Forcepoint

F1E

24.07

End User Guide

Contents

Chapter 1
Introduction to F1E

Contents
■   About the Product on page 6
■   Forcepoint F1E Agent components on page 6

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

> **Note**
>
> Some functionality might be disabled by your organization's security policies. This disabled functionality will not be available to use. Disabling the endpoint software introduces possible vulnerabilities, because you are no longer receiving the protection provided by Forcepoint Web Security Endpoint or Forcepoint DLP Endpoint.

Related concepts
Fallback mode on page 10
Viewing logs (Windows only) on page 10
RMS/MIP decryption limitation on page 14
Updating Forcepoint DLP Endpoint on page 17
Disabling Forcepoint DLP Endpoint on page 17
Enabling the Forcepoint Safari extension on page 19
Updating the Mail plug-in on page 20
Deploying Forcepoint F1E Outlook Add in on page 21
Online Applications in macOS on page 31
Custom Logo for Coaching Dialog on page 21
Forcepoint DLP Inline Proxy on page 23

Related tasks
Using the Forcepoint Web Security Endpoint Diagnostics Tool on page 9
Disabling Forcepoint Web Security Endpoint protection on page 10
Using the Forcepoint DLP Endpoint Diagnostics Tool (Windows only) on page 18
Allowing or blocking a policy violation on page 31
Setting encryption passwords on page 34
Viewing contained files and saving them to an authorized location on page 38
Viewing logs on page 39
Custom Text for Coaching Dialog on page 22

Related reference
Checking the status of Forcepoint Web Security Endpoint on page 7

About the Product

F1E solutions protect you and other users against advanced web-based threats and data theft while on and off the corporate network. F1E solutions are installed on the endpoint machines (for example, desktop computer or laptop) and communicate with Forcepoint software installed on corporate servers.

Forcepoint F1E Agent components

This guide covers details on the following F1E agents:

- **Forcepoint Web Security Endpoint**: The Forcepoint Web Security Endpoint v8.5.4 (or later) agent defends your endpoint machine against web threats.
- **Forcepoint DLP Endpoint**: The Forcepoint DLP Endpoint v8.9.x (or later) agent protects your organization from the unintended loss of data and data theft.
- **Forcepoint Endpoint Context Agent**: The Forcepoint Endpoint Context v6.10 (or later) agent monitors your Windows endpoint machine and determines which connections are allowed by the firewall.

If you see this icon () in the notification area of the task bar (Windows) or the status menu of the menu bar (Mac), one or more of the above F1E agents are enabled on your endpoint machine.

Chapter 2

Forcepoint Web Security Endpoint

Contents
■ Checking the status of Forcepoint Web Security Endpoint on page 7
■ Using the Forcepoint Web Security Endpoint Diagnostics Tool on page 9
■ Fallback mode on page 10
■ Viewing logs (Windows only) on page 10
■ Disabling Forcepoint Web Security Endpoint protection on page 10

Forcepoint Web Security Endpoint is a software application that runs on the endpoint machines (for example, desktop computer or laptop), protecting the users from malware and enforcing their organization's acceptable user policy.

Related concepts
Fallback mode on page 10
Viewing logs (Windows only) on page 10

Related tasks
Using the Forcepoint Web Security Endpoint Diagnostics Tool on page 9
Disabling Forcepoint Web Security Endpoint protection on page 10

Related reference
Checking the status of Forcepoint Web Security Endpoint on page 7

Checking the status of Forcepoint Web Security Endpoint

The F1E status icon () is shown in the task bar's notification area (Windows) or the menu bar's status menu (Mac). To view the status of Forcepoint Web Security Endpoint, move your mouse over the icon. The following table describes the available status indicators.

Icon	Meaning	Description
	Enabled	All installed F1E agents are successfully configured and activated.

Icon	Meaning	Description
	Disabled	All installed F1E agents are disabled.
		To verify the connection status, move your mouse over the F1E icon. A pop-up window shows the connection status for all installed agents. All installed agents should show **Disabled** (Forcepoint ECA shows as **Disconnected**).
		If you manually disable the agent, your endpoint machine is no longer being protected against web threats. You can re-enable the software manually or it will be enabled when your endpoint machine is restarted.
		The ability to enable/disable endpoint software is allocated by your system administrator.
		See *Disabling Forcepoint Web Security Endpoint protection*.
	Fallback Partially Disabled	This status may indicate that:
		■ One or more installed agent (Forcepoint DLP Endpoint, Forcepoint Web Security Endpoint or Forcepoint ECA) is disabled, but at least one agent is enabled or running. If all agents are disabled, this status icon is not shown (the Disabled status icon described above is shown).
		■ Forcepoint Web Security Endpoint is in Fallback mode. See *Fallback mode* for more information.

> ⚠️ **Important**
>
> ■ If you manually disable Forcepoint Web Security Endpoint, restarting the endpoint machine always re-enables it.
>
> ■ If your organization installs more than one F1E agent (Forcepoint Web Security Endpoint, Forcepoint DLP Endpoint, and/or Forcepoint Endpoint Context Agent) on your endpoint machine, you can access all installed agents from one Forcepoint icon on your task bar.

For more information on Forcepoint DLP Endpoint and Forcepoint Endpoint Context Agent, see *Forcepoint DLP Endpoint* and *Forcepoint Endpoint Context Agent*.

Related concepts

Using the Forcepoint Web Security Endpoint Diagnostics Tool

The Diagnostics Tool displays all information about the Forcepoint Web Security Endpoint that you can provide to your system administrator to assist with troubleshooting.

To launch the Diagnostics Tool:

1) Right-click the F1E icon in the task bar's notification area (Windows) or single click the menu bar's status menu (Mac).

2) Select **Open F1E Diagnostics**.

When the tool is launched, the diagnostic tests are executed in sequence. If one of the tests results in a failure, the subsequent tests are not automatically run.

Three diagnostic tests are accessed from this tool:

- **System information** - Collects basic information related to the specific endpoint machine on which the Forcepoint Web Security Endpoint software is installed.
- **Network diagnostics** - Collects information related to network connectivity.
- **PAC file status** (Windows only) - For endpoint machines that go through a proxy before connecting to the Internet, this test collects information to determine if the PAC file is accessible.

OR

Cloud services - For endpoint machines that connect directly to the Internet, this test collects information to determine if the endpoint software can contact the cloud service for disposition information (i.e., whether to block or allow the request).

To manually run the diagnostics tests, select one of the above tests and click the **Run Diagnostics** button.
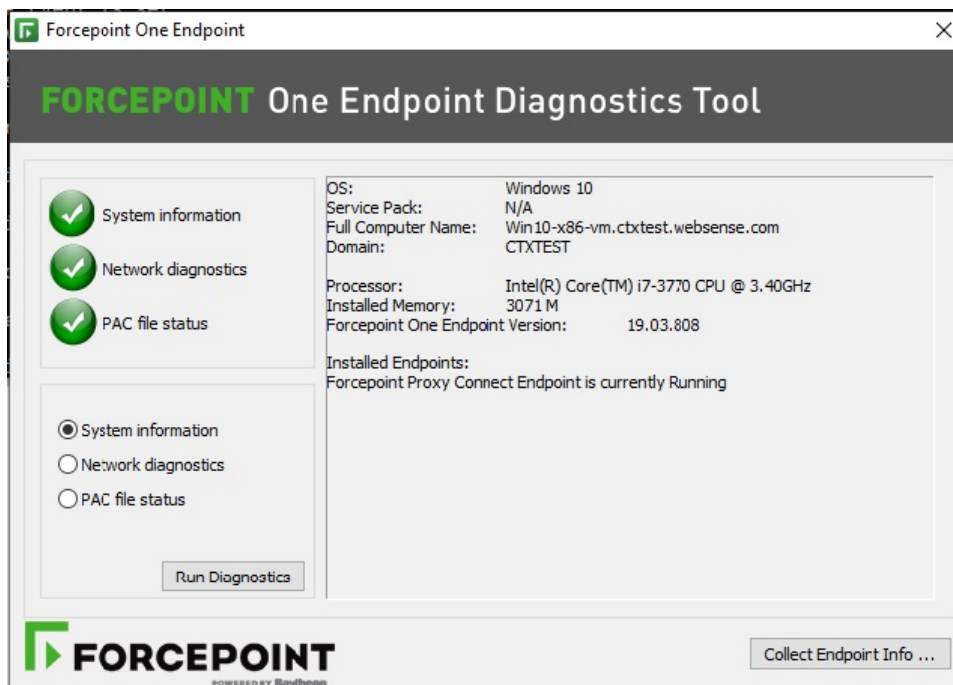
> **Note**
>
> Corresponding log files generated from these new diagnostic tests can easily be collected with the existing **CLIENTINFO.EXE** tool. Your Help Desk might ask you to run this tool to collect these files. To run it, click the **Collect Endpoint Info...** button on the diagnostics screen. The resulting file is placed onto the desktop. Attach the file to an email to your Help Desk or system administrator.

Fallback mode

Forcepoint Web Security Endpoint provides a Fallback mode if your network connection to the cloud service is interrupted. Events that might trigger Fallback mode include:

- Changing from Wi-Fi to an Ethernet network connection or vice-versa
- Connecting to a virtual private network (VPN)
- Assigning a new IP address to your laptop
- Disconnecting from the Internet

While in Fallback mode, the F1E icon displayed in your task bar changes to reflect your level of protection. If you see this icon ( ) in your task bar (Windows) or menu bar (Mac), your system is in Fallback mode and is **not** protected against web threats. When network events prevent endpoint machines from connecting with cloud services, Forcepoint Web Security Endpoint is automatically and temporarily bypassed. If this happens, you can continue to access the Internet (if Internet access is available), but endpoint protection is not provided during this time.

