



End User's Guide

Forcepoint™ Endpoint Solutions

v8.5.x

©2018 Forcepoint
All rights reserved.
10900-A Stonelake Blvd., Quarry Oaks 1, Suite 350, Austin, TX 78759, USA
Published 2018

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint. Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

Topic 1	Introduction to Forcepoint Endpoint Solutions.	1
	Forcepoint Web Security Endpoint.	1
	Forcepoint DLP Endpoint.	1
Topic 2	Forcepoint Web Security Endpoint	3
	How to check the status of Forcepoint Web Security Endpoint.	3
	How to use the Forcepoint Web Security Endpoint diagnostics tool.	5
	Fallback mode	6
	How to view logs	7
	How to disable Forcepoint Web Security Endpoint protection	8
Topic 3	Forcepoint DLP Endpoint	9
	How to check the status of Forcepoint DLP Endpoint.	9
	How to confirm or block a policy violation	11
	How to set encryption passwords.	13
	Decrypting files on a removable media device.	14
	Decrypting files on Windows	14
	Decrypting files on Mac	15
	How to view contained files and save them to an authorized location	16
	How to view logs	17
	How to update Forcepoint DLP Endpoint	18
	How to disable Forcepoint DLP Endpoint.	19

1


Introduction to Forcepoint Endpoint Solutions


End User's Guide | Endpoint Solutions | Cloud and On-Premises v8.5.x


Your organization uses Forcepoint Endpoint solutions to protect you and other users against advanced web-based threats and data theft while on and off the corporate network. Endpoint solutions include server software installed on corporate servers and client software installed on your computer.

This guide covers the following two Forcepoint Endpoint solutions:

- Forcepoint Web Security Endpoint defends your computer against web threats.
- Forcepoint DLP Endpoint protects your organization from the unintended loss of data and data theft.

If you see this icon  in your task bar, Forcepoint Web Security Endpoint protection is available and enabled on your Windows endpoint machine.

If you see this icon  in your task bar, Forcepoint DLP Endpoint is protecting you and your organization on your Windows endpoint machine.

If you see this icon  in your menu bar, Forcepoint DLP Endpoint is protecting you and your organization on your Mac endpoint machine.

This guide covers the following:

Forcepoint Web Security Endpoint

- [How to check the status of Forcepoint Web Security Endpoint, page 3](#)
- [How to use the Forcepoint Web Security Endpoint diagnostics tool, page 5](#)
- [Fallback mode, page 6](#)
- [How to view logs, page 7](#)
- [How to disable Forcepoint Web Security Endpoint protection, page 8*](#)

Forcepoint DLP Endpoint

- [How to check the status of Forcepoint DLP Endpoint, page 9](#)
- [How to confirm or block a policy violation, page 11](#)
- [How to set encryption passwords, page 13](#)

- [How to view contained files and save them to an authorized location, page 16](#)
- [How to view logs, page 17](#)
- [How to update Forcepoint DLP Endpoint, page 18](#)
- [How to disable Forcepoint DLP Endpoint, page 19*](#)

*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 or both if both are installed and disabled.



Note

This guide covers the full range of functionality available in both the Forcepoint Web Security Endpoint and Forcepoint DLP Endpoint tools. Some functionality might be disabled by your organization's security policies. This disabled functionality will not be available to use.

2

Forcepoint Web Security Endpoint

End User's Guide | Forcepoint Web Security Endpoint | Cloud and On-Premises v8.5.x

Forcepoint Web Security Endpoint is a software application that runs on your endpoint machine (e.g, desktop computer or laptop), protecting you from malware and enforcing your organization's acceptable user policy.

How to check the status of Forcepoint Web Security Endpoint





End User's Guide | Forcepoint Web Security Endpoint | Cloud and On-Premises v8.5.x

Related topics:

- [Fallback mode, page 6](#)
- [How to disable Forcepoint Web Security Endpoint protection, page 8](#)
- [How to use the Forcepoint Web Security Endpoint diagnostics tool, page 5](#)
- [How to view logs, page 7](#)

This applies to Windows operating system users. On Mac endpoint machines, the system is protected without interaction, so no icon displays.


