Contents

Chapter 1  Introducing Forcepoint Endpoint Solutions ................................. 1
  Forcepoint Web Security Endpoint .............................................. 2
  When to use Forcepoint Web Security Direct Connect Endpoint instead of
  Forcepoint Web Security Proxy Connect Endpoint ..................... 3
  Forcepoint DLP Endpoint ..................................................... 4
  System requirements .......................................................... 5
  Hardware requirements ....................................................... 5
  Operating system requirements ............................................ 5
  Virtual Desktop Infrastructure (VDI) ........................................ 5
  Browser support .............................................................. 6
  Forcepoint Web Security Endpoint .......................................... 6
  Forcepoint DLP Endpoint ..................................................... 6
  DLP channel support .......................................................... 6
  Email clients ................................................................. 6
  Printer drivers .............................................................. 6
  Application controls ......................................................... 7
  Supported removable media ................................................ 7
  LAN control ................................................................. 8
  Destination channels by operating system ............................... 8

Chapter 2  Obtaining or Creating the Installation Package ....................... 11
  Downloading installation packages from the
  Forcepoint Security Manager ............................................... 11
  On-premises Forcepoint Security Manager (hybrid deployments) .... 12
  Forcepoint Security Portal (cloud deployments) ......................... 12
  Creating installation packages from a package builder ................ 12
  Forcepoint DLP Endpoint ..................................................... 17
  Forcepoint Web Security Direct Connect Endpoint .................... 20
  Forcepoint Web Security Proxy Connect Endpoint .................... 21
  Remote filter ............................................................. 22
  Global settings .......................................................... 25

Chapter 3  Deploying endpoint software in your enterprise ..................... 27
  Before you begin ................................................................ 27
  Disabling automatic updates for Forcepoint Web Security Endpoint .. 28
  Enabling automatic updates ................................................. 28
  Deploying Windows endpoints .............................................. 29
  Manual deployment .......................................................... 30
  Stand-alone Forcepoint DLP Endpoint packages ....................... 30
  Forcepoint Web Security Endpoint packages downloaded from the Force-
  point Security Manager or Forcepoint Security Portal ............... 30
Contents

Forcepoint Web Security Proxy Connect Endpoint or mixed packages made via the package builder .......................................................... 31
Forcepoint Web Security Direct Connect Endpoint or mixed packages made via the package builder ......................................................... 32
Configuring Forcepoint Endpoint to work with Firefox 53 and Firefox 54 .................................................. 32
Testing deployment .................................................................................. 33
Deploying Mac endpoints ...................................................................... 34
  Manual deployment ............................................................................. 34
  Creating the HWSconfig.xml file ....................................................... 35
  Testing deployment ........................................................................... 35
Deploying Linux endpoints (stand-alone Forcepoint DLP Endpoint only) ...................................................................................... 36
Deploying XenApp endpoints (Forcepoint DLP Endpoint only) .......................................................... 36
Configuring and managing endpoints .................................................... 37
  Configuring the Confirmation Dialog expiration time .......................... 38
Uninstalling endpoint software ............................................................... 39
  Windows uninstallation .................................................................... 39
    Local uninstallation ...................................................................... 39
    Remote uninstallation with deployment server ............................... 40
    Remote uninstallation using distribution systems ......................... 40
  Mac uninstallation ........................................................................... 41
  Linux uninstallation (stand-alone Forcepoint DLP Endpoint only) ...... 41
Introducing Forcepoint Endpoint Solutions

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>In this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Forcepoint Web Security v8.4.x</td>
<td>● Forcepoint Web Security Endpoint</td>
</tr>
<tr>
<td>● Forcepoint DLP v8.4.x</td>
<td>● Forcepoint DLP Endpoint</td>
</tr>
<tr>
<td>● Forcepoint URL Filtering v8.4.x</td>
<td>● Hardware requirements</td>
</tr>
<tr>
<td>● Forcepoint Web Security Endpoint v8.4.x</td>
<td>● Operating system requirements</td>
</tr>
<tr>
<td>● Forcepoint DLP Endpoint v8.4.x</td>
<td>● Browser support</td>
</tr>
<tr>
<td></td>
<td>● DLP channel support</td>
</tr>
</tbody>
</table>

Forcepoint™ endpoint 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 clients and provide actionable forensic insight into potential attacks.

● **Forcepoint Web Security Endpoint** protects users from web threats. Forcepoint offers three Forcepoint Web Security Endpoint options:
  - Forcepoint Web Security Direct Connect Endpoint: Requires a Forcepoint Web Security on-premises solution with the Web Hybrid module (Windows only) or Forcepoint Web Security with the Web Cloud module (Windows only).
  - Forcepoint Web Security Proxy Connect Endpoint: Requires a Forcepoint Web Security on-premises solution with the Web Hybrid module or Forcepoint Web Security with the Web Cloud module.
  - Remote Filtering Client: Requires Forcepoint URL Filtering with the Remote Filter module.

● **Forcepoint DLP** protects organizations from data loss and data theft. It also identifies and remediates sensitive data stored on corporate computers, including laptops. Requires Forcepoint DLP Network or Forcepoint Data Discovery.