Once the network issue is resolved, Forcepoint Web Security Endpoint is automatically re-enabled.

Viewing logs (Windows only)

To view the logs about system events related to Forcepoint Web Security Endpoint, go to the Application section of the Windows system event log (**Start** > **Control Panel** > **Administrative Tools** > **Event Viewer** > **Windows Logs** > **Application**).

These logs might be helpful to share with your system administrator. All logs are in English.

> ⚠️ **Important**
>
> Log files are automatically deleted after 5 days.

Disabling Forcepoint Web Security Endpoint protection

This functionality may be turned off by your system administrator. If it is turned off, you do not see the Disable option in the F1E menu. On Windows endpoint machines, you can disable both the Proxy Connect (PC) Endpoint and the Direct Connect (DC) Endpoint. On Mac endpoint machines, you can only disable the DC Endpoint.

Disabling the Forcepoint Web Security Endpoint software removes the protection provided by the endpoint service, and stops it from intercepting traffic and securing your endpoint machine from web threats. Sometimes,

it might be useful to manually disable the endpoint software to troubleshoot issues with the assistance of your system administrator.

If your organization allows you to disable Forcepoint Web Security Endpoint:

1) Right-click the F1E icon in the task bar's notification area (Windows) or single click the menu bar's status menu (Mac).

2) Select **Disable Forcepoint Proxy Connect Endpoint** or **Disable Forcepoint Direct Connect Endpoint** from the menu. Only one of the options is shown in the menu. The option depends on the type of Forcepoint Web Security Endpoint installed.

If you see an authentication page asking for your username and logon credentials, you need to change your proxy auto-config (PAC) file settings in Internet Explorer.

Contact your system administrator for assistance with changing your PAC file settings.

To re-enable Forcepoint Web Security Endpoint:

1) Right-click the F1E icon in the task bar's notification area (Windows) or single click the menu bar's status menu (Mac).

2) Select **Enable Forcepoint Proxy Connect Endpoint** or **Enable Forcepoint Direct Connect Endpoint** from the menu. Only one of the options is shown in the menu. The option depends on the type of Forcepoint Web Security Endpoint installed.

> ⚠️ **Important**
>
> If you manually disable Forcepoint Web Security Endpoint, restarting the endpoint machine always re- enables it.

Chapter 3
Forcepoint DLP Endpoint

Forcepoint DLP Endpoint expands protection to sensitive information stored on the endpoint machines.

Depending on your corporate policy, data could be quarantined or encrypted when you try to email it, print it, or copy it to removable media such as thumb drives, CD/DVD burners, and Android devices (CD/DVD and Android support depends on your operating system).

Related tasks

Related reference

RMS/MIP decryption limitation

Using RMS/MIP decryption is not supported when more than one user is actively logged in.

Checking the status of Forcepoint DLP Endpoint

The F1E status icon (⬚) is shown in the task bar's notification area (Windows) or the menu bar's status menu (Mac). To view the status of Forcepoint DLP Endpoint, move your mouse over the icon. The following table describes the available status indicators.

Icon	Meaning	Description
⬚	Enabled	All installed F1E agents are successfully configured and activated.

Icon	Meaning	Description
	Disabled	All installed F1E agents are disabled or disconnected. To verify the connection status, move your mouse over the F1E icon. A pop-up window shows the connection status for all installed agents. All installed agents should show Disabled (Forcepoint ECA shows as Disconnected). If you manually disable the agent, your endpoint machine is no longer being protected. You can re-enable the software manually or it will be enabled when your endpoint machine is restarted. The ability to enable/disable endpoint software is allocated by your system administrator. See **Disabling Forcepoint DLP Endpoint**.
	Fallback Partially Disabled	This status may indicate that: ■ One or more installed agent (Forcepoint DLP Endpoint, Forcepoint Web Security Endpoint or Forcepoint ECA) is disabled, but at least one agent is enabled or running. If all agents are disabled, this status icon is not shown (the Disabled status icon described above is shown). ■ Forcepoint Web Security Endpoint is in Fallback mode. See **Fallback mode**, for more information.

⚠️ **Important**

If you manually disable Forcepoint DLP Endpoint, restarting the endpoint machine always re-enables it.

If your organization installs more than one F1E agent (Forcepoint Web Security Endpoint, Forcepoint DLP Endpoint, and/or Forcepoint Endpoint Context Agent) on your endpoint machine, you can access all installed agents from one Forcepoint icon on your task bar.

For more information about Forcepoint Web Security Endpoint and Forcepoint Endpoint Context Agent, see *Forcepoint Web Security Endpoint*, and *Forcepoint Endpoint Context Agent*.

Related concepts
Forcepoint Web Security Endpoint on page 7
Forcepoint Endpoint Context Agent on page 41

Viewing detailed Forcepoint DLP Endpoint status information

To see more detailed status information about Forcepoint DLP Endpoint:

1) Right-click the Forcepoint One Endpoint icon in the task bar's notification area (Windows) or single click the menu bar's status menu (Mac).

2) Select **Open Forcepoint DLP Endpoint** from the Windows menu, or **Forcepoint DLP Endpoint** from the Mac menu.
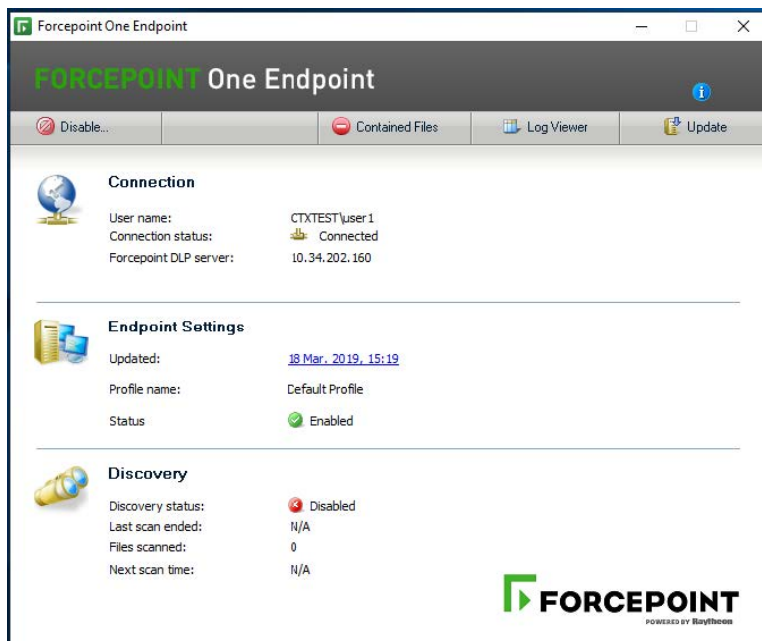
On the Forcepoint DLP Endpoint screen, you can:

- See whether your machine is connected to a Forcepoint DLP server.
- Check the IP address of the Forcepoint DLP server hosting the endpoint server software.
- View your endpoint software profile name and when it was last updated.
- Disable/enable Forcepoint DLP Endpoint. For more information, see *Disabling Forcepoint DLP Endpoint*.
- Check profile version to compare to the DLP manager.
- Determine if Forcepoint DLP Endpoint protection is enabled or bypassed.
- View discovery status and details of the last and next discovery scans.
- View Contained Files. For more information, see *Viewing contained files and saving them to an authorized location*.
- View the Forcepoint DLP Endpoint log files. For more information, see *Viewing logs*.

Related concepts
Disabling Forcepoint DLP Endpoint on page 17

> **Related tasks**
> Viewing contained files and saving them to an authorized location on page 38
> Viewing logs on page 39

Updating Forcepoint DLP Endpoint

Periodically, updated corporate policies and Forcepoint DLP Endpoint profiles are pushed to your endpoint machine to keep them up to date. To update them manually, click **Update** on the Forcepoint DLP Endpoint screen.

Disabling Forcepoint DLP Endpoint

> ⚠️ **Important**
>
> Disabling the endpoint software introduces possible vulnerabilities, because you are no longer receiving the protection provided by Forcepoint DLP Endpoint.

1) On the Forcepoint DLP Endpoint screen, click **Disable**.
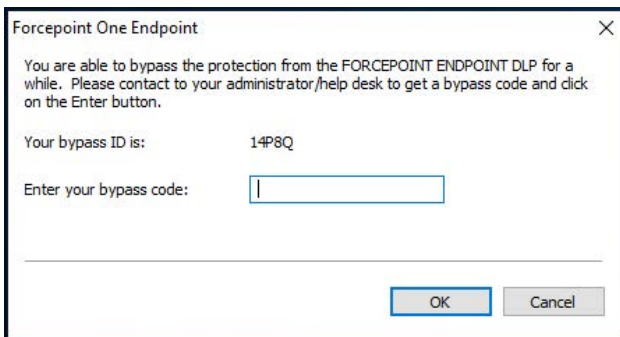
2) Report the bypass ID to your Forcepoint DLP administrator.

3) Enter the bypass code supplied by the administrator.

4) Click **OK**.

The Forcepoint DLP Endpoint software is disabled for the length of time specified when the bypass code was created. When the bypass protection expires, the Disabled icon () on the task bar updates to the Default icon ().

Enabling Monitoring in bypass mode

When we have the endpoint set to work in bypass mode, the DLP Endpoint does not report incidents to FSM (Forcepoint Security Manager) and no policies are enforced. The endpoint bypass mode might have been

enabled for a fixed period of time, to allow the user to perform certain tasks which will otherwise be blocked. For example, say to allow the user to copy a file to USB.

During the time, the endpoint is operating in bypass mode, there is no way of stopping a user from doing more than what they requested the bypass for and without the reporting, security administrators have no visibility into the user actions.

