Forcepoint

F1E

20.12

Install Guide

Contents

Chapter 1
Introducing Forcepoint F1E

Contents

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 v8.4 (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 v8.4 (or later) on-premises solution with the Hybrid Module or Forcepoint Web Security Cloud.
  - **Remote Filtering Client**: Requires Forcepoint URL Filtering v8.4 (or later) with the Remote Filter module.
- **Forcepoint CASB Endpoint** protects organizations from cloud application-based threats. It identifies and remediates sensitive data sent or received through both managed and unmanaged cloud applications accessed through the organization's network. Requires a Forcepoint CASB license.
- **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 v8.6 (or later) or Forcepoint Data Discovery v8.6 (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 v6.6 (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 17

Related reference
Deploying Forcepoint F1E in your Enterprise on page 43

Related Materials

Forcepoint F1E documentation

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

- Release Notes for Forcepoint F1E v20.12
  This document details the changes implemented in Forcepoint F1E v20.12.

- 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
- Resolved and Known Issues for Forcepoint F1E v20.12
- Enabling Full Disk Access for Forcepoint DLP Endpoint on macOS 10.15 and macOS 11
- 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 v20.12, 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)
- Forcepoint CASB installation is not required for a Forcepoint CASB Endpoint deployment. Forcepoint CASB is a cloud-based Forcepoint solution.

> **Note**
>
> 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 One Endpoint 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)

- Forcepoint CASB Administration Guide (for Forcepoint CASB Endpoint 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 v8.6, 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, Forcepoint Web Security Endpoint on the Forcepoint F1E platform is the standard agent for Forcepoint Web Security on Windows and Mac.

> **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, v20.12.xxxx) 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)
- Forcepoint CASB Endpoint on Windows only (Forcepoint F1E)

> ⚠️ **Important**
>
> The Forcepoint DLP v8.6 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.

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.

Forcepoint CASB Endpoint

Forcepoint CASB Endpoint routes cloud application connections from an organization's managed endpoint machine through the Forcepoint CASB gateway. Forcepoint CASB analyzes the activities coming to and from the cloud application and mitigates each activity based on enabled policies.

Compatibility

Forcepoint Web Security Endpoint

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

Component	Minimum support edversion	Recommended version
Forcepoint Web Security	v8.4.x	Latest v8.5.x maintenance version or later

Component	Minimum support edversion	Recommended version
Forcepoint URL Filtering (for Remote Filtering Client)	v8.4.x	Latest v8.5.x 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	v8.6.x	Latest v8.8.x maintenance version or later
Forcepoint Data Discovery	v8.6.x	Latest v8.8.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	v6.6.0	Latest v6.8.x maintenance version or later
Forcepoint NGFW Security Management Center (SMC)	v6.6.0	Latest v6.8.x 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	CASB EP
DLP EP		✔	✔	✔	✔	✔
DCEP	✔					
PCEP	✔				✔	
RF	✔					

ECA	✓		✓				
CASB EP	✓						

System requirements

Hardware requirements

Windows

Windows endpoint machines must meet the following minimum hardware requirements.

- Pentium 4 (1.8 GHz or above)
- At least 1 GB RAM
- At least 850 MB free hard disk space (250 MB for installation, 600 MB for operation)

Mac

Mac endpoint machines must meet the following minimum hardware requirements.

- At least 1 GB RAM
- At least 500 MB free hard disk space (375 MB for installation, 125 MB for operation)

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 (Desktopas- 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 both 32-bit and 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.

  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.

  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 7, Windows 8, Windows Server 2012, and Windows Server 2016 endpoint machines.

■ **Mobile devices** - On Windows 7 and 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

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). For Forcepoint CASB Endpoint, you must have a valid license for the cloud-based Forcepoint CASB product.

> **Note**
>
> **Important** The Forcepoint DLP v8.6 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 the Endpoint Security section of the Forcepoint Downloads page.

Related concepts
Guidelines for creating an anti-tampering password on page 21
Creating installation packages from the package builder (On-premises and Hybrid deployments) on page 22

Related tasks
Preparing for your Forcepoint Endpoint Context Agent installation on page 17
Downloading Forcepoint Web Security Endpoint installation packages (Cloud deployments) on page 20

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 18
Configuring Forcepoint Endpoint Context Agent settings in the SMC on page 19

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 14099. 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**
>
> 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 38

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 *(i)*
○ Direct Connect *(i)*

Platform: Windows 64-bit ▼

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 32-bit, 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 21

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

■ Forcepoint CASB Endpoint

The Forcepoint F1E package builder is a Windows utility that can create Windows 32-bit, 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 v8.4 and later, and Forcepoint DLP v8.6 and later.
>
> The Forcepoint ECA installation package is backwards compatible with Forcepoint NGFW versions 6.6 and later.