For Forcepoint DLP Endpoint, Remote Filtering Client, or mixed deployments (combinations of Forcepoint DLP Endpoint and either the proxy connect or direct connect version of Forcepoint Web Security Endpoint), you can use a Package Builder utility to generate **endpoint client software** that runs on the endpoint clients to block, monitor, and log transactions (like Internet requests or proprietary data sharing).
according to the organization’s security and acceptable use policies. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that do not restrict use of the client computer.

Forcepoint solutions include endpoint **server components** as well. These are part of your Forcepoint Web Security or Forcepoint DLP deployments.

See **System requirements**, page 5 for information about the hardware requirements for endpoint client components.

**About this guide**
This guide describes how to deploy Forcepoint Endpoint software on endpoint client machines across your enterprise.

- Chapter 1 describes system requirements, browser and operating support, benefits, and other information.
- Chapter 2 describes how to obtain or create installation packages.
- Chapter 3 describes how to globally deploy Forcepoint Endpoint software and install it on endpoint clients.

**Related materials**
- **Server installation** - Forcepoint endpoint solutions rely on other Forcepoint products for server-side functions. If you have not already done so, you must install these products before beginning an on-premises Forcepoint Endpoint installation.
  - **Installing Forcepoint DLP** (for Forcepoint DLP Endpoint)
  - **Installing Forcepoint Web Security** (for hybrid Forcepoint Web Security Endpoint deployment)
    - No installation is required for cloud Forcepoint Web Security Endpoint deployment
  - **Installing Forcepoint URL Filtering** (for Remote Filtering deployment)
- **Endpoint configuration** - Once the Forcepoint Endpoint software is deployed to your client machines, you configure it in the Forcepoint Security Manager.
  - **Forcepoint Web Security Manager Help** (for hybrid Forcepoint Web Security Endpoint deployment)
  - **Forcepoint DLP Manager Help** (for Forcepoint DLP Endpoint)
  - **Forcepoint Security Portal Help** (for cloud Forcepoint Web Security Endpoint deployment)
- **Client software usage** - If the software is not installed in stealth mode, users can interact with the user interface.
  - **End User Guide for Forcepoint Endpoint Solutions**

**Forcepoint Web Security Endpoint**
Forcepoint Web Security Endpoint includes 3 endpoint client options:
Introducing Forcepoint Endpoint Solutions

- Forcepoint Web Security Proxy Connect Endpoint
- Forcepoint Web Security Direct Connect Endpoint
- Remote Filtering Client

**Forcepoint Web Security Proxy Connect Endpoint** can be deployed to secure client machines whose Internet activity is managed by the hybrid or cloud service. The Forcepoint Web Security Proxy Connect Endpoint software 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 Web Security 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 Web Security Proxy Connect Endpoint manipulates proxy settings in real time. For example, if Forcepoint Web Security 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 Web Security Proxy Connect Endpoint for some or all machines managed by the cloud or hybrid service.

**Forcepoint Web Security Direct Connect Endpoint** (available for both full cloud and hybrid deployments) 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 Web Security 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 in complex/changing network environments.

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 a client machine with either Forcepoint Web Security Proxy Connect Endpoint or Forcepoint Web Security Direct Connect Endpoint installed.

**When to use Forcepoint Web Security Direct Connect Endpoint instead of Forcepoint Web Security Proxy Connect Endpoint**

The newly available Forcepoint Web Security Direct Connect Endpoint is now available alongside the existing Forcepoint Web Security Proxy Connect Endpoint. The Forcepoint Web Security Proxy Connect Endpoint endpoint will continue to be available and supported and remains the default solution for securing roaming users in most situations.
The Forcepoint Web Security 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 Web Security 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 Web Security Direct Connect Endpoint and Forcepoint Web Security Proxy Connect Endpoint can both be used in the same customer deployment; however, only one type can be installed on an individual client machine.

---

**Important**

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

---

**Forcepoint DLP Endpoint**

Forcepoint DLP Endpoint is designed for organizations concerned about data loss originated at the endpoint, 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 endpoints 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.
System requirements

Hardware requirements

*Windows*

Windows clients must meet the following minimal hardware requirements.

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

*Mac*

Mac clients must meet the following minimal requirements.

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

*Linux (stand-alone DLP only)*

- At least 1 GB RAM
- 1 GB free hard disk space (not including contained files and temporary buffers; see the Data Security Manager Help for information about contained files and allocating enough disk storage for them)

Operating system requirements

Endpoint clients must be running one of the operating systems listed in the Forcepoint Certified Product Matrix.

Virtual Desktop Infrastructure (VDI)

Forcepoint DLP Endpoint can also be installed on endpoint clients running Windows in Virtual Desktop Infrastructure (VDI) environments such as Citrix XenDesktop and VMWare Horizon View. Supported versions are also listed in the Certified Product Matrix.

---

*Note*

Only Forcepoint DLP Endpoint is supported in VDI environments. Forcepoint Web Security Endpoint is not supported in VDI environments.
Browser support

**Forcepoint Web Security Endpoint**

For a list of web browsers that fully support the Forcepoint Web Security Endpoint client 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, and 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 Endpoint analyzes data via the Web > Endpoint HTTP/HTTPS destination, it intercepts HTTP(S) posts as they are being uploaded within the browser. It does not monitor download requests.

The system analyzes posts from the browsers listed on the Forcepoint Certified Product Matrix.