To view the status of Forcepoint Web Security Endpoint, hover over the Forcepoint icon in your task bar. Icons serve as a status indicator and an access point to additional diagnostic information:

Icon	Meaning	Description
	Enabled	Forcepoint Web Security Endpoint software is successfully configured and activated.
	Disabled	<p>You have manually disabled the endpoint software on your computer. Your computer is no longer being protected against web threats. You can re-enable the software manually or it will be enabled when your computer is restarted.</p> <p>The ability to enable/disable endpoint software is allocated by your system administrator.</p> <p>See How to disable Forcepoint Web Security Endpoint protection.</p>
	Fallback	Network events prevented your endpoint software from connecting with cloud servers. You are no longer being protected against web threats. This icon displays for endpoint machines that go through a proxy before connecting to the Internet.
	Fallback	Network events prevented your endpoint software from connecting with cloud services. The system applies filters cached during the last connection to the Internet. Your computer is partially protected against web threats. This icon displays for endpoint machines that connect directly to the Internet.



Important

If you manually disable Forcepoint Web Security Endpoint, a reboot always re-enables it.

Note that if your organization is using both Forcepoint Web Security Endpoint and Forcepoint DLP Endpoint, a Forcepoint DLP Endpoint icon  displays on your task bar as well. For more information about Forcepoint DLP Endpoint, see [Forcepoint DLP Endpoint, page 9](#).

How to use the Forcepoint Web Security Endpoint diagnostics tool

End User's Guide | Forcepoint Web Security Endpoint | Cloud and On-Premises v8.5.x

Related topics:

- [How to check the status of Forcepoint Web Security Endpoint, page 3](#)
- [Fallback mode, page 6](#)
- [How to disable Forcepoint Web Security Endpoint protection, page 8](#)
- [How to view logs, page 7](#)

This applies to Windows operating system users. Forcepoint Web Security Endpoint offers a diagnostics tool that you can access by double-clicking the Forcepoint icon in the task bar. The tool displays information that you can provide to your system administrator to assist with troubleshooting if Forcepoint Web Security Endpoint is not behaving as expected.

When the tool is launched, each of the diagnostic tests is 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:

1. **System information** - Collects basic information related to the specific system on which the Forcepoint Web Security Endpoint software is installed.
2. **Network diagnostics** - Collects information related to basic network connectivity.
3. **PAC file status** - For endpoint machines that go through a proxy before connecting to the Internet, collects information to determine if the PAC file is accessible.

OR

Cloud services - For endpoint machines that connect directly to the Internet, 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 diagnostics 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 HelpDesk or system administrator.

Fallback mode

End User's Guide | Forcepoint Web Security Endpoint | Cloud and On-Premises v8.5.x


Related topics:


- [How to check the status of Forcepoint Web Security Endpoint, page 3](#)
- [How to disable Forcepoint Web Security Endpoint protection, page 8](#)
- [How to use the Forcepoint Web Security Endpoint diagnostics tool, page 5](#)
- [How to view logs, page 7](#)

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 Forcepoint icon displayed in your task bar changes to reflect your level of protection.

If you see this icon  in your task bar, 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 (provided Internet access is available), but endpoint protection is not provided during this time.

If you see this icon  in your task bar, your system is in Fallback mode and is **partially** protected. When network events prevent endpoint machines from

connecting with cloud services, Forcepoint Web Security Endpoint applies the filter cached from the last connection to the Internet. For example, if the user normally sees a block page when visiting Facebook, then the user would also see a block page when visiting Facebook while in Fallback mode. The block page indicates that it is a result of cached results.

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

How to view logs

End User's Guide | Forcepoint Web Security Endpoint | Cloud and On-Premises v8.5.x

Related topics:

- [How to check the status of Forcepoint Web Security Endpoint, page 3](#)
- [Fallback mode, page 6](#)
- [How to use the Forcepoint Web Security Endpoint diagnostics tool, page 5](#)

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

- Event ID 258: "User disabled Forcepoint SaaS Service."
- Event ID 257: "Forcepoint SaaS Service has entered cloud enforce mode."