Downloading the package builder

Steps

1) Log on to the Forcepoint Downloads page.

2) Go to **Endpoint Security > Forcepoint One Endpoint**, select a version, then download the package builder. The downloaded file is a ZIP file named **ForcepointOneEndpointPackage.zip**. It contains:

- **The package builder utility**: The Windows utility that creates Windows 32- bit, 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.
  - **EPA.msi**: The Endpoint Classifier file for Windows 32-bit endpoint machines.
  - **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

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.

- **Forcepoint ECA**
Configure Forcepoint ECA in the SMC as described in *Preparing for your Forcepoint Endpoint Context Agent installation,* page 18.

- **Forcepoint DLP Endpoint**
Make sure you have a v8.6 or later management server installed and functioning. You must be logged on to the Forcepoint DLP server with a Service Account before you run the package builder. Otherwise, incorrect communication keys are created and Forcepoint DLP Endpoint cannot connect to the Forcepoint DLP server.

Copy the Endpoint Classifier file from the downloaded ZIP file to the folders specified below:

- Windows 32-bit: Copy the **EPA.msi** file into the **C:\Program Files(x86)\Websense\Data Security \client** folder.

- 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:

- Open the **ForcepointOneEndpointPackage.zip** file.

- 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)
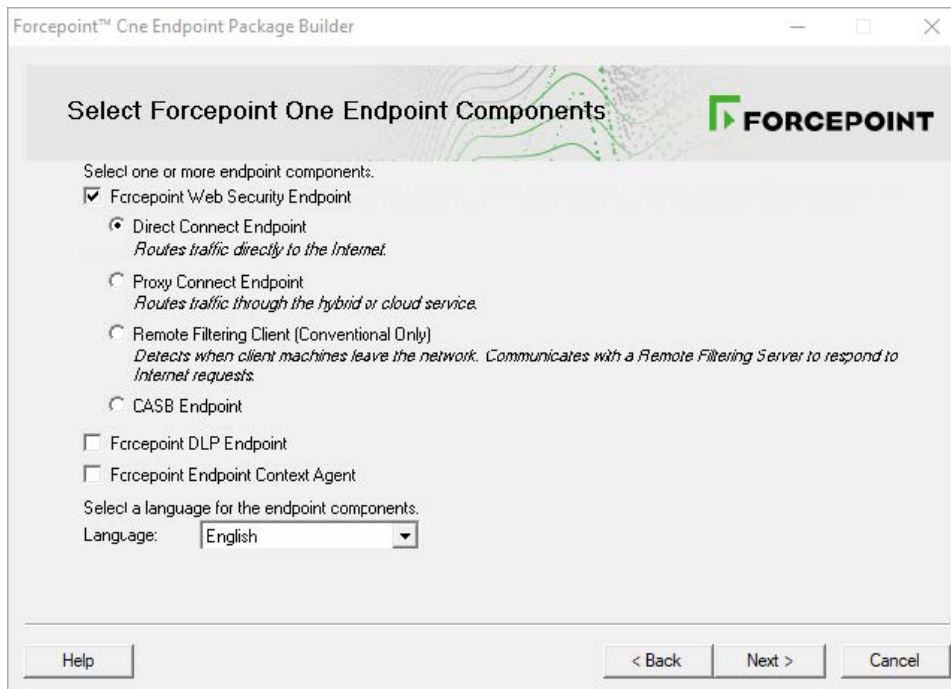
4) If you selected **Forcepoint Web Security Endpoint**, also select one of the following:

- **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).

- **CASB Endpoint** (requires Forcepoint CASB license). If you select CASB Endpoint here, the package builder automatically selects **Forcepoint DLP Endpoint**. Forcepoint CASB Endpoint is not a part of Forcepoint Web Security Endpoint, but it is included here so it cannot be selected with a Forcepoint Web Security Endpoint option. Currently, Forcepoint CASB Endpoint cannot be installed with Forcepoint Web Security Endpoint.

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:

a) Select the operating systems where Forcepoint F1E will be installed.

- 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 (32-bit or 64-bit) or Mac.

- If you are creating a stand-alone Forcepoint ECA package, you can only select Windows (32-bit or 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*, page 21. 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**
>
> Password hashes are stored in an encrypted file. The system does not store passwords in plain text. Customers requiring FIPS compliance can set the anti tampering 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.