DLP channel support

**Email clients**

Forcepoint DLP analyzes all email messages sent from endpoint users, even if they send them to external Web mail services such as Yahoo.

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

The system 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.

For Mac clients, Forcepoint DLP can analyze endpoint 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, not those that print to file or PDF.
Application controls

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

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

It can also control access to files. For example, you can monitor uploads to cloud storage clients like DropBox and also IM / VOIP clients like GoToMeeting or Skype for Business.

The applications that Forcepoint DLP can monitor out of the box are found in the Technical Library article, 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 such as thumb drives and external hard drives. If desired, you can configure Windows and Linux endpoint policies to encrypt files being transferred to removable media.

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

  - **Encrypt with profile key**: Windows and Linux only. Encrypt with a password deployed in the endpoint profile. This is for users who will be on an authorized machine—one with the endpoint agent 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 endpoints regardless of your action plan setting.

  - **Encrypt with user password**: Windows only. Encrypt with a password supplied by endpoint users. This is for users who will be decrypting files from other machines—those without the endpoint agent installed. Select **Encrypt with user password** when configuring your action plans for endpoint removable media. The action defaults to permitted on Linux and Mac endpoints regardless of your action plan setting.

  See Configuring encryption for removable media in the Forcepoint DLP Administrator Help for more information.

---

**Important**

Removable media encryption is only available on Windows and Linux endpoint machines.

Encryption is **not** supported on Mac endpoint machines.
Introducing Forcepoint Endpoint Solutions

- **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.


Linux endpoint does not support CD/DVD burners.

- **Mobile devices** - On Windows 7 and Windows 10 (Creators Update, version 1703 and higher), Forcepoint DLP can also monitor unencrypted data being copied to mobile devices through the Windows Portable Devices (WPD) protocol. This allows you to use application file access monitoring on software clients like Apple iTunes and Samsung Kies when needed.

**LAN control**

Users commonly take their laptops home and then copy data through a LAN connection to a network drive or share on another computer. They also commonly take data from a shared folder (at work) to copy onto their laptop. 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**

Not all destination channels apply to all operating systems. Endpoint destination support is shown below.

<table>
<thead>
<tr>
<th>Destination Channel</th>
<th>Windows</th>
<th>macOS</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web HTTP/HTTPS</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Printing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Applications</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Removable media</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LAN</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

*The cut, copy, paste, file access, and download operations are not supported for cloud apps on Windows endpoints when they are used through a Windows Store browser.*
Obtaining or Creating the Installation Package

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>In this topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Forcepoint Web Security v8.4.x</td>
<td>● Downloading installation packages from the Forcepoint Security Manager</td>
</tr>
<tr>
<td>● Forcepoint DLP v8.4.x</td>
<td>● Creating installation packages from a package builder</td>
</tr>
<tr>
<td>● Forcepoint URL Filtering v8.4.x</td>
<td></td>
</tr>
<tr>
<td>● Forcepoint Web Security Endpoint v8.4.x</td>
<td></td>
</tr>
<tr>
<td>● Forcepoint DLP Endpoint v8.4.x</td>
<td></td>
</tr>
</tbody>
</table>

You can obtain endpoint installation packages in one of 2 ways:

● Download them from the Forcepoint Security Manager or Forcepoint Security Portal (for hybrid or cloud web deployments that do not include DLP)

● Create them using the Forcepoint Endpoint Package Builder (for remote filter, DLP, hybrid, and mixed deployments)

Before beginning this process, you must install the Forcepoint product that is relevant to your environment: Forcepoint Web Security (Cloud or Hybrid module) or Forcepoint DLP (DLP module). Refer to the Technical Library for instructions.

Downloading installation packages from the Forcepoint Security Manager

If you are planning to deploy Forcepoint Web Security Endpoint alone, you can download an endpoint installation package from the Forcepoint Security Portal (for cloud deployments) or Forcepoint Security Manager (for hybrid deployments). If needed—for example, if you do not have Internet access—you can use the Forcepoint Endpoint Package Builder instead.

If you plan to use Forcepoint DLP Endpoint or Remote Filtering Client, you must use the Package Builder.
On-premises Forcepoint Security Manager (hybrid deployments)

Customers with on-premises Forcepoint Web Security installations can log on to the Web Security module of the Forcepoint Security Manager and then navigate to Settings > Hybrid Configuration > Hybrid User Identification to obtain the endpoint installation package.

- You must set an anti-tampering password to enable the package download links.
- Different endpoint packages are available for 32-bit and 64-bit clients. Select the appropriate package (or combination of packages) from the list provided.

See the Forcepoint Web Security Administrator Help for more information about hybrid deployments of Forcepoint Web Security Endpoint.

Forcepoint Security Portal (cloud deployments)

Customers with a full-cloud deployment (Forcepoint Web Security with the Web Cloud module) can log on to the Forcepoint Security Portal, and then navigate to Web > Endpoint > General to obtain the endpoint installation package.

On that page, you have two types of endpoints to choose from: Direct Connect and Proxy Connect. You can deploy a combination of Direct Connect and Proxy Connect endpoint clients in your organization if desired; however, only one type can be installed on an individual client machine.