To allow the security administrators to see incidents for user actions for endpoint that are in bypass mode, we need to be able to see what policies would have been triggered on an endpoint that is in bypass mode, even when the endpoint is in bypass mode. For example, say the endpoint is in bypass mode, and the user copies a file that should be blocked to a USB, but because the endpoint is in bypass mode the file copy is allowed.

The endpoint will now record the actual action (Allowed) and the action that would have occurred if not in bypass mode (blocked). This information would be sent to the FSM (Forcepoint Security Manager) where it will get reported in the incident report.

Settings on the FSM to enable monitoring in bypass mode:

Security Administrators need to optionally select to monitor (report) polices violations when the Endpoint is in Bypass mode.

Set at the profile level in the "**Deployment** > **Endpoint Profiles**" section under the "**Properties**" tab.

Using the Forcepoint DLP Endpoint Diagnostics Tool (Windows only)

The Diagnostics Tool shows Forcepoint DLP Endpoint information that you can provide to your system administrator to assist with troubleshooting.

To launch the Diagnostics Tool:

1) Right-click the F1E icon in the task bar's notification area (Windows).

2) Select **Open F1E Diagnostics**.

When you launch the tool, the Diagnostics Tool automatically executes the **System information** diagnostics test, which collects basic information related to the specific

endpoint machine on which the Forcepoint DLP Endpoint software is installed. To manually run the diagnostics test, click the **Run Diagnostics** button.
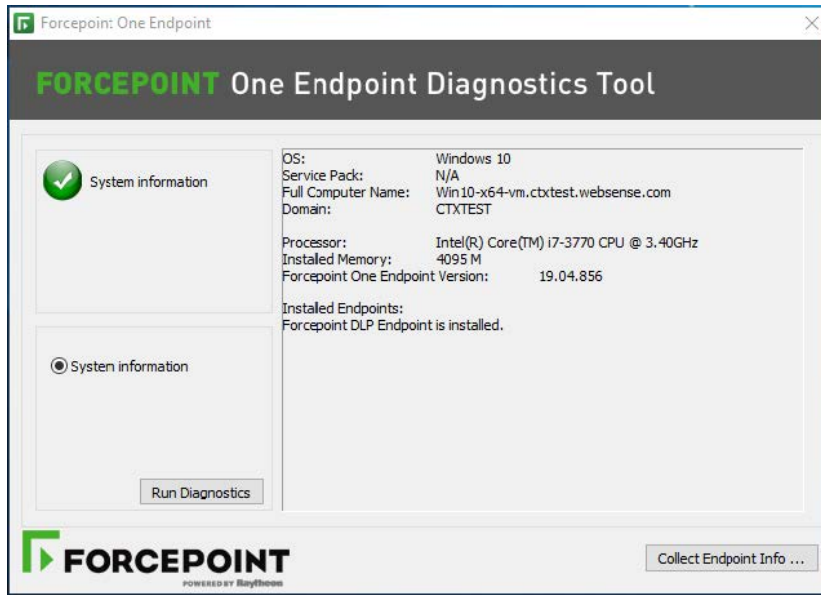
If Forcepoint Web Security Endpoint is also installed on your endpoint machine, the Diagnostics Tool shows additional information. See *Using the Forcepoint Web Security Endpoint Diagnostics Tool* for more information.

If Forcepoint Endpoint Context Agent is also installed on your endpoint machine, the Diagnostics Tool shows additional information for Forcepoint ECA.

> **Note**
>
> Corresponding log files generated from these new diagnostic tests can easily be collected with the existing **CLIENTINFO.EXE** tool. Your Help Desk might ask you to run this tool to collect these files. To run it, click the **Collect Endpoint Info...** button on the diagnostics screen. The resulting file is placed onto the desktop. Attach the file to an email to your Help Desk or system administrator.

Related tasks

Enabling the Forcepoint Safari extension

Forcepoint DLP Endpoint on macOS 10.14 and higher uses a Safari browser extension for Safari 12 and higher. This extension must be enabled. If the Forcepoint Safari extension is disabled on a JAMF-managed endpoint machine, a notification is shown when you open the Safari browser:
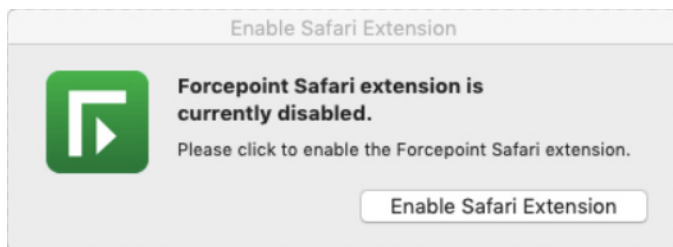
To enable the Forcepoint Safari extension, click the **Enable Safari Extension** button. An Extension window opens, allowing you to enable the Safari extension.

If the endpoint machine is not JAMF managed, the following notification is shown when you open the Safari browser:
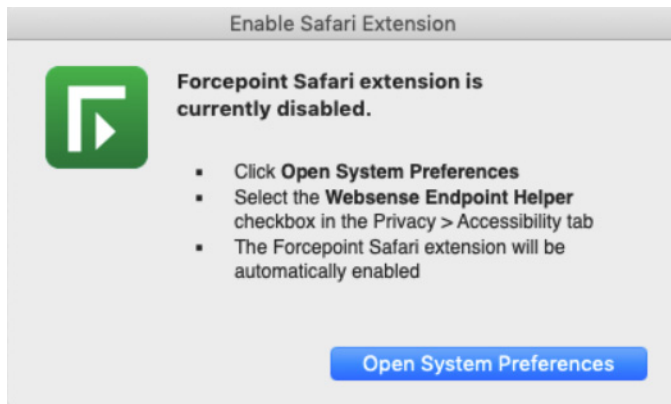
To enable the Forcepoint Safari extension from this notification, click the **Open System Preferences** button. Select the **Websense Endpoint Helper** check box in the **Privacy > Accessibility** tab. Then, the Forcepoint Safari extension is automatically enabled.

Updating the Mail plug-in

Forcepoint DLP Endpoint on macOS 10.14 and higher uses an Apple Mail plug-in for Safari 12 and higher. If the Forcepoint Mail plug-in needs to be updated on a JAMF- managed endpoint machine, a notification is shown when you open Mail:
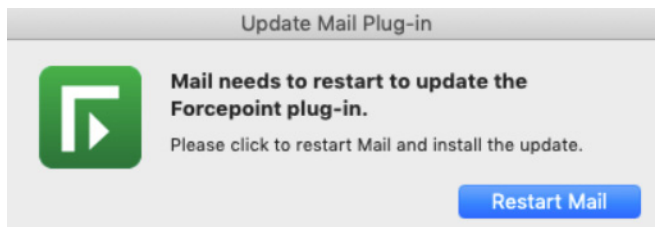
To enable the Forcepoint Mail plug-in, click the **Restart Mail** button. Mail is automatically restarted with the update installed.

If the endpoint machine is not JAMF managed, the following notification is shown when you open Mail:
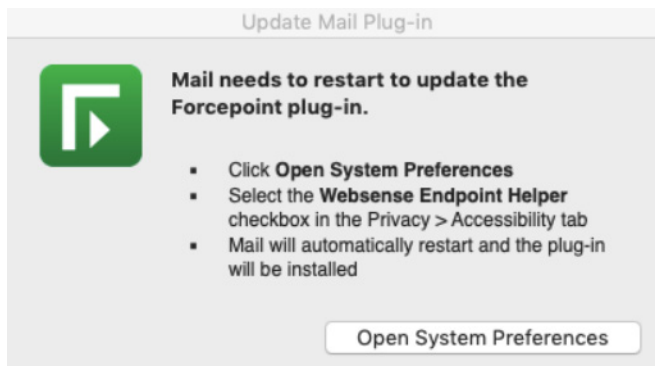
To enable the Forcepoint Mail plug-in from this notification, click the **Open System Preferences** button. Select the **Websense Endpoint Helper** check box in the **Privacy**

> Accessibility tab. The Forcepoint Mail plug-in is automatically restarted with the update installed.

Deploying Forcepoint F1E Outlook Add in

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

Custom Logo for Coaching Dialog

The coaching dialog feature allows to add a customer specific logo while building the installer for Forcepoint DLP Endpoint.

Steps to enable customer logo on the user's Endpoint machine:

1) On the DLP Server, navigate to **C:\Program Files(x86)\Websense\Data Security\client**. (See the image below)
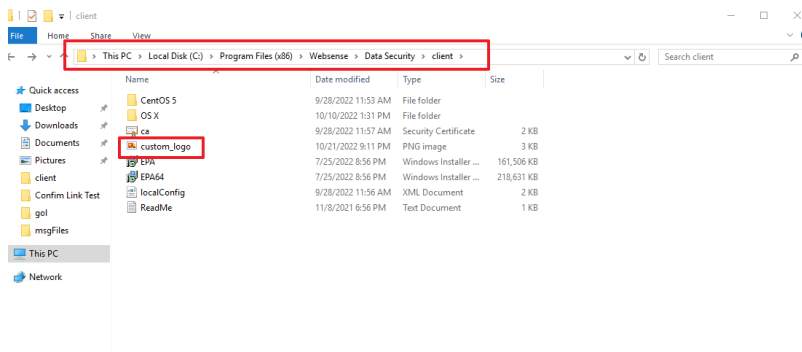
2) Add "custom_logo" file in the folder and run the **Package Build v22.12 or later** as you normally would.

> ⚠️ **Important**
>
> a) Make sure the name of the logo file to be added is correct.(File name should be "custom_logo.png")
>
> b) When you are adding the image file of the custom logo, make sure that:
>
>   i) The image height is less than 35px and the image width is less than 300px.
>
>   ii) The file type of the image should be of PNG format.

> **Note**
>
> You will receive the notification of successful installation after waiting for few minutes post running the package builder.