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

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) 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 (e.g., 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(e.g., 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.

c) 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

Related tasks

Forcepoint DLP Endpoint

Steps

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

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.

Receive automatic software updates (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.

This option does not apply to Mac endpoint machines.

To automate software updates for Forcepoint DLP Endpoint:

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**.

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.

2)   Click **Next** to show the **DLP Client Settings** screen:
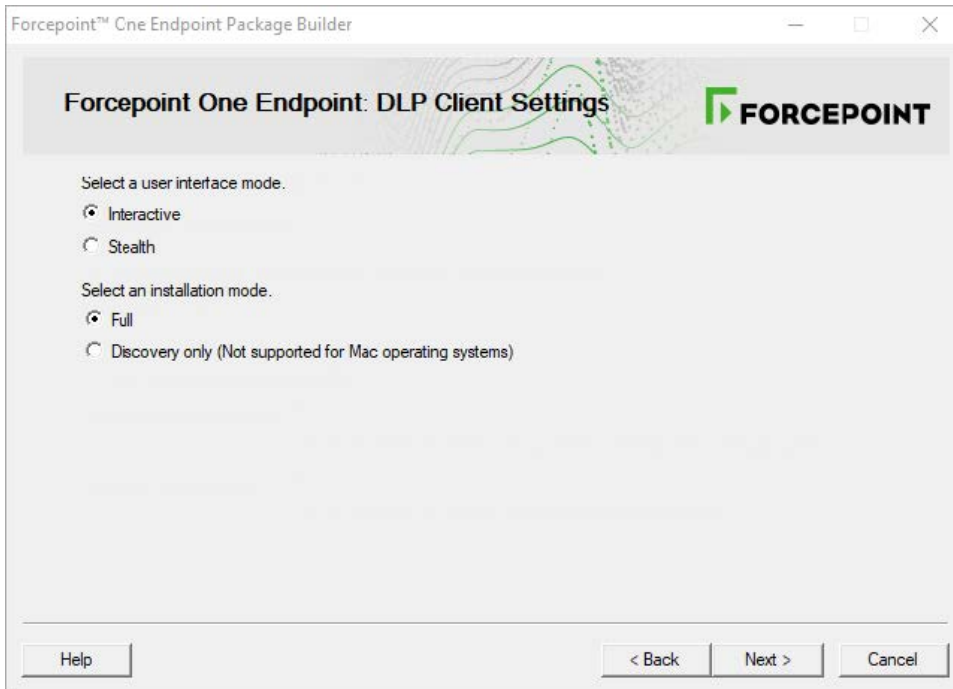
3)   Select the fields.

4)   Click **Next**.

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

Related tasks

Global settings on page 41

Related reference

Deploying Forcepoint F1E in your Enterprise on page 43
DLP Client Setting fields on page 31

DLP Client Setting fields

User interface mode	Select from the following 2 options:
	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:
	■ 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.
	Because users do not see any notifications, stealth mode is best reserved for discovery tasks and audit-only policies.
	Note that you must reinstall the endpoint machine and deploy a new profile to switch user interface modes.

Installation Mode	Applies to Windows only. Select from the following 2 options:
	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

Steps

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

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 show 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 shown 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 is shown 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 47