Creating installation packages from a package builder

If you are using Forcepoint DLP Endpoint (alone, or in a mixed deployment with either Forcepoint Web Security Proxy Connect Endpoint or Forcepoint Web Security Direct Connect Endpoint) or you are using Remote Filter, you must use the Forcepoint Endpoint Package Builder to create a custom endpoint installation package.
If you are using Forcepoint Web Security Endpoint alone, you can obtain the installation package from the Forcepoint Security Manager or Forcepoint Security Portal, or use the Package Builder.

The installation package (a single executable file) is used to deploy the endpoint clients to user machines.

The Forcepoint Endpoint Package Builder is a Windows utility that can be used to create 32- and 64-bit Windows packages, Mac packages, or (DLP only) Linux endpoint clients.

The utility can be found on any Windows server that includes Forcepoint Web Security, Forcepoint URL Filtering, or Forcepoint DLP.

---

**Note**

The packages created by the Forcepoint Endpoint Package Builder are backwards compatible with previous endpoint versions.

---

1. **Launch the Forcepoint Endpoint Package Builder.**
   
   For on-premises deployments, do one of the following on the management server:
   
   - **Forcepoint Endpoint or Forcepoint URL Filtering** - Navigate to `C:\Program Files (x86)\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack`
   
   - **Forcepoint DLP** - Select `Start > All Programs > Forcepoint`.
   
   On Windows Server 2012, browse to the Start page and select the Endpoint Package Builder.
   
   For either on-premises web or DLP deployments, or cloud web deployments, you can download the latest Package Builder from the Forcepoint website:
   
   - Log on to [My Account](#).
   
   - Navigate to ENDPOINT SECURITY, select a Forcepoint Endpoint version, and then download the Package Builder.
   
   The Forcepoint Endpoint Package Builder utility extracts required files and launches.

2. **On the Select Endpoint Components screen, select one or both of the following:**
   
   - **Forcepoint Web Security Endpoint** provides web security to your endpoint devices.
   
   - **Forcepoint DLP Endpoint** for data loss protection (requires Forcepoint DLP)
   
   Under Endpoint web protection, 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 with the Web Cloud module) or a hybrid cloud/on-premises deployment (requires Forcepoint Web Security with the Web Hybrid module).
- **Proxy Connect Endpoint**: Choose this if you want to create a Forcepoint Web Security Proxy Connect Endpoint installation package for a full cloud deployment (requires Forcepoint Web Security with the Web Cloud module) or a hybrid cloud/on-premises deployment (requires Forcepoint Web Security with the Web Hybrid module).

- **Remote Filtering Client**: Choose this if you want to provide just remote filtering of endpoint clients (requires Forcepoint Web Security or Forcepoint URL Filtering).

Also select a language for the client components.

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 (buttons, captions, fields, etc.) can only be set during packaging.

Click **Next** when you are done.
3. On the **Installation Platform and Security** screen, select the operating system or systems for which you want to create an installation package, create the administrator password that will be used to uninstall or modify endpoint client software, and enable anti-tampering. When you are finished, click **Next**.

![Installation Platform and Security](image)

- You can create Windows (32-bit or 64-bit) or Mac installation packages for Forcepoint Web Security Proxy Connect Endpoint deployments, or for deployments with both Forcepoint Web Security Proxy Connect Endpoint and Forcepoint DLP Endpoint features.

  If you are creating a stand-alone Forcepoint Web Security Direct Connect Endpoint package, you can only select Windows (32-bit or 64-bit).

  If you are creating a stand-alone Forcepoint DLP Endpoint package, you can also select Linux.

- For security purposes, anyone who tries to modify or uninstall endpoint software is prompted for a password.

  Once the endpoint client contacts the server, this password is overwritten with the password specified by an administrator. Set this password in one of the following places (it is not necessary to do it in both):

  - **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 an anti-tampering password.

  - **Forcepoint Web Security Endpoint (Cloud module)**: In the Forcepoint Security Portal, go to **Web > Endpoint > Deployment Settings > Set Anti-Tampering Password**, and enter and confirm a password.

  Note that password hashes are stored in an encrypted file. The system does not store plain text passwords.
If no password is specified, every user with admin privileges is able to uninstall the endpoint software from their computer.

Click **Show characters** to display the password characters while you type.

- Sometimes when users cannot modify or uninstall the endpoint software, they try to delete the directory where the software is installed.

  Click **Protect installation directory from modification or deletion** if you do not want users to be able to perform these functions.

4. On the **Installation Path** screen, specify the directory to use for installing endpoint software on each endpoint device. The directory path must contain only English characters.

   Note that this screen does not display if you are creating only a Mac endpoint package. On Mac machines, the endpoint client is installed in the /Applications directory.

   ![Installation Path](image)

   - **Use default location**: The endpoint software is installed in a default directory: \Program Files\Websense\Websense Endpoint (*Windows*) or /opt/websense/LinuxEndpoint (*Linux*).
   - **Use this location**: Manually specify the installation path for the endpoint software. Environment variables are supported.

5. Click **Next**.

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

   Follow the instructions for the individual endpoint components below.
Obtaining or Creating the Installation Package

Forcepoint DLP Endpoint

1. If you selected Forcepoint DLP Endpoint from the Select Endpoint Components screen, the Server Connection screen displays next:

   ![Server Connection 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. Once configured, endpoints retrieve policy and profile updates from the endpoint server defined in their profiles.

   **Receive automatic software updates (Windows endpoints only)**: When new versions of the endpoint are released, you may upgrade the software on each endpoint—this can be done 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 Linux or Mac endpoints.