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

How to disable Forcepoint Web Security Endpoint protection

End User's Guide | Forcepoint Web Security Endpoint | Cloud and On-Premises v8.5.x

Related topics:

- [How to check the status of Forcepoint Web Security Endpoint, page 3](#)
- [Fallback mode, page 6](#)
- [How to use the Forcepoint Web Security Endpoint diagnostics tool, page 5](#)
- [How to view logs, page 7](#)

Disabling the Forcepoint Web Security Endpoint software removes the protection provided by the endpoint service, and stops it from intercepting traffic and securing your computer 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, when you right click the Forcepoint Web Security Endpoint icon, you will see the option to **Disable** it. Select **Disable** to disable the endpoint software at any time.

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, click **Enable**.



Important

If you manually disable Forcepoint Web Security Endpoint, a reboot always re-enables it.

3

Forcepoint DLP Endpoint

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x



Forcepoint DLP Endpoint (Data Loss Prevention) expands protection to sensitive information stored on your computer. 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.)

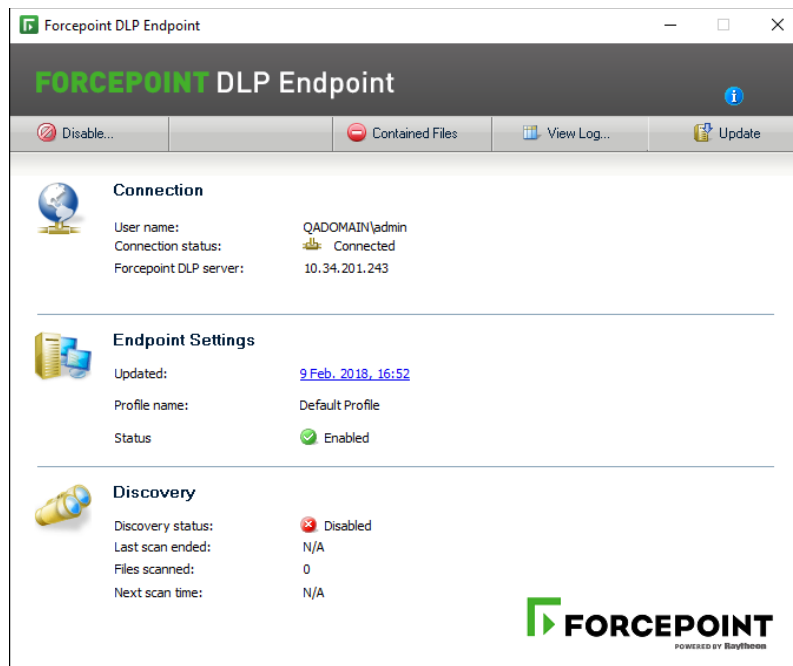
How to check the status of Forcepoint DLP Endpoint

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

Related topics:

- [How to disable Forcepoint DLP Endpoint, page 19](#)
- [How to confirm or block a policy violation, page 11](#)
- [How to view contained files and save them to an authorized location, page 16](#)
- [How to view logs, page 17](#)
- [How to update Forcepoint DLP Endpoint, page 18](#)

To view status information for Forcepoint DLP Endpoint, click the Forcepoint DLP Endpoint icon  on your task bar (Windows) or the Forcepoint DLP Endpoint icon  on your menu bar (Mac).



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.
- Determine if Forcepoint DLP Endpoint protection is enabled or bypassed.
- View discovery status and details of the last and next discovery scans.

Note that if your organization is using both Forcepoint Web Security Endpoint and Forcepoint DLP Endpoint, a Forcepoint Web Security Endpoint icon displays on your task bar as well. For more information about Forcepoint Web Security Endpoint, see [Forcepoint Web Security Endpoint](#), page 3.

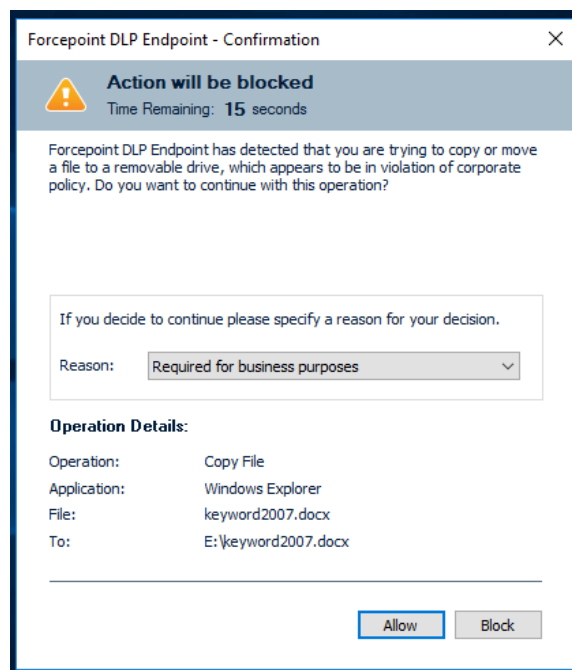
How to confirm or block a policy violation