Custom Text for Coaching Dialog

The custom text feature allows a custom message to be displayed to the end user whenever a confirm action plan is triggered. The text can be customized per policy rule.

The text can explain the reason for the block, and when required, a URL can be configured to provide the end user extra information.

> **Note**
>
> - The character limit of custom text is 250 characters.
> - The number of lines is limited to 5 rows.
> - Make sure the custom message(text) and the URL are arranged in the following format:
> - Correct syntax: `<link>url="https://forcepoint.com" text="More Info"</link>`.
> - The required policy must have the confirmation action before implementation.

Steps

1) Navigate to **FSM** > **Policy Management** > **DLP Policies** > **Manage DLP Policies**.

2) Expand your preferred policy and click on the policy rule.

3) Insert the custom text and URL in the **"confirmation dialog text"** field.

> **Note**
>
> You can also add custom text at the policy rule exception level.
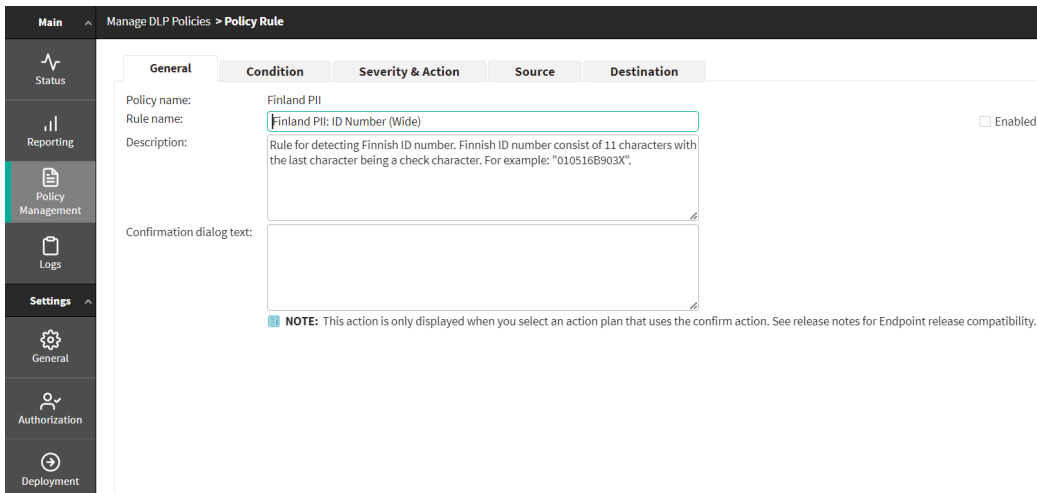
4) Click **OK**.

5) Click **Deploy** to implement the policy rule to the Endpoint.

> **Note**
>
> After the deployment is finished, switch to any Endpoint to check its functionality.

Forcepoint DLP Inline Proxy

Currently, Forcepoint F1E DLP uses its browser extensions to capture actions within web browsers. These extensions (in conjunction with File Access channel monitoring through the Advanced Tab) are used to enforce web inspection/policies on the endpoint machine.

The inline proxy, which runs locally on the Endpoint Client machine, is an alternative to enforce web policies and is intended to replace the use of Forcepoint Endpoint browser extensions eventually. Browser extensions will continue to be supported until we are satisfied with the inline proxy covering the web channel use cases.

It carries out local SSL decryption on the Endpoint Client to perform the required DLP analysis. Content is only decrypted locally and is re-encrypted before leaving the Endpoint.

Enabling Inline Proxy Mode in FSM

Users have the option to switch over to the Inline Proxy or stay in the browser extension mode to enable web traffic detection.

1) Go to **FSM** > **Deployment** > **Endpoint Profiles**.
You can see the list of profiles available for users.
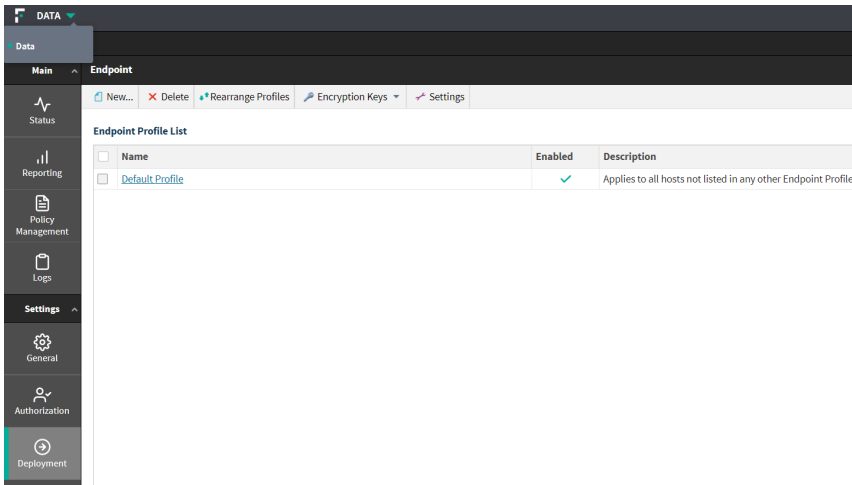
2) Click on the required Profile and go to **Properties** section.

3) In the **Endpoint Web Traffic Detection Mode**, you have the following options:

   a) Endpoint Inline Proxy

   b) Browser Extensions
   Select your preferred web traffic detecting option.
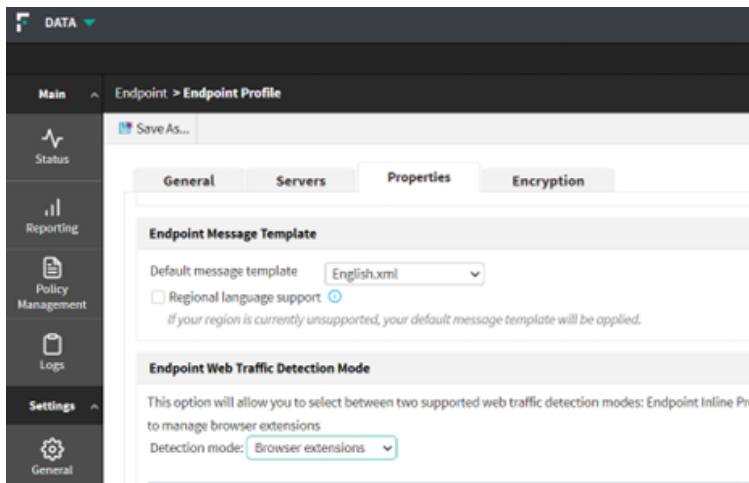
4) Select **Save**.

5) Click **Deploy**.

	Note
	Update the Forcepoint DLP Endpoint software.

6) Close your already opened browser session and reopen it.

Choosing Endpoint Web Traffic Capturing Mode

In the Inline Proxy mode, users can choose how they want the web traffic to be captured and sent to inline proxy. There are 2 options and both of them are enabled by default.

1) Using the system PAC.

2) Using the Forcepoint Driver.

This feature is useful when the user is using another agent, that uses the system PAC. In such case, user should deselect the system PAC in the FSM and use the driver only to capture traffic.

Steps

1) Navigate to **FSM** > **Deployment** > **Endpoint Profiles**.

You can see the list of profiles available for users.

2) Click on the required Profile and go to **Properties** Section.
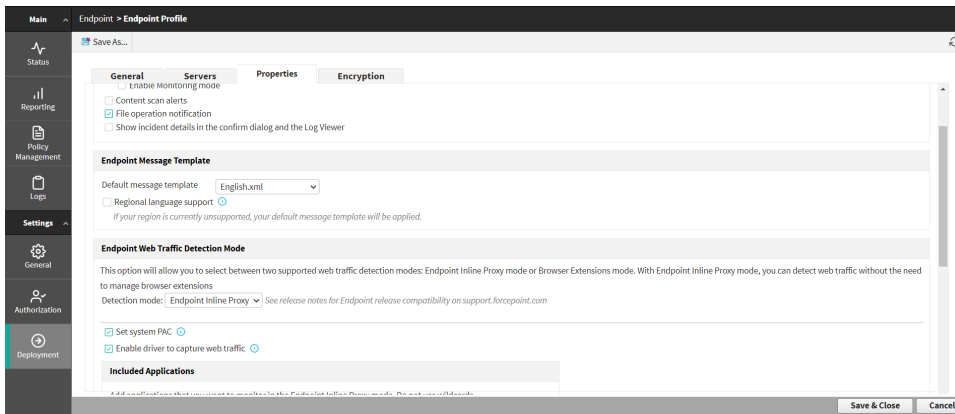
> 📝 **Note**
>
> Both the system PAC and Endpoint Driver are enabled by default in FSM.

3) Un-select **system PAC/Enable driver** and save it.

4) Click **Deploy**.

5) Update the Forcepoint DLP Endpoint software.

Adding applications to monitor list in Inline Proxy mode

Users can add applications they want to monitor in the Endpoint Inline Proxy Mode. They can also remove any application they want from the list. When a user removes any application from the list, the inline proxy stops monitoring the origin of the web traffic on the specific application.

Steps

1) Navigate to **FSM** > **Deployment** > **Endpoint Profiles**.