Related tasks
Global settings on page 41

Forcepoint Web Security Proxy Connect Endpoint

Steps

1) If you selected **Proxy Connect Endpoint** on the Select **Forcepoint One Endpoint Components** screen, the **Proxy Settings** screen is shown after the **Installation Path and Firefox Settings** screen:
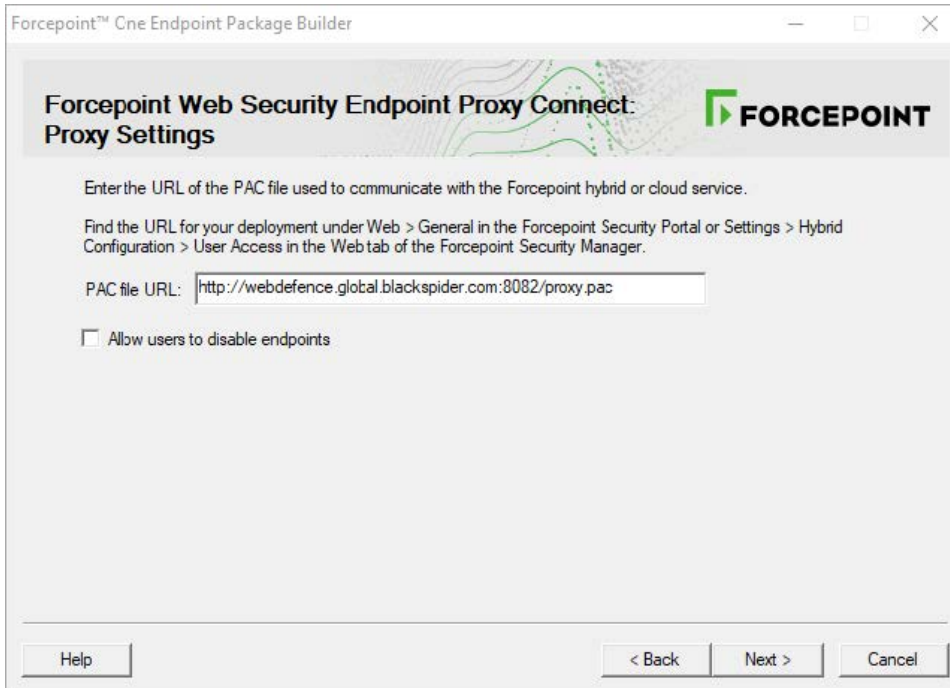
Specify the URL for your organization's PAC file. Replace the default URL with the customized URL for your deployment.

- **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.
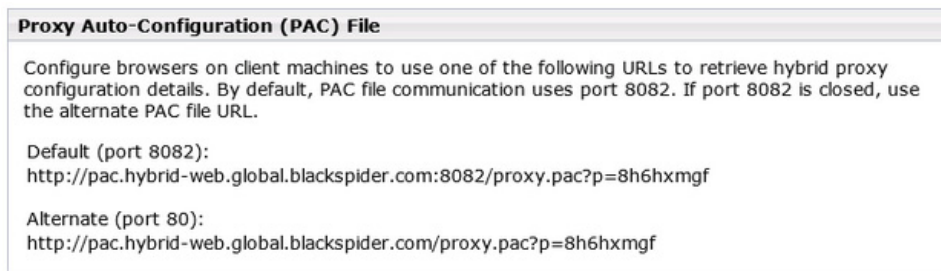
Select the URL appropriate for your environment (either port 8082 or port 80). For example: `Default (port 8082): http://pac.hybridweb. global.blackspider.com:8082/proxy.pac?p=8h6hxmgf Alternate (port 80): http://pac.hybridweb. global.blackspider.com/proxy.pac?p=8h6hxmgf`

In this example, **8h6hxmgf** 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=8h6hxmgf Alternate (port 80): http:// webdefence.global.blackspider.com/proxy.pac?p=8h6hxmgf`

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, if you want them to edit local proxy settings. Be aware that selecting this option allows users to circumvent the protections offered 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 is shown 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 41

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:

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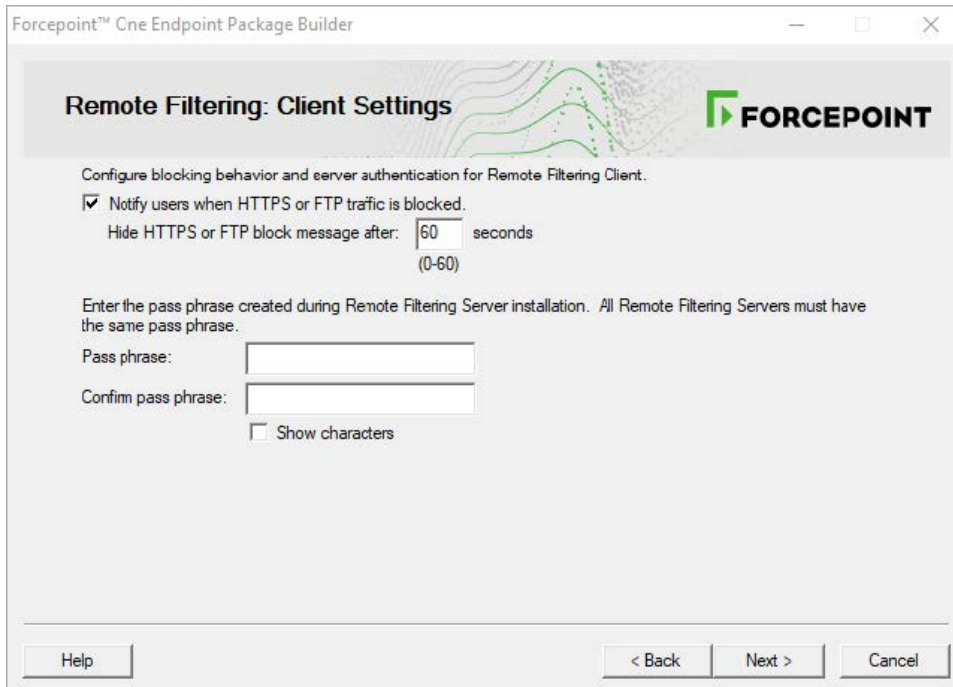
6) Click **Next** to show the **Trusted Sites** screen.