   To automate software updates for DLP or combined web/DLP endpoints:
   a. Prepare a server with the latest updates on it (see “Configuring the auto-update server” for details).
   b. Select **Receive automatic software updates**.
   c. Specify the URL of the server you created. (It cannot be secure http (https).)
d. Indicate how often you want endpoint machines to check for updates.

2. Click **Next** and the **Client Settings** screen displays:
Complete the fields as follows:

<table>
<thead>
<tr>
<th>User interface mode</th>
<th>Select from the following 2 options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>Interactive</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Stealth</strong>: The Forcepoint DLP Endpoint user interface is not displayed to the user. In this mode, users will not know that the endpoint software is operating on their machine. The following features are affected in this mode:</td>
</tr>
<tr>
<td></td>
<td>■ The Forcepoint DLP Endpoint icon will not display in the task bar. Users will see the endpoint installation if they check the Windows Control Panel.</td>
</tr>
<tr>
<td></td>
<td>■ Users will not be able to view the client user interface. As a result, they will not have access to the connection status, the Contained Files viewer, the Log Viewer, or the bypass option. ( Experienced users, however, will be able to see Contained folders and files in the installation path.)</td>
</tr>
<tr>
<td></td>
<td>■ Users will not receive pop-up messages.</td>
</tr>
<tr>
<td></td>
<td>■ Although administrators can choose Confirm and Encrypt with user password in the Data Security manager as part of an action plan for the endpoint, these are not possible enforcement actions. When these options are selected, operations that violate policy are blocked. The Encrypt with profile key action will still take place, however.</td>
</tr>
<tr>
<td></td>
<td>■ When a user attempts to access a blocked page, a 404 error message will display rather than a block page.</td>
</tr>
<tr>
<td></td>
<td>Because users will not see any notifications, stealth mode is best reserved for discovery tasks and audit-only policies. Note that you must reinstall the endpoint and deploy a new profile to switch user interface modes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Installation Mode</th>
<th>Applies to Windows only. Select from the following 2 options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>Full</strong>: Installs the endpoint with full policy monitoring and blocking capabilities upon a policy breach. All incidents are reported in the Forcepoint Security Manager. Endpoints that are installed in Full Mode require a restart.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Discovery Only</strong>: Configures the endpoint to run discovery analysis but not DLP. Discovery Only installation does not require a restart.</td>
</tr>
</tbody>
</table>

3. Click **Next**.
Forcepoint Web Security Direct Connect Endpoint

1. If you selected Direct Connect Endpoint from the Select Endpoint Components screen, the Account Identification screen displays:

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 Security Portal. See Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Security Manager or Forcepoint Security Portal, page 30 for more information.

2. Click Next and the Local Block Pages screen displays:

Use the Local Block Pages screen to change the description and logo that displays at the bottom of the local block pages. Local block pages are used by the
endpoint when it is in Fallback mode and cannot connect to endpoint services. These pages are only displayed when in Fallback mode. If the endpoint is connected to endpoint services, the default block page is displayed.

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 displays if you attempt to load a website with an invalid security certificate.

3. Click Next.

**Forcepoint Web Security Proxy Connect Endpoint**

1. If you selected Proxy Connect Endpoint from the Select Endpoint Components screen, the Proxy Settings screen displays:

   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 > Hybrid Configuration > 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:


In this example, **8h6hxmgf** is a unique identifier for an organization. Yours will be different. Yours explicitly 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:


In this example, **8h6hxmgf** is a unique identifier for an organization. Yours will be different. Yours explicitly defines your organization.

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

### Allow users to disable endpoints

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 client 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.

Click **Next**.

### Remote filter

1. Prepare Remote Filtering Server components as described [here](#).
2. If you selected **Remote Filtering Client** from the Select Endpoint Components screen, the **Internal Connections** screen displays.
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. When you are finished, click **Next**.

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. 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, and then click **Next**.

5. 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.
When you are finished, click **Next**.

6. Indicate whether or not to **Notify users when HTTPS or FTP traffic is blocked**, then, if notification is enabled, specify how long (in seconds) the message is displayed.

   Enter and confirm the **Pass phrase** used for communication with Remote Filtering Server. This must match the pass phrase created when the Remote Filtering Server was installed.

   When you are finished, click **Next**.
Global settings

1. When you are done configuring your endpoint selections, use the **Save Installation Package** screen to enter a directory path to use for storing the installation package before it is deployed to client machines.

![Save Installation Package](image)

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

2. Click **Finish**.

You will see a system message if the package is created successfully. If the creation of the package fails, you will see an error message. If this happens, contact Forcepoint Technical Support for assistance.

3. Click **OK**.

Once the packaging tool has finished, the packages are created in the designated path. Refer to *Deploying endpoint software in your enterprise, page 27* for instructions on distributing the package to the endpoint devices.
Obtaining or Creating the Installation Package

26  Forcepoint Endpoint
Deploying endpoint software in your enterprise

This section describes how to deploy Forcepoint endpoint software on client machines.