You can see the list of profiles available for users.
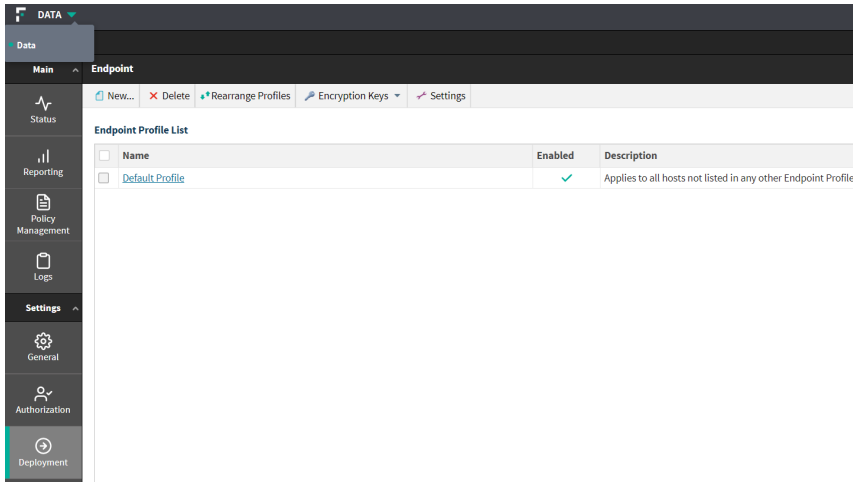
2) Click on your required Profile and go to **Properties** Section.

3) Scroll down to the **Included Applications** section.

> **Note**
>
> This section is only available when you have selected Inline Proxy mode for Web Traffic Detection.
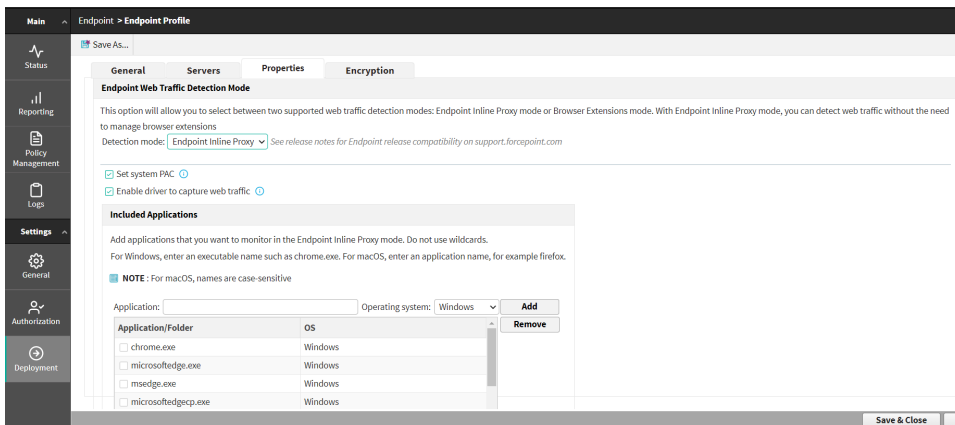
> **Note**
>
> Currently, the Inline Proxy mode supports the monitoring of browsers as applications.

4) Write the application name and select the OS.

5) Click **ADD**.

Check your application is added to the list.

6) Select **Save&Close**.

7) Click **Deploy**.

Excluding domains for JavaScript Injection

In Forcepoint Security Manager (FSM) 10.2 onwards, you can add or remove a domain to or from the domain list of an endpoint profile. When you add a domain URL to the list, JS injection is applied to all sites except to those in the list. F1E retrieves the JS injection bypass list from FSM, and apply policies accordingly.

Steps

1) Navigate to **FSM** > **Deployment** > **Endpoint Profiles**.

The list of profiles available for users appears.
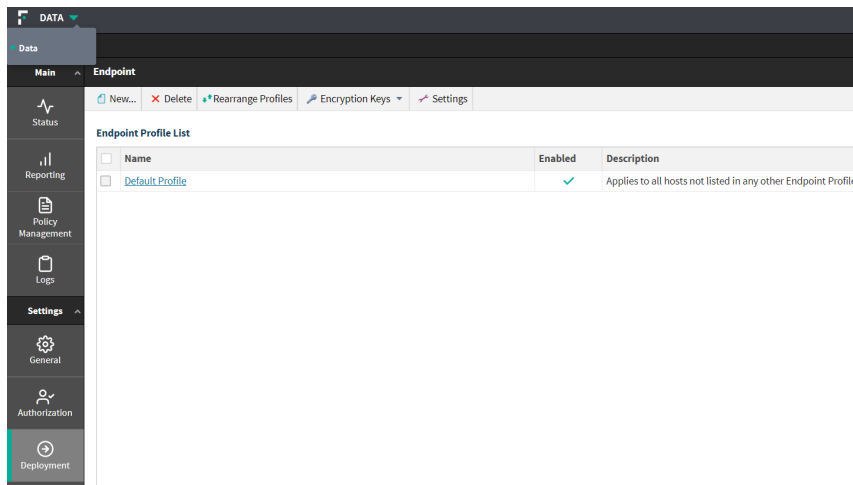
2) Click your required profile and go to **Properties** section.

3) Navigate to **Excluded Domains for JavaScript Injection** section.
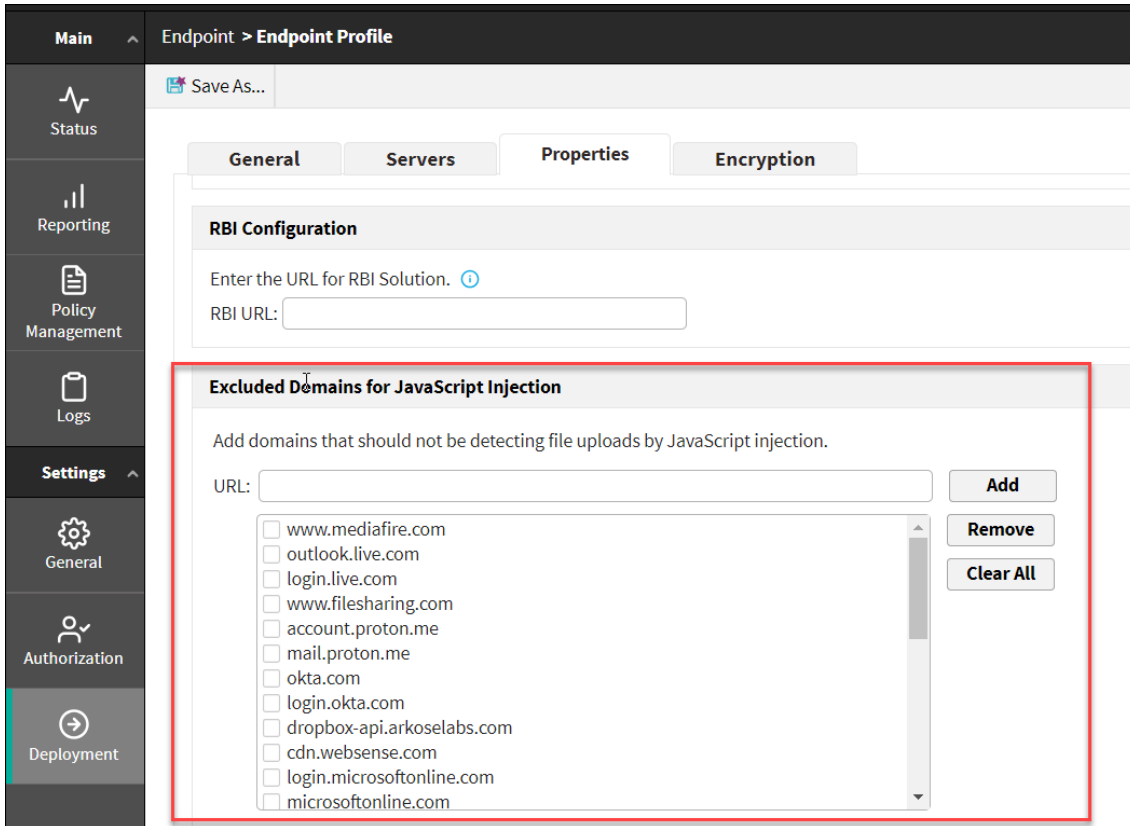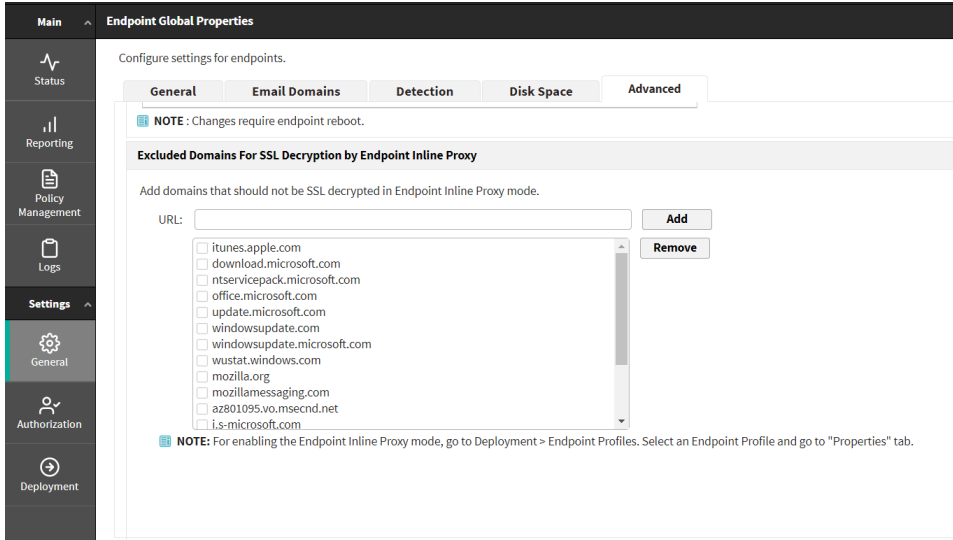
4) To add the URL to the excluded list, complete the steps below:

    a) Enter the domain name into **URL** field.

    b) Click the **Add** button to add the URL to the excluded domain list.

5) To remove the URL from list, complete the steps below:

    a) Mark the desired check boxes from the list to select the URLs.

    b) Click the **Remove** button to remove the URL from the excluded domain list.

    c) Click **Clear All** button to clear all URLs from the excluded list.