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 is shown 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 41

Forcepoint Endpoint Context Agent

Steps

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

2) 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*.

3) Click **Next**.

- If you are only creating a Forcepoint ECA package, the **Save Installation Package** screen is shown next. Continue with *Global settings*.

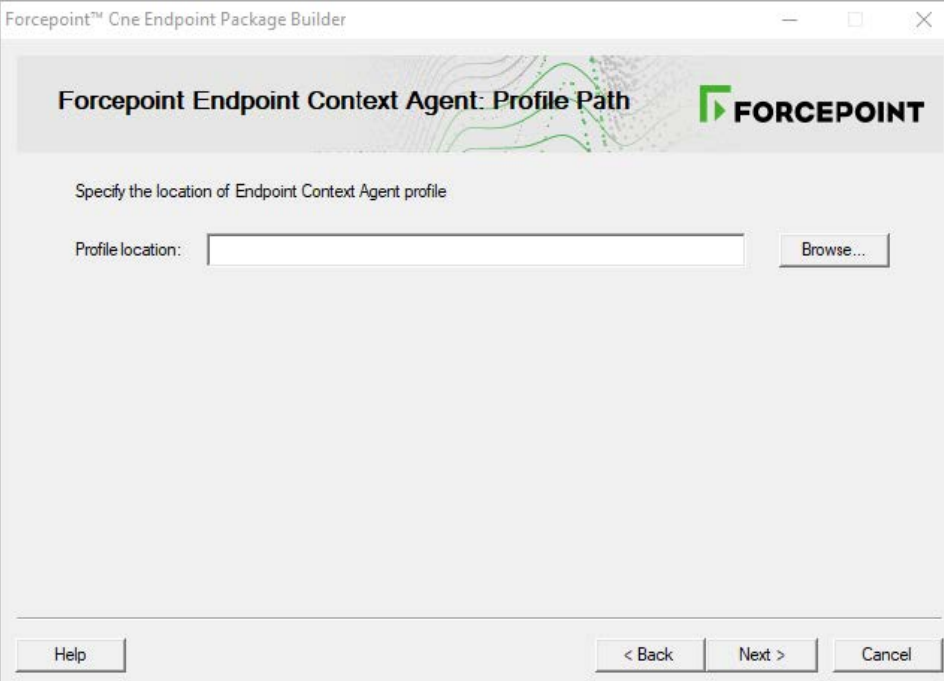- If you are creating a package with another agent, continue with the relevant section below.

Related tasks
Global settings on page 41
Preparing for your Forcepoint Endpoint Context Agent installation on page 17

Forcepoint CASB Endpoint

Steps

1) If you selected **Forcepoint CASB Endpoint** on the **Select Forcepoint One Endpoint Components** screen, the **Configuration** screen is shown after the **Installation Path and Firefox Settings** screen:

2) Complete the following fields to configure Forcepoint CASB Endpoint:

- **Hostname of the Forcepoint CASB Gateway or load balancer**: Enter the name (not the IP address) of your organizational Forcepoint CASB gateway. If you do not know the name of your gateway, open Forcepoint CASB, then go to **Settings > Resources > Assets >** *any asset* **> Access Mapping**. The gateway name is shown under **Forcepoint CASB proxy URL**.

- **Port**: Enter the port number for the organizational Forcepoint CASB gateway. The default is **443**.

- **Range of ports available for host-internal communications**: Enter the **Min** and **Max** values for the range of ports that Forcepoint CASB Endpoint can use for host-internal communications with local client applications.

- **Verification domains**: Enter one or more domains to be used in DNS requests to identify if the endpoint machine is on a known, or safe, network. Separate domains with a comma. For example, domain1.com@0.0.0.0,domain2.com@255.255.255.255.

- **CASB certificate file to install**: Enter the location, or Browse to the file location, of the certificate file (in .pfx format) to be installed with Forcepoint CASB Endpoint. This certification authenticates Forcepoint CASB Endpoint on the endpoint machine to the Forcepoint CASB server.

