Applications Monitored in the Endpoint Application Channel for Forcepoint DLP Endpoint

Endpoint Applications | Forcepoint DLP Endpoint | v8.4.x

You can monitor the operations performed by end users on any number of applications to prevent data loss from endpoint clients both on and off network—operations such as file access, cut or copy, and paste. Forcepoint has analyzed the metadata for more than a hundred applications, and has provided templates for these applications so you can monitor them in the Endpoint Application channel.

This document lists the predefined application templates by Application Group and lists the operating systems and operations that are monitored. While Forcepoint has analyzed the metadata for these applications, Forcepoint has not formally tested and certified these applications in all environments for each Forcepoint DLP Endpoint release. After selecting a specific application to monitor, test the application file access monitoring in your environment and reconfigure if needed.

This document also describes how to import user-defined applications if desired.

- *Built-in application templates*, page 1
- *Importing other applications*, page 11

Built-in application templates

Endpoint Applications | Forcepoint DLP Endpoint | v8.4.x

In the Forcepoint Security Manager, select **Main > Resources > Endpoint Applications** to choose the applications to monitor for the Endpoint Application channel, or select **Endpoint Application Groups** to select entire groups of applications, such as encryption software or browsers.

Following are the application templates that you can choose to monitor on the endpoint when you set up your endpoint policy in the Forcepoint Security Manager. This includes software applications, web applications, and cloud applications.

Also noted is whether the application is supported on Windows endpoints, Mac endpoints, or both, and the type of operations that can be analyzed by Forcepoint DLP.

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
Browsers	Chrome	✓	✓		Copy/Cut Paste File Access	Copy/Cut Paste
	Firefox	✓	✓			
	Internet Explorer (IE)	✓				
	Microsoft Edge	✓				
	Opera	✓	✓			
	Safari	✓	✓			
	Tor	✓				
	Torch	✓	✓			
CD Burners	Acoustica MP3 CD Burner	✓			Copy/Cut Paste File Access	Copy/Cut Paste File Access
	Alcohol 120%	✓				
	CD-Mate	✓				
	Disk Utility		✓			
	iTunes	✓	✓			
	Nero Burning ROM	✓				
	Roxio – Easy Media Creator	✓				
	Windows Media Player	✓				

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
Cloud Storage	Amazon Cloud Drive		✓		Copy/Cut Paste File Access	Copy/Cut Paste File Access
	Box	✓	✓	Box.com for Windows and Mac; Box store app for Windows		
	Dropbox	✓	✓	Dropbox store app		
	Egnyte	✓	✓		File Access Only	File Access Only
	Google Drive	✓	✓		Copy/Cut Paste File Access	Copy/Cut Paste File Access
	iCloud*	✓		iCloud Drive for both Windows and Mac	File Access	File Access
	OneDrive	✓	✓	OneDrive store app** for Windows	Copy/Cut Paste File Access	Copy/Cut Paste File Access
	Salesforce Files	✓	✓***			
	ShareFile	✓	✓			
	Syncplicity	✓	✓			
	WatchDox	✓	✓			

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
Email	Apple Mail		✓		Copy/Cut Paste File Access	Paste
	Eudora	✓		Eudora Light Eudora Pro		
	Lotus Notes	✓	✓			
	MailMate		✓			
	Microsoft Outlook	✓	✓			
	Microsoft Outlook Express	✓	✓			
	Mozilla Thunderbird	✓	✓			
	Pegasus Mail	✓				
	Postbox	✓	✓			
	Sparrow		✓			
	Windows Live Mail	✓				
	Windows Mail	✓				
Encryption Software	DK2 Network Server Remote Monitor - DK2 DESkey	✓			Copy/Cut Paste File Access	File Access
	File Encryption XP	✓				
	Windows Privacy Tray (WinPT)	✓				

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
FTP	Core FTP LE	✓			Copy/Cut Paste File Access	File Access
	Cute FTP Home 8.2	✓	✓			
	File Transfer Program (Microsoft Utility)	✓				
	FileZilla FTP Client	✓	✓			
	Flash FXP 3.6 build 1240	✓				
	FTP Voyager 15	✓				
	Ipswitch WS FTP Home	✓				
	Leech FTP	✓				
	Serv-U	✓		File Server EXE; File Server Tray Application; FTP Server Setup Utility		
	Smart FTP Client	✓				