Adding domains to the SSL bypass list

Steps

1) Go to **General** > **Endpoint** > **Advanced tab**.

2) Scroll down to **Excluded Domains For SSL Decryption by Endpoint Inline Proxy**.

> **Note**
>
> This section is only available when you have selected Inline Proxy mode for Web Traffic Detection.

3) Add the domain which you want to bypass in the URL section.

4) Click **ADD**.

The domain update gets applied to both macOS and Windows Endpoints.

5) Click **Deploy**.

> ⛔ **Warning**
>
> No DLP Policies are applicable to the Inline Proxy bypassed URLs when these sites use HTTPS or Encryption.

Port Forwarding to Support Third Party Agents

The port forwarding feature allows users having more than one local proxy, to enter multiple IP addresses and port numbers of their local proxies, thus enabling the inline proxy to forward the web traffic to the user's local proxies.

This feature can be used if a 3rd party agent is also running on the endpoint which is intercepting traffic using a PAC file and redirecting to a local proxy. In this case, the IP address and port of the local proxy needs to be configured to ensure Forcepoint F1E endpoint also receives the traffic.

Steps to configure port forwarding

1) Navigate to **FSM** > **Deployment** > **Endpoint Profiles**.
You can see the list of profiles available for users.
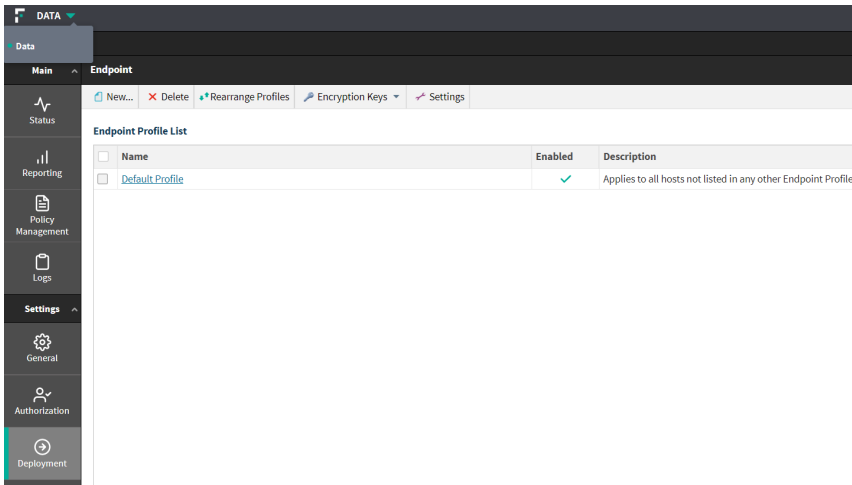
2) Click on the required Profile and go to **Properties** Section.

3) In the **Web Traffic Detection Mode**, select **Endpoint Inline Proxy**.

4) Disable the system PAC file.

5) Enter your local proxy IP address and port number.

> **Note**
>
> If more than one proxy is to be set, then each entry should be separated by a comma ","
>
> E.G:- 127.0.0.1:9000, 127.0.0.100:9001
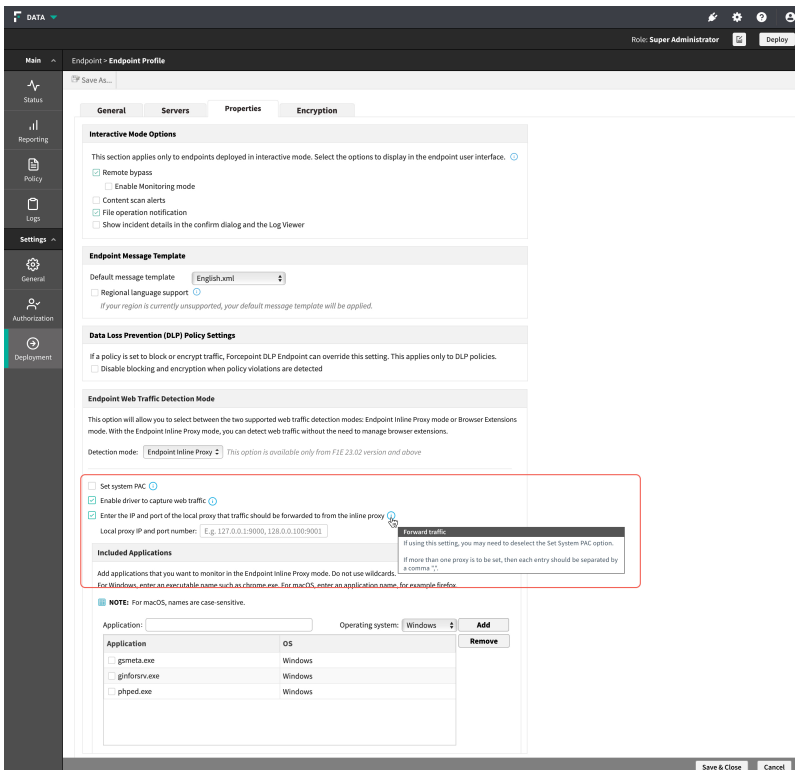
6) Select **Save**.

7) Click **Deploy**.

> **Note**
>
> Update the Forcepoint DLP Endpoint software.

8) Close your already opened browser session and reopen it.

Inline Proxy Settings for Forcepoint DLP Endpoint

This topic covers the FSM Inline Proxy Settings for various product combinations on different Endpoint machines. For detailed information, see Agent Compatibility.

Online Applications in macOS

Online applications are web-based mail services (e.g., Gmail and Yahoo Mail) and file storage systems (e.g., Google Drive). Protection for sensitive data in attachments for these services mitigates upload risk for Chrome, Firefox, and Safari browsers in macOS. This protection (Online Apps) is supported for macOS 10.14 and higher.

> **Note**
>
> The online applications are only available in the browser extensions mode.

Allowing or blocking a policy violation

When the confirmation dialog functionality is enabled at your site, corporate policy violations are not automatically blocked by Forcepoint DLP Endpoint. Instead, they are allowed if you provide a valid explanation for the operation.

If a policy violation is detected, Forcepoint DLP Endpoint displays a confirmation dialog box.

Forcepoint ONE Endpoint

Action required
Time Remaining: **28** seconds

ⓘ This operation appears to be in violation of corporate policy.

Policy violations: ⓘ test_policy - 1 Violation triggers

If you feel this operation is justified, please select a reason and click Allow. If you would like to cancel this operation, please click Block.

◯ Acceptable operation (false positive)
◯ Required for business purposes
◯ Approved by my manager
◯ Personal data
◯ Redacted data

Enter justification (optional)

Read more about our corporate policy

| Allow | Block |

From this confirmation dialog box, you can choose to allow the operation to continue, or you can block the operation and cancel the request.

To continue with the action:

1) Select a valid reason from the list.

2) Optionally, type additional information in the text box (maximum 256 characters).

3) Click **Allow**.

To cancel the action, click **Block**.

If the timer expires, the default action is taken. The timer default is set to 30 seconds, but can be changed by your system administrator to between 9 and 58 seconds.

⚠ **Important**

If you click the corporate policy link at the bottom of the window and Chrome is your default browser, Chrome does not open the link until you close the confirmation dialog window.

The behavior of the confirmation or block action varies depending on the action and the affected channel:

- Removable Media Channel:
  - If you copy or move sensitive documents either through the Windows command line or by dragging and dropping the files through Windows Explorer to a USB drive, a writable DVD, or a mobile phone through WPD protocol, and choose the Block action in the confirmation box, Forcepoint DLP Endpoint might also block non-sensitive files if they are copied or moved with the sensitive files.

- LAN Channel:
  - If you copy or move files to other machines mounted on the endpoint machine in the same local network, and choose the Block action in the confirmation dialog box, Forcepoint DLP Endpoint might incorrectly state that the files were copied or moved.
  - If you try to move a sensitive file to a network share folder using cut and paste, then choose the Block action in the confirmation dialog box, Forcepoint DLP Endpoint removes the file from both the source location and the destination. If this happens, look for the file in the Contained Files. See *Viewing contained files and saving them to an authorized location*.

- HTTP/HTTPS (Web) Channel:

- If you compose email through a web-based mail service (e.g., Gmail or Yahoo Mail), a confirmation dialog box is shown whenever the service syncs to the hosting server (i.e., when the email is auto-saved). This causes the confirmation dialog box to be shown multiple times within a short timeframe.

- Each sensitive attachment within an email triggers a separate confirmation dialog box.

- If you choose the Block action, you might receive an error message from the mail service, because the Block action interrupts the activity with the mail service.

- Print Channel:

  - This channel blocks the printing of sensitive content when you try to print a hard copy through a printer or a soft copy through a PDF converter.

- Application Clipboard Channel:

  - This channel allows you to copy and/or paste sensitive content within the same document, or to the same type of document (e.g., from one Microsoft Word document to another Word document).

- Application File Access Channel:

  - If you choose the Block action, you might receive an error message from the application, because the Block action interrupts the activity with the application.

  - When saving a sensitive document, you might receive multiple confirmation dialog boxes, because temporary files created by the application trigger the confirmation dialog box.

- Email Channel:

  - In Outlook, the Outlook process is suspended when the confirmation dialog box is shown. This makes it appear as if Outlook is no longer working. Once you choose either the Allow or Block action, the Outlook process works as normal.

Related tasks
Viewing contained files and saving them to an authorized location on page 38

Applying policies to Google Drive mounted as a USB device

F1E DLP applies web channel policies to files transferred in Google Drive.

Google Drive, when mounted as a USB device or other network drive is classified as cloud storage rather than removable media. When you upload a file having sensitive information restricted for web channels to Google Drive, F1E DLP applies policies and blocks the file from being uploaded to Google Drive. Files containing sensitive information that is blocked for a USB device is not blocked in Google Drive.