- **Certificate password**: Enter the password for the certificate file. The password characters are hidden by default. To see the password characters as you type, select **Show characters**.

3) Click **Next**.

- If you are only creating a Forcepoint CASB Endpoint package, the **Save Installation Package** screen is shown 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 41

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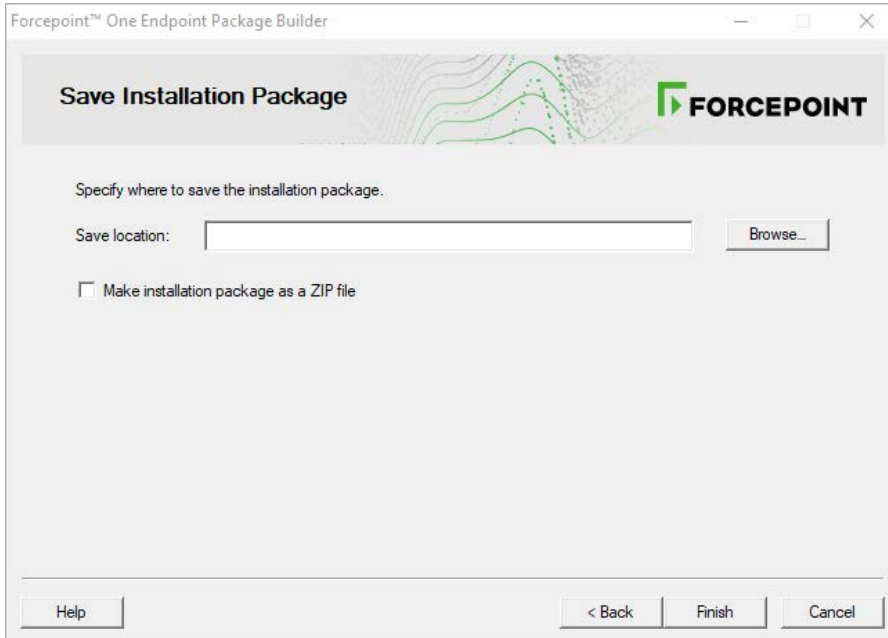
Either manually enter a path or click **Browse** to find the location.

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

Chapter 3

Deploying Forcepoint F1E in your Enterprise

Contents

This chapter describes how to deploy Forcepoint F1E software on endpoint machines.

Related concepts

Related information

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. See *System requirements* for details.
- 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 encrypted using full disk encryption. Forcepoint F1E must be installed after the disk has been encrypted.

- If you are deploying Forcepoint DLP Endpoint, disable the auto-update feature in the Web Security module of the Forcepoint Security Manager.

- For hybrid web deployments, make sure 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.

Sync Service Communication Results	
Sync Service location: 10.212.5.212	
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

Refresh

- For Forcepoint Endpoint Context Agent (Forcepoint 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) Deselect **Enable installation and update of Web Endpoint on client machines**.