### Before you begin

- For best practice, start by deploying and testing endpoint software to 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*, page 5 for details.
- Exclude the following directories from any antivirus software that is deployed to endpoint clients:
  - The endpoint installation folder
  - Endpoint processes:
    - `wepsvc.exe`
    - `dserui.exe`
    - `ProxyUI.exe`
    - `RFUI.exe`
  - `EndpointClassifier.exe` and `kvoop.exe`
Deploying endpoint software in your enterprise

- Ensure the endpoint installation path is not encrypted by file and folder encryption software. All folders and files within the installation path must be left unencrypted.

- Forcepoint Endpoint can be installed on an endpoint machine encrypted using full disk encryption. Forcepoint Endpoint must be installed after the disk has been encrypted.

- If you are including Forcepoint DLP Endpoint, ensure that the auto-update feature in the Web Security module of the Forcepoint Security Manager is disabled. If you want auto-updates, you can use the Forcepoint DLP method described below. (Windows only)

- 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.

### Disabling automatic updates for Forcepoint Web Security Endpoint

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 endpoint update, you must restart the endpoint for the updates to take effect.

### Enabling automatic updates

Windows only. To deploy endpoint updates automatically, you must create an update server that hosts endpoint installation packages. See “Automatic Updates for Forcepoint DLP Endpoint Software” for details.
You must also select **Receive automatic software updates** on the Forcepoint Endpoint Package Builder “Server Connections” screen. On this same screen, specify the URL of the server you created and indicate how often you want endpoint machines to check for updates (every 2 hours by default).

When configured properly, your update server pushes software updates out to endpoint machines and installs the packages in the background silently.

---

**Note**

If you want to change the components installed on a Forcepoint Endpoint client with components of the same version (for example, switch from a mixed deployment to a stand-alone Forcepoint DLP Endpoint deployment), you must use the Package Builder to generate a new package and use one of the other deployment options to deploy it. You cannot use the auto-update feature to update endpoints with the same version.

---

### Deploying Windows endpoints

---

**Important**

After deploying the installation package, you must restart the endpoint software to complete the installation process.

There are a few ways to distribute the endpoint software on Windows clients, including virtual desktop clients running Windows:

- Manually on each endpoint device
- Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS)
  See *Creating and distributing Forcepoint endpoints using SCCM or SMS* for details.
- Using a Microsoft Group Policy Object (GPO) or other third-party deployment tool for Windows. See *Distributing the endpoint via GPO* for details. To distribute executables created with the Package Builder via GPO, contact Forcepoint Technical Support.
Manual deployment

Stand-alone Forcepoint DLP Endpoint packages

Windows packages created with the Package Builder contain a single executable file: TRITONAP-ENDPOINT-x32.exe or TRITONAP-ENDPOINT-x64.exe. If you are installing only Forcepoint DLP Endpoint software:

1. Copy one of these files to the client machine.
2. Double-click the executable file and step through the installation wizard.

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

Forcepoint Web Security Endpoint packages downloaded from the Forcepoint Security Manager or Forcepoint Security Portal

ZIP files downloaded from the Forcepoint Security Manager or Forcepoint Security Portal (web endpoint packages) contain the MSI file: Websense Endpoint.msi.

1. Copy the MSI file to the client machine.
2. Run the following command (with the straight quotes around the msi file name):

   "Websense Endpoint.msi" WSCONTEXT=<token>

where <token> is the WSCONTEXT value displayed in the GPO command 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 Security Portal. For example:
The WSCONTEXT argument 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: TRITONAP-ENDPOINT-x32.exe or TRITONAP-ENDPOINT-x64.exe.

1. Copy one of these files to the client machine.
2. Run the following command:
   ```
   TRITONAP-ENDPOINT-x64.exe /v"XPSWDPXY=<password>
   WSCONTEXT=<token>"
   ```

   where:
   - `<password>` is the anti-tampering password used by the previous-version endpoint client (if upgrading) or to be used by the new endpoint.
   - `<token>` is the WSCONTEXT value displayed in the GPO command 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 Security Portal.

   The WSCONTEXT argument 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:
   ```
   TRITONAP-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:
   ```
   TRITONAP-ENDPOINT-x64.exe /v"/qn /norestart
   XPSWDPXY=<password> WSCONTEXT=<token>"
   ```
Deploying endpoint software in your enterprise

The command switches are summarized below:

<table>
<thead>
<tr>
<th>Function</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent install</td>
<td>TRITONAP-ENDPOINT-x64.exe /v&quot;/qn&quot;</td>
</tr>
<tr>
<td>Silent install without restart</td>
<td>TRITONAP-ENDPOINT-x64.exe /v&quot;/qn /norestart&quot;</td>
</tr>
<tr>
<td>Set WSCONTEXT</td>
<td>TRITONAP-ENDPOINT-x64.exe /v&quot;WSCONTEXT=xxxx&quot;</td>
</tr>
<tr>
<td>Set uninstall password</td>
<td>TRITONAP-ENDPOINT-x64.exe /v&quot;XPSWDPXY=xxxx&quot;</td>
</tr>
<tr>
<td>Set WSCONTEXT and silent install</td>
<td>TRITONAP-ENDPOINT-x64.exe /v&quot;/qn</td>
</tr>
<tr>
<td></td>
<td>WSCONTEXT=xxxx</td>
</tr>
</tbody>
</table>

### 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: TRITONAP-ENDPOINT-x32.exe or TRITONAP-ENDPOINT-x64.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 client machine.
2. Double-click the executable file and step through the installation wizard.

### Configuring Forcepoint Endpoint to work with Firefox 53 and Firefox 54

Forcepoint DLP Endpoint and Forcepoint Web Security Endpoint are unable to support the following in Firefox v53 and Firefox v54 on Windows endpoints:

- Sensitive data protection in web-based mail services (e.g., Gmail and Yahoo Mail)
- Google Drive

When you deploy the Forcepoint Endpoint software to Windows endpoints with Firefox v53 or v54 installed, follow the below deployment guidance:

**Forcepoint Web Security Direct Connect Endpoint:**
Deploying endpoint software in your enterprise

Edit the **DCUserConfig.xml** configuration file to specify the following configuration parameters in “DCSetting”:

