 4) Update your profile.
- 5) Open browsers, and verify if extensions are removed.
- 6) Open Activity Monitor, and ensure the `fpnpsd` process is running.

Enabling Safari extension manually

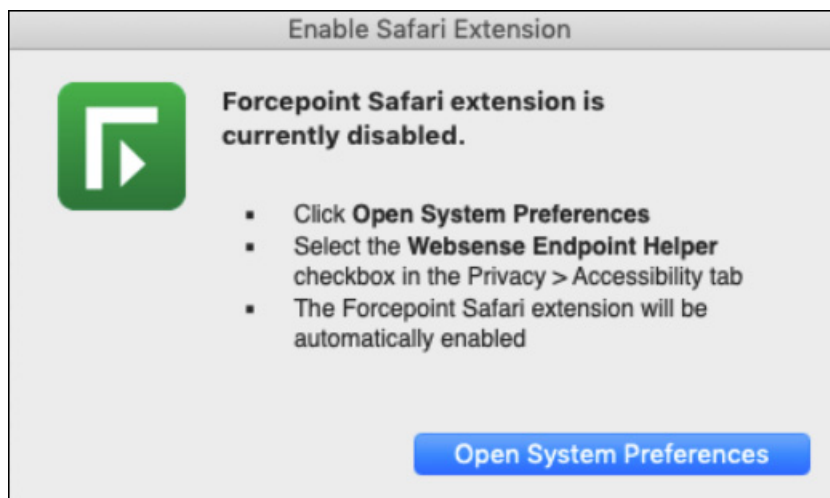
The Forcepoint DLP Endpoint Safari extension must be enabled for Safari 12 and above on macOS environments v10.14 and above.

If the Forcepoint Safari extension is disabled on a Jamf-managed endpoint machine, the following notification displays when you open the Safari browser:



On Jamf-managed environments, unlike the process for Firefox and Chrome, it is not possible for the Forcepoint Safari Extension to be silently enabled in a similar manner. The user must select the **Enable Safari Extension** option within the popup window and enable the Safari extension from the Extension window that opens.

If the endpoint machine is not JAMF managed, the following notification displays when you open the Safari browser:



To enable the Forcepoint Safari extension from this notification, click the **Open System Preferences** button and select the **Websense Endpoint Helper** check box in the **Accessibility** tab in **Privacy**. Then, the Forcepoint Safari extension is automatically enabled.

Apple has made it a requirement for any Safari extensions to not be loaded without the user's consent. Therefore in modern macOS and Safari versions, it is not possible to enable a Safari extension without the user personally enabling it.

Related tasks

[Deploying Chrome extension](#) on page 103

[Deploying Firefox extension](#) on page 104

Restarting an endpoint machine after an install or uninstall

When you install or uninstall Forcepoint F1E agents on your endpoint machines, you might need to restart the endpoint machine to complete the install or uninstall. The following table shows the scenarios where a restart is required when you install or uninstall the v25.xx agent.

Forcepoint F1E agent	Restart required?
Forcepoint DLP Endpoint (Windows)	<ul style="list-style-type: none"> ■ Install: Yes ■ Uninstall: Yes
Forcepoint DLP Endpoint (Mac)	<ul style="list-style-type: none"> ■ Install: No, but an account sign out is required. ■ Uninstall: No
Forcepoint Web Security Proxy Connect Endpoint (Windows)	<ul style="list-style-type: none"> ■ Install: Yes ■ Uninstall: No
Forcepoint Web Security Proxy Connect Endpoint (Mac)	<ul style="list-style-type: none"> ■ Install: No, but an account sign out is required. ■ Uninstall: No

Forcepoint F1E agent	Restart required?
Forcepoint Web Security Direct Connect Endpoint (Windows)	<ul style="list-style-type: none"> ■ Install: No ■ Uninstall: No
Forcepoint Web Security Direct Connect Endpoint (Mac)	<ul style="list-style-type: none"> ■ Install: No, but an account sign out is required. ■ Uninstall: No
Forcepoint ECA (Windows)	<ul style="list-style-type: none"> ■ Install: No ■ Uninstall: No

Deploying Forcepoint F1E agents and the Neo agent on an endpoint machine

If you are working with multiple agent installation, refer to the [Forcepoint Agent Compatibility](#) Knowledge Base article.