3) Deselect **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
```

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

Copy your DCUserConfig.xml file into this folder.

4) Running 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 using one of the methods in *Deploying Windows endpoints*.

> **Related concepts**
> Deploying Windows endpoints on page 45

Deploying 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.

  See *Manually deploying Forcepoint F1E agents on a Windows 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 ECA to a limited set of endpoint machines using the ECA Evaluation deployment option. Forcepoint NGFW 6.6 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
Manually deploying Forcepoint F1E agents on a Windows endpoint machine on page 46

Manually deploying Forcepoint F1E agents 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-ENDPOINT-x32.exe** or **FORCEPOINT-ONE-ENDPOINTx64. exe**. If you are installing Forcepoint DLP Endpoint only:

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.

Combined Forcepoint DLP Endpoint and Forcepoint CASB Endpoint packages

In this Forcepoint F1E release, Forcepoint CASB Endpoint can only be installed with Forcepoint DLP Endpoint. Windows packages created with the package builder contain a single executable file: **FORCEPOINT-ONE-ENDPOINT-x32.exe or FORCEPOINT-ONE-ENDPOINT-x64.exe**. If you are installing the combined Forcepoint DLP Endpoint and Forcepoint CASB Endpoint package:

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.

> ⚠️ **Important**
>
> You cannot downgrade this combined installation to a previous Forcepoint F1E release, because the Forcepoint CASB Endpoint was not included in previous Forcepoint F1E installations. To downgrade, you must manually uninstall Forcepoint F1E, then install the previous version of Forcepoint DLP Endpoint.

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:

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-ENDPOINT-x32.exe** or **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 21

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-ENDPOINT-x32.exe or 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. For more information, see *Testing your deployment.*

Related concepts
Testing your deployment on page 51

Forcepoint Endpoint Context Agent packages made via the package builder

Windows packages created with the package builder contain a single executable file: **FORCEPOINT-ONE-ENDPOINT-x32.exe** or **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.

See *Authenticating Forcepoint ECA using client certificates* in the previous chapter 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* in the previous chapter for the full procedure.

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 v6.6 or later deployed in your organization.

Related tasks
Authenticating Forcepoint ECA using client certificates on page 18
Configuring Forcepoint Endpoint Context Agent settings in the SMC on page 19

Testing your deployment

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

- 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 **Windows Administrative Tools** > **Services**, 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 bar 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, make sure 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 ECA deployments:

  - Under **Windows Administrative Tools** > **Services**, 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 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.

- For Forcepoint CASB Endpoint deployments:

- Under **Windows Administrative Tools** > **Services**, verify that the **Skyfence Security 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 CASB 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 bar and select **Open Forcepoint One Endpoint Diagnostics**. The status is shown under the **System information** diagnostics test.

Most failed Forcepoint F1E software installation issues are permission related. An endpoint installation requires local administrator rights.

Troubleshooting a Forcepoint Endpoint Context Agent deployment

If you encounter issues during the Forcepoint 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, make sure 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.

Deploying Mac endpoints

There are a few ways to distribute Forcepoint DLP Endpoint or Forcepoint Web Security on Mac endpoint machines:

- Manually on each endpoint machine
  See *Manually deploying Forcepoint F1E agents on a Mac endpoint machine*.
- Using Remote Desktop
- Using mobile device management (MDM) software, such as Jamf, to automatically deploy Forcepoint F1E to your Mac endpoint machines.

Related tasks

Manually deploying Forcepoint F1E agents on a Mac endpoint machine

Steps

1) Mac packages contain a zip file, **FORCEPOINT-ONE-ENDPOINT-Mac.zip**. Copy FORCEPOINT-ONE-ENDPOINT-Mac.zip to the endpoint machine, then double-click the file.

2) MacOS automatically creates a directory named "EndpointInstaller," which contains a file called **WebsenseEndpoint.pkg**.

3) If you are deploying a Forcepoint Web Security Proxy Connect Endpoint package, copy the HWSConfig.xml configuration file to the EndpointInstaller folder. This XML file must be in the same folder as the **WebsenseEndpoint.pkg** file before starting the installation. See *Creating the HWSConfig.xml file (Proxy Connect Endpoint only)*for more information.

4) Double-click **WebsenseEndpoint.pkg** to start the installation process.

5) Click **Continue**, and agree to the license agreement.

6) Click **Install**.

7) Enter a user name and password for a user with administrator rights to install the software.
   A confirmation message is shown when the Forcepoint One Endpoint software is successfully installed.

8) *If you are installing Forcepoint DLP Endpoint v20.12 on macOS 11 (Big Sur) onwards*, you are prompted to enable full disk access (FDA) for 4 new processes:

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

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

    c) Click the + button under the list.

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

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

    f) Click the + button under the list.

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

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

    i) Close the Security & Privacy window.

> **Note**
>
> If you are deploying Forcepoint DLP Endpoint using Jamf, you can enable FDA for these processes using a configuration file. See the Enabling Full Disk Access for Forcepoint DLP Endpoint on macOS 10.15 and macOS 11 Knowledge Base article.

9) To complete the install, restart the endpoint machine.

> **Related concepts**
> Creating the HWSConfig.xml file (Proxy Connect Endpoint only) on page 55

Deploying Forcepoint DLP Endpoint using Jamf

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.

For Forcepoint DLP Endpoint deployments, Forcepoint provides Knowledge Base articles for specific configuration issues:

- Deploying the Forcepoint DLP Endpoint Chrome Extension on Mac endpoints using Jamf
- Enabling Full Disk Access for Forcepoint DLP Endpoint on macOS 10.15 and macOS 11

Enabling full disk access on macOS 10.15 and macOS 11(Forcepoint DLP Endpoint only)

When you install or upgrade Forcepoint DLP Endpoint on an endpoint machine running macOS 10.15 (Catalina), macOS 11 (Big Sur), 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 (see step 8 in the procedure above).
- On multiple endpoint machines by deploying a configuration file through MDM, such as Jamf. For more information, see the Enabling Full Disk Access for Forcepoint DLP Endpoint on macOS 10.15 and macOS 11 Knowledge Base article.

Creating the HWSConfig.xml file (Proxy Connect Endpoint only)

Before deploying a Forcepoint Web Security Proxy Connect Endpoint package to Macendpoint machines, you must create a configuration file named HWSConfig.xml. This configuration file contains the WSCONTEXT ID and the PAC file location.

Here is an example of a HWSConfig.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<ProxySetting>
```

```
<Context InitContext="<token>"/>
```

```
<PACFile URL="<pacfile>"/>
```

```
</ProxySetting>
```