```xml
<FirefoxSetting FirefoxConfigCFGFileName="mozilla.cfg"
FirefoxConfigJSFileName="channel-perfs.js" />
```

**Forcepoint Web Security Proxy Connect Endpoint:**

Edit the **HWSConfig.xml** configuration file to specify the following configuration parameters in “ProxySetting”:

```xml
<FirefoxSetting FirefoxConfigCFGFileName="mozilla.cfg"
FirefoxConfigJSFileName="channel-perfs.js" />
```

**Forcepoint DLP Endpoint:**

Edit the following configuration files to enable silent installation of the Firefox extension:

1. Open the Firefox installation folder. For example: `C:\Program Files (x86)\Mozilla Firefox\defaults\pref`
2. Add the following text to the `channel-prefs.js` file:
   ```javascript
   pref("general.config.obscure_value", 0);
   pref("general.config.filename", "firefox.cfg");
   ```
3. Create a new file named `firefox.cfg` and put it into the Firefox folder. For example, `C:\Program Files (x86)\Mozilla Firefox`.
4. Add the following text to `firefox.cfg`:
   ```javascript
   // empty comment up top - must be here
defaultPref("extensions.autoDisableScopes", 0);
defaultPref("extensions.enabledScopes", 15);
   ```
5. Restart Firefox.

**Testing deployment**

To confirm that the Forcepoint Endpoint software is installed and running on a machine:

- For Forcepoint Web Security Endpoint deployments, go to **Start > Control Panel > Administrative Tools > Services**. Check that **Websense SaaS Service** is present in the Services list and is started. An icon ( ![icon](image) ) also displays on the endpoint machine’s task bar.
- When Forcepoint DLP Endpoint is installed in interactive mode, an icon ( ![icon](image) ) displays on the endpoint machine’s task bar. Click the icon for status information. (No icon shows in stealth mode.)

Most failed endpoint installation issues are permission related. An endpoint installation requires local administrator rights.
Deploying Mac endpoints

There are a few ways to distribute Forcepoint DLP Endpoint or Forcepoint Web Security Proxy Connect Endpoint on Macs:

- Manually on each endpoint device
  See Manual deployment, page 34.
- Using Remote Desktop (macOS only)
  See Installing Mac endpoints with Remote Desktop for details.

Forcepoint Web Security Direct Connect Endpoint is not available for Mac endpoints.

Manual deployment

1. Mac packages contain a zip file, TRITONAP-ENDPOINT_Mac.zip. Copy TRITONAP-ENDPOINT_Mac.zip to the client machine, and 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, page 35 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.
   You will receive a confirmation message if the endpoint was successfully installed.

   Note
   If you are using the Firefox browser and the Forcepoint Endpoint Firefox extension was not installed, perform one of the following actions:
   - Stop and start the service from the command line:
     websvc --stop && wepsvc --start
   - Restart the endpoint machine.
   Relaunch Firefox. The Firefox extension is now installed and visible in the list of extensions.
Creating the HWSconfig.xml file

Before deploying a Forcepoint Web Security Proxy Connect Endpoint package to Mac endpoints, 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
<?xml version="1.0" encoding="UTF-8"?>
<ProxySetting>
    <Context InitContext="<token>"/>
    <PACFile URL="<pacfile>"/>
</ProxySetting>
```

where:

- `<token>` is the WSCONTEXT value displayed in the GPO command 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 Security Portal.

  The WSCONTEXT argument 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 Security Portal. If you would rather use an account-level PAC file, navigate 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 deployment

To confirm that the endpoint is installed and running on a machine:

- Endpoint files are installed in the /Library/Application Support/Websense Endpoint/ directory.
When Forcepoint DLP Endpoint is installed and running in interactive mode, an icon (/favicon) displays on the endpoint machine’s task bar. Click the icon for status information. (No icon shows in stealth mode.)

To check whether the endpoint is running, open Activity Monitor and select All Processes under the menu option View. The process ‘wspxyd’, ‘wsdlp’ or ‘wsrfd’ should be running depending on which endpoint product is installed.

**Deploying Linux endpoints (stand-alone Forcepoint DLP Endpoint only)**

Linux packages contain the following installer: ForcepointTRITONAP-ENDPOINT_Linux_el5. Use this installer with Red Hat Enterprise Linux version 5.x.

To install Forcepoint DLP Endpoint software on a Linux computer, copy the installer to the machine and run it in the terminal console. Restart the machine when done.

**Deploying XenApp endpoints (Forcepoint DLP Endpoint only)**

Forcepoint DLP Endpoint can be deployed on Citrix XenApp servers to provide data loss and data theft prevention on client machines.