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

Related topics:

- [How to check the status of Forcepoint DLP Endpoint, page 9](#)
- [How to update Forcepoint DLP Endpoint, page 18](#)
- [How to disable Forcepoint DLP Endpoint, page 19](#)

Occasionally, you might be asked to continue an operation that is known to be in violation of corporate policy. These violations are not automatically blocked by Forcepoint DLP Endpoint, and are allowed if you provide a valid explanation for the operation. If a policy violation is detected, Forcepoint DLP Endpoint displays a confirmation dialog window. From this confirmation dialog, you can choose to allow the operation to continue, you can block the operation and cancel the request, or you can block the operation and review the details in the log.



To continue with the action, select a **Reason** from the drop-down menu, and click **Allow**.

To cancel the action, click **Block** to close the window.

If the timer expires, the default action is taken. The default action is displayed above the timer. For example: **Action will be blocked** or **Action will be permitted**. The timer default is set to 30 seconds, but can be changed by your system administrator to between 9 and 58 seconds.

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 dialog window, 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 window, Forcepoint DLP Endpoint might incorrectly state that the files were copied or moved.
- Web Channel:
 - If you compose email through a web-based mail service (e.g., Gmail or Yahoo Mail), a confirmation dialog window displays whenever the service syncs to the hosting server (i.e., when the email is auto-saved). This causes the confirmation dialog window to display multiple times within a short timeframe.
 - Each sensitive attachment within an email triggers a separate confirmation dialog window.
 - 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.
- 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).
- 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 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 windows, because temporary files created by the application trigger the confirmation dialog.
- Email Channel:
 - In Outlook, the Outlook process is suspended when the confirmation dialog window displays. 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.

How to set encryption passwords

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

Related topics:

- [How to disable Forcepoint DLP Endpoint, page 19](#)
- [How to view contained files and save them to an authorized location, page 16](#)
- [How to view logs, page 17](#)
- [How to update Forcepoint DLP Endpoint, page 18](#)
- [Decrypting files on a removable media device, page 14](#)

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.

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.

To specify the encryption password:

1. Right-click the Forcepoint DLP Endpoint icon on your task bar, and select **Set Encryption Password**.
2. 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

3. Click **OK**.

Decrypting files on a removable media device

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

Related topics:

- [How to disable Forcepoint DLP Endpoint, page 19](#)
- [How to view contained files and save them to an authorized location, page 16](#)
- [How to view logs, page 17](#)
- [How to update Forcepoint DLP Endpoint, page 18](#)

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, however.)

The Forcepoint Decryption Utility is copied to your removable media device along with the encrypted files.

- [Decrypting files on Windows](#)
- [Decrypting files on Mac](#)

Decrypting files on Windows

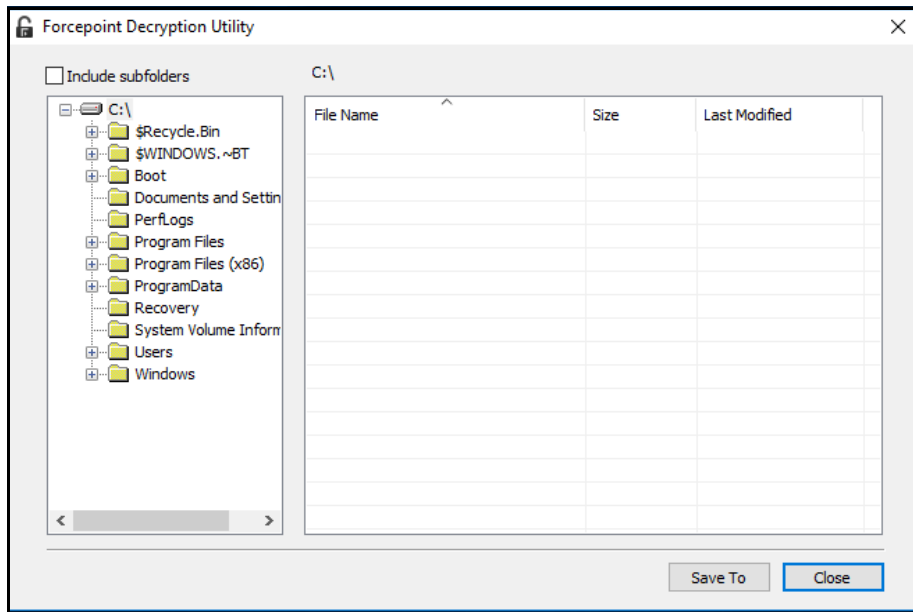
1. Insert the removable device into a Windows laptop or desktop.
2. Double-click **Forcepoint Decryption Utility.exe** or **wsdecrypt.exe**, depending on the Forcepoint DLP Endpoint version installed:
 - a. Forcepoint Decryption Utility.exe:
 - Decrypts files on a Windows endpoint machine that does not 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.
 - b. 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 Forcepoint DLP Endpoint 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.