For more information, see *Configuring the Web DLP Policy in* Forcepoint DLP v10.2 Administrator Help guide.

Encrypting files for removable media

Forcepoint DLP Endpoint provides two methods for encrypting sensitive data that is copied to removable media:

- **Encrypt with profile key** (Windows only): When you transfer files to removable media, the files are encrypted automatically with an encryption password deployed in the endpoint profile. When you try to transfer the encrypted files again, Forcepoint DLP Endpoint automatically decrypts the files using the deployed password if the user decrypting the files is using the same profile.

■ **Encrypt with user password** (Windows only): When you transfer files to removable media, the files are encrypted automatically. When you try to transfer the encrypted files again, you must use the Forcepoint Decryption Utility and an encryption password to decrypt the files.

For more information about setting your encryption password, see *Setting encryption passwords*.

For more information about decrypting files, see *Decrypting files on a removable media device.*

Contact your administrator to see which option is configured in your organization. To see if your organization encrypts data with a user password, right-click the Forcepoint One Endpoint icon in the task bar's notification area on a Windows endpoint machine. If you see a **Set Encryption Password** option, your organization encrypts data with a user password.

> **Related concepts**
> Decrypting files on a removable media device on page 35

> **Related tasks**
> Setting encryption passwords on page 34

Setting encryption passwords

Some corporate policies dictate that sensitive data be encrypted before being copied to a removable media device such as a USB drive. If this is the case for your organization, you cannot copy files to such media until you set the password to decrypt them.

> 📝 **Note**
>
> Forcepoint DLP Endpoint does not support the encryption of data transferred to a Windows Portable Device (WPD) from a Windows endpoint machine.

Set the password one time, then any time you copy sensitive data to removable media, it is encrypted and copied along with a Forcepoint Decryption Utility to the device. You, or any other user accessing the files on endpoint machines where the Forcepoint DLP Endpoint is not installed, or where the password configured for encryption is different than yours, must enter this password.

> ⚠️ **Important**
>
> The encryption password can only be set on a Windows endpoint machine running Forcepoint DLP Endpoint, You cannot set an encryption password or encrypt files on a Mac endpoint machine. You can only decrypt files on a Mac endpoint machine.

To set the encryption password:

1) Right-click the F1E icon in the task bar's notification area.

2) Select **Set Encryption Password** from the menu.

3) Enter your password, then re-enter your password.

> **Note**
>
> The password should be at least 8 characters in length (maximum is 15 characters), and it should contain:
>
> - At least one numeral
> - At least one symbol
> - At least one capital letter
> - At least one lowercase letter
>
> The following example shows a strong password:
>
> - 8%w@s1*F

4) Click **OK**.

> **Warning**
>
> Keep the encryption password in a safe place. If you forget your password, it cannot be recovered and the file cannot be decrypted.

Decrypting files on a removable media device

To decrypt the content on your removable media device, you must run a Forcepoint Decryption Utility. Content that was encrypted on Windows can be decrypted on any Windows or Mac machine. (Content cannot be encrypted on Mac. It can only be decrypted on Mac.)

The Forcepoint Decryption Utility is copied to your removable media device along with the encrypted files. For more information, see *Decrypting Files on Windows* and *Decrypting Files on Mac*.

> **Related tasks**

Decrypting files on Windows

Steps

1) Insert the removable device into a Windows laptop or desktop.

2) Double-click **Forcepoint Decryption Utility.exe** or **wsdecrypt.exe**, depending on the Forcepoint DLP Endpoint version installed:

- Forcepoint Decryption Utility.exe:
  - Decrypts files on a Windows endpoint machine that does not have Forcepoint DLP Endpoint installed.
  - Decrypts files that were encrypted on a Windows endpoint machine with TRITON AP-ENDPOINT v8.3, Forcepoint DLP Endpoint v8.4, or higher.
- wsdecrypt.exe:
  - Decrypts files that were encrypted on a Windows endpoint machine with TRITON AP-ENDPOINT DLP v8.2.5 or lower installed.

> **Note**
>
> If you don't know the version, open Forcepoint Decryption Utility.exe. This utility checks the version and either decrypts the files, or opens wsdecrypt.exe if the version is v8.2.5 or lower.

3) Enter the encryption password when prompted. For more information about setting the encryption password, see *Setting encryption passwords*.

> **Warning**
>
> Keep the encryption password in a safe place. If you forget your password, it cannot be recovered and the file cannot be decrypted.

A dialog box opens and displays lists of subdirectories and files on your system.

4) Navigate to the folder containing the encrypted files. By default, the files are on your removable media device.

5) Select the folders and files to decrypt, right-click, and select **Save To**.

6) Select the folder in which to save the decrypted files.

> **Note**
>
> The Decryption Utility Help page might show an older version (8.5.x) and updated date. This is the latest version of the utility and works with Forcepoint DLP Endpoint v22.12.

Related tasks
Setting encryption passwords on page 34

Decrypting files on Mac

Steps

1) Insert the removable device into a Mac laptop or desktop.

2) Double-click **Forcepoint Decryption Utility.dmg** and mount it as a disk volume.

3) Launch the application **Forcepoint Decryption Utility** in the disk volume or from the launchpad.

4) Drag and drop the encrypted files from the removable media device into the application's list window.
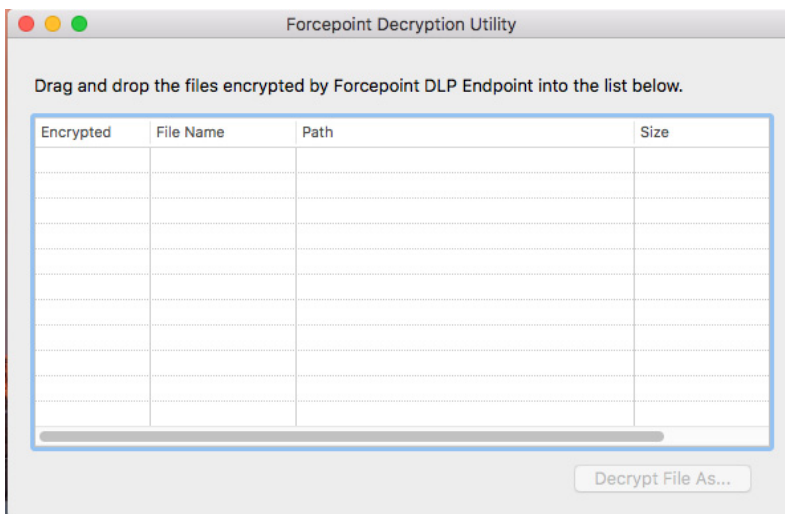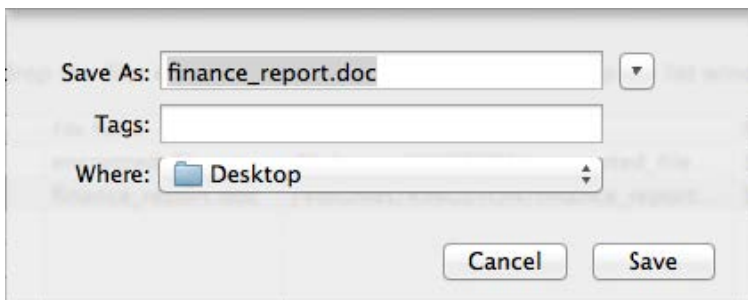

5) Select the file to decrypt, and select **Decrypt File As**. If the selected file is not encrypted by Forcepoint DLP Endpoint, the operation is disabled.

6) Enter the encryption password when prompted, then click **OK**. For more information about setting the encryption password, see *Setting encryption passwords*.
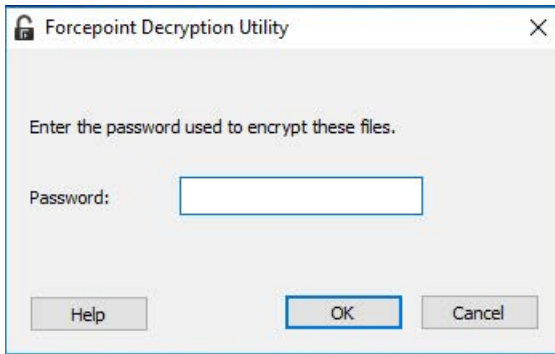
A file save dialog box opens if the correct password is entered.

7) Enter the file name that you want to save the decrypted file as.

8) If necessary, select the next file to decrypt. The password prompt is not shown again if the file is encrypted by the same password.

The Forcepoint Decryption Utility decrypts the files using the password you provided and places them in this path. Files that were encrypted with a different password are not decrypted.

> **Note**
>
> The Decryption Utility Help page might show an older version (8.5.x). This is the latest version of the utility and works with Forcepoint DLP Endpoint v22.12.

Related tasks
Setting encryption passwords on page 34

Viewing contained files and saving them to an authorized location

Contained files are files that are held in temporary storage on an endpoint machine.

Files are contained if your organization prevents sensitive information from being written from an endpoint machine to a removable device (such as a USB flash drive, CD/DVD, or external hard disk) or a network drive, and you try to move a file to an unauthorized device. If the file has been modified, the contained file includes the modified file, but removes the modified file from the unauthorized device.

> ⚠️ **Important**
>
> Contained files are automatically deleted after 7 days.

You can view the contents of contained files and choose to save them to an authorized location instead.