1. Create a Windows 64-bit endpoint package using the Package Builder utility described in the previous chapter.
2. To deploy the endpoint software, follow the instructions in Deploying Windows endpoints, page 29, but instead of deploying the software to each endpoint client, deploy it to a network server.
3. To support XenApp hardware resources, configure the endpoint to support additional threads and improve memory usage. This change needs to be made on each XenApp server running Forcepoint DLP Endpoint.

To customize the configuration, do the following:

1. Open the file, AlternateResource.config.xml.
2. In a text editor and do the following:
   a. Set <numOfThreads>, the number of threads per processor, to at least twice the number of cores on the Terminal Services server. For example, if you have 4 cores on the Terminal Services server, set <numOfThreads>8</numOfThreads>.
   b. Change all resource IDs in the document to reflect the number of threads you wish to use.
Deploying endpoint software in your enterprise

c. Increase `<MemoryInfo>` to optimize endpoint memory usage. To do so, multiply the number of supported sessions * 50M * .125. For example, if there are 8 supported sessions, multiply 8 * 50 * .125 = 50.

Round up the result to the nearest integer in multiples of 50M not less than 100M. Set `<MaxRamSpace>` to this value. In the example, set `<MaxRamSpace>` to 100.

3. Save and copy the `AlternateResource.config.xml` file to C:\Program Files\Websense\Websense Endpoint. To do so:
   a. Using CMD, navigate to C:\Program Files\Websense\Websense Endpoint.
   b. Run the following command:
      ```
      WDEUtil.exe -set disableantitampering=true
      ```
   c. Copy `AlternateResource.config.xml` file to the directory.

4. In Windows Task Manager, restart the **EndpointClassifier** service.

5. From the ..\Websense\Websense Endpoint folder, use CMD to run the following commands:
   ```
   WDEUtil.exe -stop wsdlp
   WDEUtil.exe -start wsdlp
   ```

For more information, see [Deploying Forcepoint DLP Endpoint on Citrix XenApp clients](#).

#### Configuring and managing endpoints

Once the endpoint software is deployed, endpoint web protection is automatically started. The policies and exceptions you created for users whose requests are managed by the hybrid service are applied automatically.

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

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 on and off the network.

See the [Forcepoint DLP Manager Help](#) for specific instructions.
To configure remote filtering settings, use the **Settings > General > Remote Filtering** page in the Web Security module of the Forcepoint Security Manager. Refer to [Forcepoint Web Security Administrator Help](#) for details.

**Configuring the Confirmation Dialog expiration time**

The Confirmation Dialog window displays to end users when they perform an action that is against policy, but may still be performed if a business reason is given. The Confirmation Dialog timeout defaults to 30 seconds, but it is configurable between 9 and 58 seconds in Forcepoint DLP.

To configure this expiration time, contact Forcepoint Support.
Uninstalling endpoint software

Windows uninstallation

You can uninstall endpoint software 2 ways:

- Locally on each endpoint client
- Remotely through a deployment server or distribution system

**Note**

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

Local uninstallation

1. Go to **Start > Control Panel > Programs and Features**.
2. Scroll down the list of installed programs, select **Forcepoint Endpoint**, and click **Uninstall**.
3. Click **Yes** in the confirmation message asking if you are sure you want to delete the endpoint software.
4. 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**.
5. You will see a system message indicating you must restart your system. Click **Yes** to restart or **No** to restart your system later. Once the computer has been restarted, the configuration changes apply.
Remote uninstallation with deployment server

If you use a deployment server to deploy endpoint software, you can perform a silent uninstall 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.

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 perform a silent uninstall that does not require a restart, add the `/norestart` parameter as follows:

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

The command switches are summarized below.

<table>
<thead>
<tr>
<th>Function</th>
<th>Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent uninstall</td>
<td><code>msiexec /x {ProductCode} /qn XPSWDPXY=xxxx</code></td>
</tr>
<tr>
<td>Silent uninstall without restart</td>
<td><code>msiexec /x {ProductCode} /qn XPSWDPXY=xxxx /norestart</code></td>
</tr>
</tbody>
</table>

Remote uninstallation using distribution systems

You can uninstall endpoint software remotely by using distribution systems. If you used an SMS distribution system to create packages for installation, those packages can be reused, with a slight modification, for uninstalling the software. If a package was not created for deployment of the endpoint software, a new one needs to be created for uninstalling.

To uninstall with package:

1. Follow the procedure for [Creating and distributing Forcepoint endpoints using SDCCM or SMS](#).
2. In step 1, select **Per-system uninstall**.
3. Complete the remaining procedures.
4. After deploying the package, Forcepoint endpoint software will be uninstalled from the defined list of computers.
Mac uninstallation

1. Go to System Preferences.
2. In the Other section, click the icon for the Forcepoint endpoint software.
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 endpoint client software, enter that password.
7. Click OK to begin uninstalling the endpoint.
8. You will receive a confirmation message if the endpoint was successfully uninstalled.

To uninstall the Mac endpoint remotely, you can use the following command line option with Apple Remote Desktop:

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

Linux uninstallation (stand-alone Forcepoint DLP Endpoint only)

Run the `ep-uninstall` script (located by default at `/opt/websense/LinuxEndpoint/ep-uninstall`). You may be prompted for an administrative password, if one was defined by your system administrator.