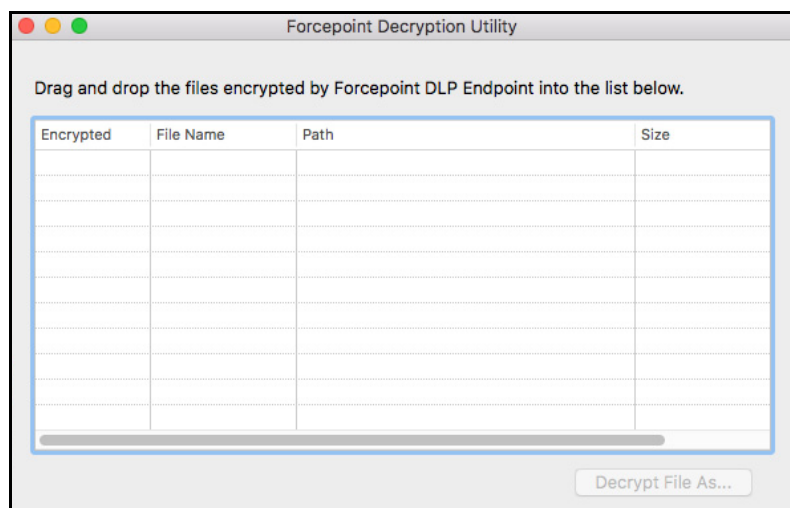
3. Enter the encryption password when prompted. A dialog appears and displays lists of subdirectories and files on your system.



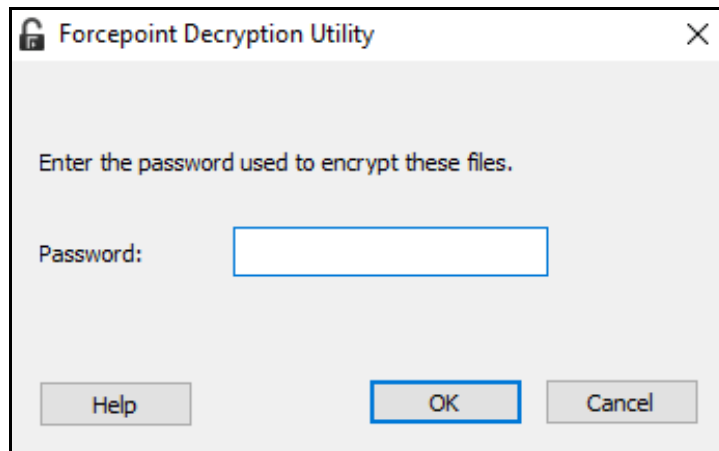
4. Navigate to the folder containing the encrypted files. By default, the files are on your removable media device.
5. Select the folders and files to decrypt, right-click, and select **Save To**.
6. Select the folder in which to save the decrypted files.