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
IM and VOIP	Adium		✓		Copy/Cut Paste File Access	File Access Paste
	AIM	✓	✓			
	Apple Messages		✓			
	Camfrog	✓	✓			
	Cisco WebEx	✓	✓			
	GoToMeeting	✓	✓		Copy/Cut Paste	Copy/Cut Paste
	ICQ	✓	✓	ICQ store app (for Windows)	Copy/Cut Paste File Access	File Access Paste
	Jabber Messenger	✓				
	ManyCam	✓	✓			
	Microsoft Lync 2010	✓	✓			
	Miranda IM	✓				
	ooVoo	✓	✓			
	Pidgin	✓				
	Skype for Business	✓				
	TeamViewer	✓	✓			
	Teccent QQ	✓	✓			
	Trillian	✓	✓			
	Viber	✓	✓			
	Yahoo! Instant Messenger	✓	✓	Instant Messenger (Windows and Mac); YServer Module Server (Windows)		

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
Office Applications	Adobe Reader	✓	✓		Copy/Cut Paste File Access	Copy/Cut
	Bean		✓			
	Eclipse	✓	✓			
	Emacs	✓	✓*			
	Evernote	✓	✓			
	Keynote		✓			
	LibreOffice/ Apache OpenOffice	✓	✓			
	Mellel		✓			
	Microsoft Office Access	✓			Copy/Cut Paste File Access	
	Microsoft Office Excel	✓	✓			
	Microsoft Office InfoPath	✓				
	Microsoft OneNote	✓				
	Microsoft Office PowerPoint	✓	✓			
	Microsoft Office Project	✓				

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
Office Applications (Continued)	Microsoft Office Publisher	✓			Copy/Cut Paste File Access	Copy/Cut
	Microsoft Office Visio	✓				
	Microsoft Office Word	✓	✓			
	Notepad	✓				
	Numbers		✓			
	OpenOffice.org Calc	✓	✓			
	OpenOffice.org Draw	✓	✓			
	OpenOffice.org Math	✓	✓			
	OpenOffice.org Writer	✓	✓			
	Pages		✓			
	Reminders		✓			
	Stickies		✓			
	TextEdit		✓			
	WordPad	✓				
Online Medical (online)	AllegianceMD	✓			Copy/Cut Paste File Access Download	Copy/Cut Download
	eClinicalWorks	✓				
	ECLIPSYS	✓				
	INGENIX	✓				
	inteGreat	✓				
	Sequel	✓				

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
P2P	Ares	✓			Copy/Cut Paste File Access	File Access Paste
	Azureus	✓				
	BearShare	✓				
	BitComet	✓				
	BitLord	✓				
	BitTornado	✓				
	BitTorrent	✓				
	eMule	✓				
	FrostWire	✓				
	Kazaa Lite	✓		Kazaa download/ database viewer a - K-Dat; Kazaa QuickLinks Handler/ Generat - K-Sig; klrun: protocol - Kazaa Lite Extension		
	LimeWire	✓				
	Pando	✓				
	Transmission	✓	✓			
	uTorrent	✓	✓			
Packaging Software	7-Zip File Manager	✓			Copy/Cut Paste File Access	File Access
	iArchiver		✓			
	WinRAR	✓	✓			
	WinZip	✓	✓			

Group	Application	Windows	Mac	Includes	Monitored Operations	Default Operations
Portable Devices	Bluetooth Stack COM Server - BTStackServer	✓			Copy/Cut Paste File Access	File Access
	Fsquirt	✓				
	iTunes	✓	✓			
	Wireless Link File Transfer App – Irftp	✓				
	WCESMgr	✓	✓			
Cloud (SaaS)****	Aplicor (online)	✓			Copy/Cut Paste File Access Download	Copy/Cut Download
	CRM.com	✓				
	HostAnalytics	✓				
	Intacct	✓				
	NetSuite	✓				
	Oracle CRM on demand	✓				
	RightNow	✓				
	Salesforce	✓				
	WorkDay	✓				
None	FoxPro	✓			Copy/Cut Paste File Access	None
	Ld	✓				
	MSTSC	✓				
	NT backup tool	✓				
	Vista backup tool	✓				
	VMWare	✓				

*File Access only. The Copy, Cut, and Paste operations are not monitored.

Requires adding the applications **runtimebroker.exe, **bulkoperationhost.exe**, and **filemanager.exe** to the FTP application group. See the section on importing *Windows desktop applications* for instructions.

*** This application does not operate correctly on Mac 10.11.1, regardless of endpoint.

****The cut, copy, paste, file access, and download operations are not monitored for cloud apps on Windows endpoints when they are used through a Windows Store browser. Online application download is not supported in Firefox.

You can also configure the system to block and/or audit screen captures when a specific endpoint application is running. Navigate to the **Resources > Endpoint Applications** page and click on the application name to enable this feature.

Importing other applications

Endpoint Applications | Forcepoint DLP Endpoint | v8.4.x

If you want to monitor an endpoint application that is not not already provided as a template by Forcepoint, follow the instructions below. The instructions vary depending on the operating system, as well as the type of application.