1) On the Forcepoint DLP Endpoint screen, click **Contained Files**.
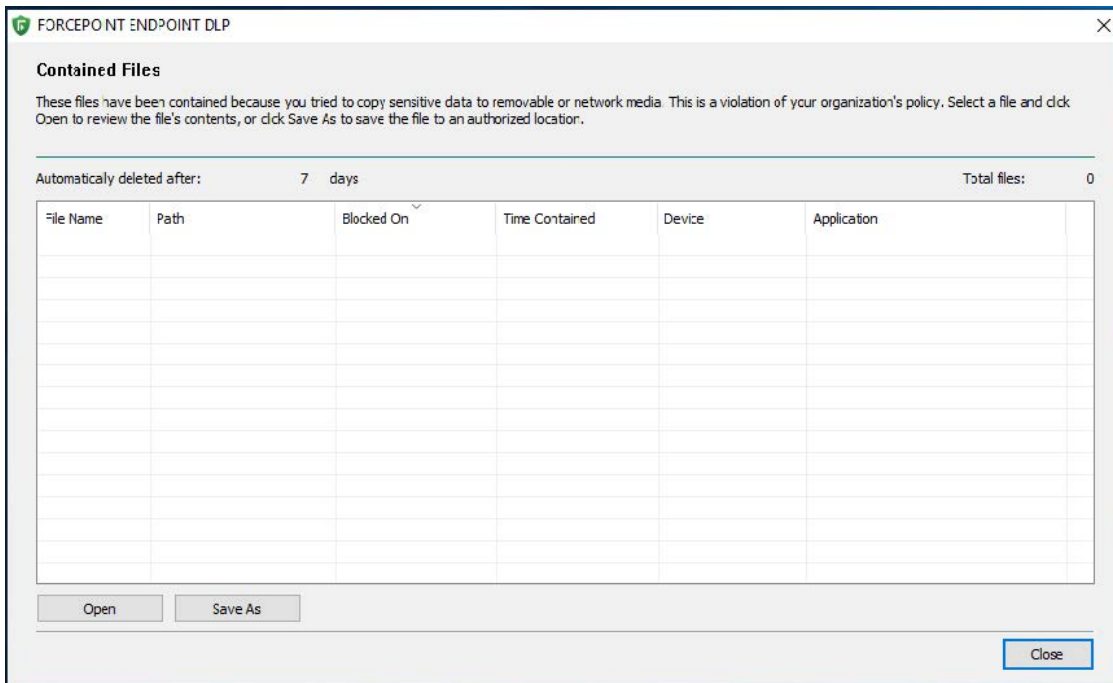
2) To see the contents of a file, select the file and click **Open**.

3) To save a file to an authorized location, select the file and click **Save As**. You can now view the file from the new location.

4) Click **Close** when done.

Viewing logs

There are two logs available in Forcepoint DLP Endpoint:

- The **System Log** contains information about changes on your machine. For example:
  - Changes of connection status, such as your endpoint machine moving from an office to a remote location
  - When Forcepoint DLP Endpoint is enabled or disabled
  - When Forcepoint DLP Endpoint profiles are applied and updated
  - When Forcepoint DLP Endpoint is connected to or disconnected from the Forcepoint DLP Endpoint server
- The **Content Log** contains information about file operations that have been picked up by the endpoint policy and any actions taken by Forcepoint DLP Endpoint as a result.

To see the log details, choose one of the following options:

1) On the Forcepoint DLP Endpoint screen, click **Log Viewer**.

2) Right-click the F1E icon in the task bar's notification area and select **Open Log Viewer** from the menu (Windows), or single click the menu bar's status menu (Mac) and select **Log Viewer** from the menu.

3) To see the latest log information, click **Refresh**.

> ⚠️ **Important**
>
> Log files are automatically deleted after 5 days.

Chapter 4

Forcepoint Endpoint Context Agent

Contents

Forcepoint Endpoint Context Agent (Forcepoint ECA) is a software application that runs on your Windows endpoint machine (e.g., desktop computer or laptop), providing user and application information to the Forcepoint Next Generation Firewall (Forcepoint NGFW).

Related concepts
Viewing Forcepoint Endpoint Context Agent connection details on page 43

Related tasks
Using the Forcepoint ECA Diagnostics Tool on page 43

Related reference
Checking the status of Forcepoint Endpoint Context Agent on page 41

Checking the status of Forcepoint Endpoint Context Agent

The F1E status icon () is shown in the task bar's notification area. To view the status of Forcepoint ECA, move your mouse over the icon. The following table describes the available status indicators.

Icon	Meaning	Description
	Running	Forcepoint ECA software is successfully connected to Forcepoint NGFW, configured and activated.

Icon	Meaning	Description
	Disconnected	All Forcepoint ECA connections are disconnected from Forcepoint NGFW. If other agents are installed on your endpoint machine, this status indicates that all installed F1E agents are disabled or disconnected. To verify the connection status, move your mouse over the F1E icon. A pop-up window shows the connection status for all installed agents. All installed agents should show **Disabled** (Forcepoint ECA shows as **Disconnected**).
	Fallback Partially Disabled	This status may indicate that: ■ One or more installed agent (Forcepoint DLP Endpoint, Forcepoint Web Security Endpoint or Forcepoint ECA) is disabled, but at least one agent is enabled or running. If all agents are disabled, this status icon is not shown (the Disabled status icon described above is shown). ■ Forcepoint Web Security Endpoint is in Fallback mode. See *Fallback mode* for more information.

If your organization installs more than one F1E agent (Forcepoint Web Security Endpoint, Forcepoint DLP Endpoint and/or Forcepoint ECA) on your endpoint machine, you can access all installed agents from one Forcepoint icon on your task bar.

For more information about Forcepoint Web Security Endpoint and Forcepoint DLP Endpoint, see *Forcepoint Web Security Endpoint* and *Forcepoint DLP Endpoint*.

Related concepts
Fallback mode on page 10
Forcepoint Web Security Endpoint on page 7
Forcepoint DLP Endpoint on page 13

Viewing Forcepoint Endpoint Context Agent connection details

To see a list of Forcepoint ECA connections to Forcepoint NGFW:

1) Right-click the F1E icon located in the Windows task bar's notification area.

2) Select **View Forcepoint ECA Connection Status** from the menu.

A window opens showing all available connections to Forcepoint NGFW and the connection status.

The connection status can be one of the following:

- **DISCONNECTED**: Forcepoint ECA is not connected to the Forcepoint NGFW Engine.
- **WAITING_RECONNECT**: The connection between Forcepoint ECA and the Forcepoint NGFW Engine was stopped. Forcepoint ECA is trying to establish the connection again.
- **CONNECTING**: Forcepoint ECA is connecting to the Forcepoint NGFW Engine.
- **CONNECTED**: Forcepoint ECA is connected to the Forcepoint NGFW Engine.
- **HANDSHAKING**: Forcepoint ECA is establishing a communication link to the Forcepoint NGFW Engine.
- **CONFIGURING**: Forcepoint ECA is getting configuration information from the Forcepoint NGFW Engine.
- **CONFIGURED**: Forcepoint ECA is successfully configured on the endpoint machine and is sending data to the Forcepoint NGFW Engine.

Using the Forcepoint ECA Diagnostics Tool

The Diagnostics Tool shows Forcepoint ECA information that you can provide to your system administrator to assist with troubleshooting.
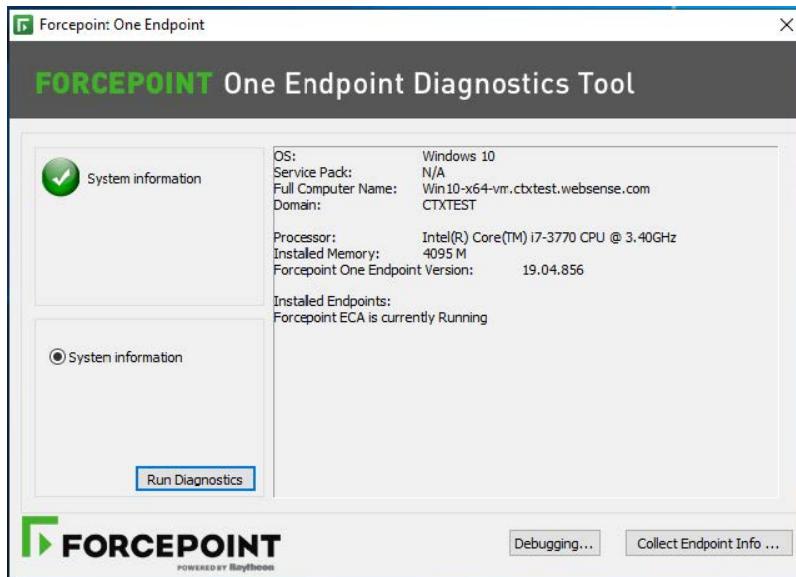
To launch the Diagnostics Tool:

Steps

1) Right-click the F1E icon located in the Windows task bar's notification area.

2) Select **Open F1E Diagnostics** from the menu.

Next steps

When you launch the tool, the Diagnostics Tool automatically executes the **System information** diagnostics test, which collects basic information related to the specific endpoint machine on which the Forcepoint ECA software is installed. To manually run the diagnostics test, click the **Run Diagnostics** button.

If Forcepoint Web Security Endpoint is also installed on your endpoint machine, the Diagnostics Tool shows additional diagnostics tests and Forcepoint Web Security Endpoint information. See *Using the Forcepoint Web Security Endpoint Diagnostics Tool* for more information.

If Forcepoint DLP Endpoint is installed on your endpoint machine, the Diagnostics Tool shows both Forcepoint DLP Endpoint and Forcepoint ECA information.

> **Note**
>
> Corresponding log files generated from these new diagnostic tests can easily be collected with the existing **CLIENTINFO.EXE** tool. Your Help Desk might ask you to run this tool to collect these files. To run it, click the **Collect Endpoint Info...** button on the Diagnostics Tool. The resulting zip file is placed onto the desktop. Attach the file to an email to your Help Desk or system administrator.

Related tasks
Using the Forcepoint Web Security Endpoint Diagnostics Tool on page 9