Decrypting files on Mac

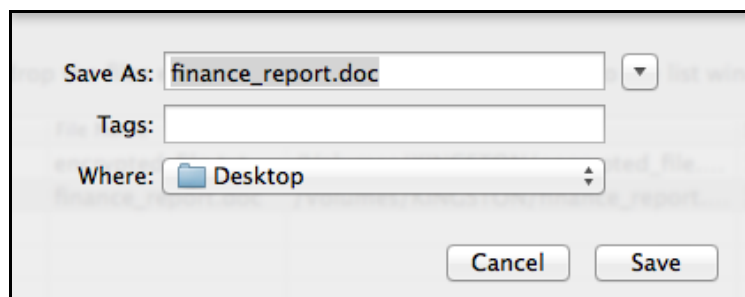
1. Insert the removable device into a Mac laptop or desktop.
2. Double-click **Forcepoint Decryption Utility.dmg** and mount it as a disk volume.
3. Launch the application **Forcepoint Decryption Utility** in the disk volume.
4. Drag and drop the encrypted files from the removable media device into the application's list window.



5. Select the file to decrypt, and select **Decrypt File As...**. If the file selected is not encrypted by Forcepoint DLP Endpoint, the operation is disabled.
6. Enter the encryption password when prompted. A file save dialog appears 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. No prompt appears as long as it 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.

How to view contained files and save them to an authorized location

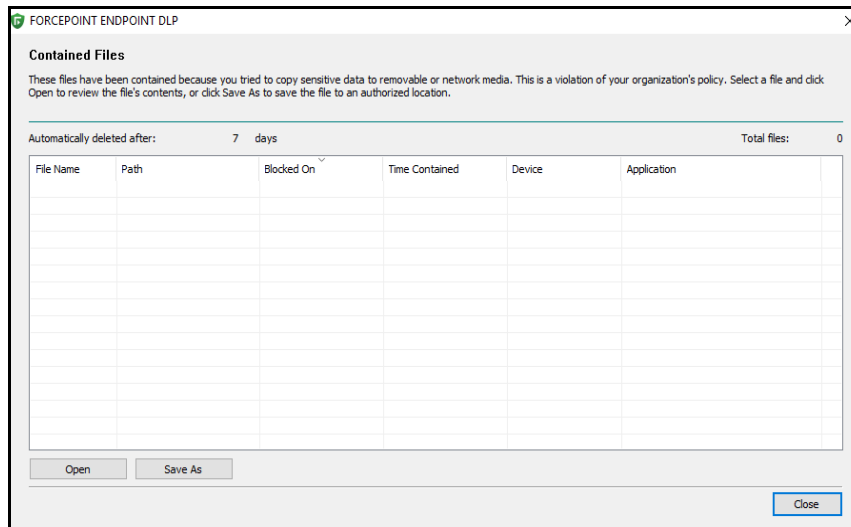
End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

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

Files are contained if your organization chose to prevent 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—and you try to copy a file to an unauthorized device. If the file has been modified, the contained file will include these modifications, while removing the modified file from the unauthorized device.

You can view the contents of contained files from the endpoint machine, 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**, then browse to the new location.
4. Click **Close** when done.

How to view logs

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

Related topics:

- [How to disable Forcepoint DLP Endpoint, page 19](#)
- [How to view contained files and save them to an authorized location, page 16](#)
- [How to view logs, page 17](#)
- [How to update Forcepoint DLP Endpoint, page 18](#)

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 computer 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

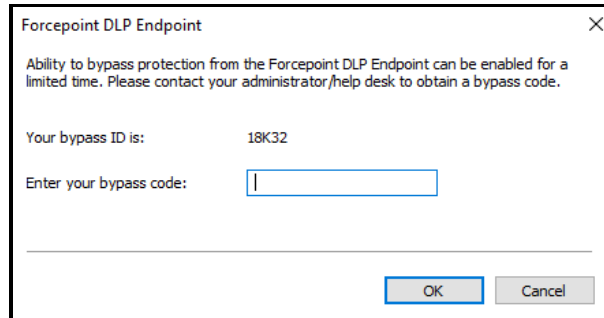
- To see the log details, on the Forcepoint DLP Endpoint screen, click **View Log**.

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



How to disable Forcepoint DLP Endpoint

End User's Guide | Forcepoint DLP Endpoint | On-Premises v8.5.x

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 **Enter**.

The Forcepoint DLP Endpoint software is disabled for the length of time specified when the bypass code was created. On Windows endpoint machines, the Disable icon  on the task bar updates to the Default icon  when the bypass protection expires. The icon does not change on Mac endpoint machines.