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.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.
- <pacfile> is the URL for your PAC File. For hybrid deployments, the URL can be found on the **Settings > Hybrid Configuration > User Access** page in the Web Security module of the Forcepoint Security Manager. For full cloud deployments, 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.

Save the HWSConfig.xml file in the same directory as the **WebsenseEndpoint.pkg** installation package file.

> **Note**
>
> If you already have a HWSConfig.xml file, or one was provided for you, make sure your correct XML file is in the same directory as the **WebsenseEndpoint.pkg** installation package file.

Testing your deployment

To confirm that the Forcepoint F1E software is installed and running on a Mac endpoint machine:

- 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. Click the icon for status information. (No icon is shown in stealth mode.)

To check whether the Forcepoint One Endpoint software is running, open **Activity Monitor** and select **All Processes** under the menu option **View**. The process "wspxyd", "wsdc", "wsdlpd" or "wsrfd" should be running depending on which Forcepoint One Endpoint product is installed.

> **Note**
>
> If you are using the Firefox browser and the Forcepoint One Endpoint Firefox extension is not installed, complete one of the following actions:
>
> - Stop and start the service from the command line:
>   ```
>   wepsvc --stop && wepsvc --start
>   ```
> - Restart the endpoint machine.
>
> Relaunch Firefox. The Firefox extension is now installed and visible in the list of extensions.

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

Neo is a new endpoint agent that communicates with the new Forcepoint DynamicUser Protection solution. Neo is not a Forcepoint F1E agent.

If you plan to install the Neo agent along with one or more Forcepoint F1E agents on an endpoint machine, they must be installed in the following order:

- Install the Forcepoint F1E agents (v20.09 or later) through the package builder.
- Install Neo.

If you install Neo before Forcepoint F1E, then Forcepoint F1E uninstalls Neo. There is one exception: The Forcepoint F1E does not uninstall Neo if the Forcepoint F1E package contains Forcepoint DLP Endpoint. The Forcepoint DLP Endpoint and Neo installation is a supported installation for Risk-Adaptive DLP,which 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.

Configuring Forcepoint CASB Endpoint

Forcepoint CASB Endpoint requires configuration in Forcepoint CASB. For more information, see the Forcepoint CASB Administration Guide.

Uninstalling Forcepoint F1E software

Uninstalling Forcepoint F1E from a Windows endpoint machine

You can uninstall Forcepoint F1E software two ways:

- Manually on each endpoint machine
- Remotely through a deployment server or distribution system

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

Manually uninstalling Forcepoint F1E from a Windows endpoint machine

Steps

1) Use the Add/Remove Programs tool in Windows to uninstall the Forcepoint One Endpoint.

   You are prompted to confirm that you want to delete the Forcepoint One Endpoint agent.

2) Click **Yes**.

3) You may be prompted to provide an administrative password, if you defined one. If so, enter the password in the field provided and click **OK**.

   If you are uninstalling Forcepoint DLP Endpoint, restart the endpoint machine. The configuration changes are applied only when the endpoint machine has restarted.

Uninstalling Forcepoint F1E using a deployment server

If you deployed Forcepoint F1E 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 One 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 (32-bit versus 64-bit).

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

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 One Endpoint without a restart, include the `/norestart` parameter as follows:

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

The command switches are summarized below.

Function	Swtich
Silent uninstall	**msiexec /x {ProductCode} /qn XPSWDPXY=xxxx**
Silent uninstall without restart	**msiexec /x {ProductCode} /qn XPSWDPXY=xxxx/ norestart**

Related concepts
Guidelines for creating an anti-tampering password on page 21

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.

Uninstalling Forcepoint F1E from a Mac endpoint machine

Steps

1) Go to **System Preferences**.

2) In the **Other** section, click the icon for the Forcepoint F1E agent.

3) Click **Uninstall Endpoint**.

4) Enter the local administrator name and 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 make sure you are entering the correct password.

7) Click **OK** to uninstall the Forcepoint F1E software.

8) A confirmation message is shown when Forcepoint F1E is successfully uninstalled.

To uninstall Forcepoint F1E 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.