About Risk-Adaptive DLP (Windows only)

Risk-Adaptive DLP combines the on-premises capabilities of Forcepoint DLP with the cloud-based capabilities of Forcepoint Dynamic User Protection.

If you install Forcepoint DLP Endpoint and Neo on the same Windows endpoint machine, the Neo icon is hidden on the Windows system tray. The Neo information is available in the Forcepoint F1E Diagnostics Tool when you open it from the Forcepoint F1E icon on the Windows system tray. If you install other Forcepoint F1E agents (such as the Proxy Connect Endpoint) and Neo on the same endpoint machine, each installation adds a separate Forcepoint icon to the Windows system tray.

For detailed information about installing endpoint agents for Risk-Adaptive DLP using the package builder, as well as using and configuring Forcepoint Dynamic User Protection, see the [Forcepoint Dynamic User Protection Help](#).

Configuring and managing Forcepoint F1E agents

When Forcepoint F1E is deployed, endpoint protection automatically starts. The policies and exceptions you created for users whose requests are managed by the hybrid service are applied automatically.

Configuring Forcepoint DLP Endpoint

Forcepoint DLP Endpoint requires configuration in the Forcepoint Security Manager. This entails:

Steps

- 1) Adding an endpoint profile to the Data Security module of the Forcepoint Security Manager or using the default. A default profile is automatically installed with the client package. (**Settings > Deployment > Endpoint**)
- 2) Rearranging endpoint profiles. (**Settings > Deployment > Endpoint**)
- 3) Configuring endpoint settings. (**Settings > General > System > Endpoint**)
- 4) Creating endpoint resources. (**Main > Policy Management > Resources > Endpoint Devices/Endpoint Applications/Application Groups**)
- 5) Creating or modifying a rule for endpoint channels. (**Main > Policy Management > DLP / Discovery Policies, Destination** tab)
- 6) Defining the type of endpoint machines to analyze, as well as the network location. (**Main > Policy Management > DLP / Discovery Policies, Custom Policy** wizard, **Source** tab).
Use the **Network Location** field to define the behavior of the endpoint machine on and off the network.

Next steps

See the [Forcepoint DLP Manager](#) Help for specific instructions.

Configuring the Forcepoint DLP Endpoint Confirmation Dialog (Windows only)

The Confirmation Dialog window is shown to end users when they perform an action that is against policy, but may still be performed if a business reason is given.

To enable this functionality, the action in policy management must be set to **confirm**.

In Forcepoint Security Manager v8.6 or later:

Steps

- 1) Go to **DATA > Settings > Deployment > Endpoint Profiles**.
- 2) Select the current active profile.
- 3) In the **Properties** tab, select the check box **Show incident details in the confirm dialog and the Log Viewer**.
- 4) Deploy the profile.

Next steps

The Confirmation Dialog timeout defaults to 30 seconds, but it is configurable to between 9 and 58 seconds in Forcepoint DLP. To configure this expiration time, contact [Forcepoint Support](#).

Configuring Forcepoint Web Security Endpoint

Forcepoint Web Security Endpoint Hybrid requires configuration in the Forcepoint Security Manager. For more information, see the [Forcepoint Web Security Endpoint Administrator Help](#).

Forcepoint Web Security Endpoint Cloud requires configuration in the Forcepoint Cloud Security Gateway Portal. For more information, see the [Forcepoint Cloud Security Gateway Portal Help](#).

Configuring Forcepoint Endpoint Context Agent

Forcepoint ECA requires configuration in the SMC. For more information, see the [Forcepoint NGFW Online Help](#).

Configuring Remote Filtering Client

To configure remote filtering settings, use the **Settings > General > Remote Filtering** page in the Web Security module of the Forcepoint Security Manager. For more information, see the [Forcepoint Web Security Administrator Help](#).