- *Windows desktop applications*, page 11
- *Windows Store apps*, page 12
- *Mac Applications*, page 13

Windows desktop applications

The following applies to Windows applications prior to Windows 8, as well as Windows 8 desktop applications. For instructions on how to monitor Windows Store applications, see the section below, *Windows Store apps*.

There are 2 ways to import applications onto the Forcepoint DLP server for Windows desktop applications:

1. Selecting **Main > Resources > Applications > New Application/Online Application**. See Endpoint Applications.

   When you add applications using this screen, they are identified by their executable name. Occasionally, users try to get around being monitored by changing the executable name. For example, if you are monitoring “winword.exe” on users’ endpoint devices, they may change the executable name to “win-word.exe” to avoid being monitored.
2. Using an external utility program, **EPRegApps.exe**. This method records the application’s metadata, so that Forcepoint DLP can analyze the metadata.

   In other words, if the name of the application is modified by an end user, Forcepoint DLP Endpoint can still identify the application and apply policies.

Note

This tool can be copied to any other machine and be executed on it as long as it has connectivity to the Forcepoint Security Manager.

To use the external tool to import applications in the Forcepoint DLP server:

1. Go to [%DSS_Home%] directory (Default: C:\Program Files\Websense\Data Security Suite) and double-click **EPRegApps.exe**. The Get File Properties screen displays.
2. Complete the following fields:

Field	Description
IP Address/ Hostname	Insert the IP Address or Hostname of the Forcepoint DLP server.
User Name	Provide the user name used to access the Forcepoint DLP server. This is the user name assigned to administrators that have relevant permissions.
Password	Enter the password used to access the Forcepoint DLP server. This is the password assigned to administrators with relevant permissions
File Name	Insert the File Name of the application (e.g., Excel.exe) OR click the Browse... button and in the Open dialog box, navigate to the File Name of the application and double-click it.
Display Name	Enter the name of the application as you want it displayed in the Forcepoint Security Manager.

3. Click **OK**.

A message displays indicating that the application was successfully registered with the Forcepoint DLP server. The Get File Properties screen is then re-displayed with the Forcepoint DLP server fields completed, but the File Name and Display Name empty. This allows you to select additional applications to register with the Forcepoint DLP server. Continue this process until all applications are registered. When you are finished adding applications, click the **Cancel** button in the Get File Properties screen.

Windows Store apps

The following instructions apply only to Windows Store apps, and do not apply to Windows 8/8.1 desktop applications. For instructions on how to monitor Windows 8/8.1 desktop applications, see the section above, *Windows desktop applications*.

Note

To monitor file access on Windows 8 Store apps, you must first add **RuntimeBroker.exe** as an endpoint application, and monitor file access on this application. For Windows 8.1 store apps, you must also add **BulkOperationHost.exe** and **FileManager.exe**. The endpoint monitors all Windows Store apps accessing files through the runtime broker and not just the designated app. **RuntimeBroker.exe** is a Windows desktop application, so follow the instructions in *Windows desktop applications* to add this as an endpoint application.

To import Windows 8 Store apps, select **Main > Resources > Applications > New Application**. See Endpoint Applications.

Windows 8 Store app are identified by their application name. You should use this name in the executable name field on this screen. Wildcards are supported.

To identify the application name:

1. Open **PowerShell** (run as administrator if you want to collect Windows 8 Store apps for all users, or run as the current user if you want to collect apps for the current user).
2. Run the command "Get-AppXpackage -Allusers" to list apps for all users (requires you to run PowerShell as administrator).

   or

   Run the command "Get-AppXpackage" to list apps for the current user.
3. Find the application name located in either the **Name** field or **PackageFullName** field.
   a. When entering the value from the **Name** field into Forcepoint DLP, you must add the wildcard "*" after the application name (e.g., microsoft.microsoftonedrive*). This method allows for greater flexibility when the app version changes.
   b. When entering the value from the **PackageFullName** field into Forcepoint DLP, no wildcard is necessary, but you will need to update the value if the app version changes.

Mac Applications

To import Mac applications, select **Main > Resources > Applications > New Application**. See Endpoint Applications.

To find the value to enter for Mac applications:

1. Locate the application you want to monitor.
2. Right-click on the application and click **Show Package Contents**.
3. Open the file **info.plist** in the **Contents** folder.
4. Look for the key(s) **CFBundleName** and enter the value of the string(s) under it (e.g., for "<string>Example</string>" enter "Example").
5. If there is no key by that name, or no **info.plist** file, use the process(es) name(s).

If there are multiple **CFBundleName keys** and/or multiple string entries below the key(s), each string value must be added separately.

Very rarely, apps will launch other processes along with the main application. These processes should be added as endpoint applications as well. To know what processes belong to an app you need to see what processes are created when opening an application, for example by using **Activity Monitor**.