Data Security Endpoint Applications

Endpoint Applications | Data Security Solutions | Version 7.7.x

You can monitor any number of applications on the endpoint. Websense has analyzed the metadata for dozens of applications and can monitor these with great accuracy. (They are listed in this article.) You can add other applications to the list. If you want to analyze the applications based on their metadata, you can use a utility that Websense provides.

- ♦ Built-in support, page 1
- ◆ Importing other applications, page 8

Built-in support

Endpoint Applications | Data Security Solutions | Version 7.7.x

Following are the applications that you can choose to monitor on the endpoint when you set up your endpoint policy. This includes software applications, Web applications, and SaaS (software as a service) applications.

Also noted is whether the application is supported on Windows endpoint, Mac endpoint, or both, and the type of operations that can be analyzed by Data Security.

Mac Endpoint was introduced in v7.7.2. Please note that only File Access can be analyzed on Mac endpoint.

Group	Application	Windows	Мас	Supported Operations	Default Operations
Browsers	Chrome	✓	*	Copy/Cut	Copy/Cut Paste
	Firefox	Paste File Access		1 asic	
	Internet Explorer	1			
	Opera Internet Browser	1	/ *		
	Safari Web Browser	1	* **		

Group	Application	Windows	Мас	Supported Operations	Default Operations
CD Burners	Acoustica MP3 CD Burner	1		Copy/Cut Paste File Access	File Access
	Alcohol 120%	1		1 10 1 200000	
	Alcohol Launcher	1			
	CD Mate	1			
	Disk Utility		*		
	Nero Burning ROM	1			
	Roxio Creator Classic	1			
	iTunes	1	/ *		
Email	Apple Mail		/ *	Copy/Cut Paste	Paste
	Eudora	1		File Access	
	Eudora Light	1			
	Eudora Pro	1			
	Lotus Notes	1			
	Microsoft Outlook 2003, 2007, 2010	4	*		
	Microsoft Outlook Mobile Manager 2003, 2007, 2010	4	/ *		
	Mozilla Thunderbird	4			
	Outlook Express	1			
	Pegasus Mail for Windows	1			
	Pegasus Mail WSENDTO Utility	1			
	Windows Mail	1			

Group	Application	Windows	Mac	Supported Operations	Default Operations
Encryption Software	DK2 Network Server Remote Monito - DK2 DESkey	1		Copy/Cut Paste File Access	File Access
	File Encryption XP	1			
	Windows Privacy Tray (WinPT)	1			
FTP	Core FTP App	1		Copy/Cut Paste	File Access
	CuteFTP File Transfer Application	1		File Access	
	Dropbox	1	*		
	FileZilla FTP Client	1	*		
	FlashFXP	1			
	FTP Voyager®	1			
	LeechFTP	1			
	Serv-U File Server EXE	1			
	Serv-U File Server Tray Application	1			
	Serv-U FTP Server Setup Utility	1			
	SmartFTP Client	1			
	WS_FTP Pro Application - WS_FTP Professional	1			

Group	Application	Windows	Мас	Supported Operations	Default Operations
IM	Adium		*	Copy/Cut Paste	File Access Paste
	AOL Instant Messenger	1		File Access	Taste
	Google Talk	1			
	iChat		*		
	ICQ Library	1			
	ICQLite	1			
	Jabber Messenger	1			
	Messenger	1			
	Microsoft Communicator 2007	1			
	Microsoft Communicator 2010	1			
	Microsoft Lync 2007	1			
	Microsoft Lync 2010	1			
	MXit PC v1.2	1			
	Office Communicator 2005	4			
	QQ	1	*		
	Skype	1	*		
	Windows Live Messenger	1			
	Windows Messenger	1			
	Yahoo! Messenger	1			
	YServer Module - Yahoo! Messenger	1			

Group	Application	Windows	Мас	Supported Operations	Default Operations
Office Applications	Adobe Reader 8.1	1		Copy/Cut Paste	Copy/Cut
	Microsoft Access 2003, 2007, 2010	1		File Access	
	Microsoft Excel 2003, 2007, 2010	1	*		
	Microsoft InfoPath 2007, 2010	1			
	Microsoft OneNote 2003, 2007, 2010	1			
	Microsoft PowerPoint 2003, 2007, 2010	1	*		
	Microsoft Project 2003, 2007, 2010	1			
	Microsoft Publisher 2003, 2007, 2010	1			
	Microsoft Visio 2003	1			
	Microsoft Visio 2007, 2010	1			
	Microsoft Word 2003, 2007, 2010	1	*		
	Notepad	1			
	OpenOffice.or g Suite	4	*		
	Stickies		*		
	TextEdit		*		
	WordPad	4			

Group	Application	Windows	Мас	Supported Operations	Default Operations
Online Medical (online)	AllegianceMD	1		Copy/Cut Paste	Copy/Cut Download
	eClinicalWork s	√		File Access	
	ECLIPSYS	1		—— Download	
	INGENIX	1			
	inteGreat	4			
	Sequel	4			
P2P	Ares p2p for windows	1		Copy/Cut Paste	File Access Paste
	Azureus	1		File Access	
	BearShare	1			
	BitComet	1			
	BitLord	1			
	BitTornado	1			
	Bittorrent	4			
	eMule - eMule	4			
	FrostWire	1			
	Kazaa download/ database viewer a - K- Dat	~			
	Kazaa QuickLinks Handler/ Generat - K- Sig	✓			
	klrun: protocol - Kazaa Lite Extensions	1			
	LimeWire	1			
	pando	1			
	Transmission		/ *		
	uTorrent	1	√ **		

Group	Application	Windows	Мас	Supported Operations	Default Operations
Packaging Software	7-Zip File Manager	4		Copy/Cut Paste	File Access
	iArchiver		/ *	File Access	
	WinRAR archiver	4			
	WinZip	4			
Portable Devices	Bluetooth Stack COM Server - BTStackServe r	~		Copy/Cut Paste File Access	File Access
	Fsquirt	4			
	iTunes	1	*		
	Wireless Link File Transfer App - Irftp	1			
SaaS (online)	Aplicor	4		Copy/Cut	Copy/Cut Download
	CRM.com	1		Paste File Access	
	HostAnalytics	1		Download	
	Intacct	1			
	NetSuite	1			
	Oracle CRM on demand	4			
	outlook.com	4			
	RightNow	4			
	Sales-Force	1			
	WorkDay	1			

Group	Application	Windows	Mac	Supported Operations	Default Operations
None	FoxPro	1		Copy/Cut Paste	None
	LD	4		File Access	
	MSTSC	4			
	NT Backup Tool	1			
	Vista Backup Tool	1			
	VMWare	1			

^{*}Starting in v7.7.2. **Note**: Mac Endpoint only analyzes the File Access operation

You can also configure Data Security 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. This feature is only supported on Windows operating systems.

Importing other applications

Endpoint Applications | Data Security Solutions | Version 7.7.x

If you want to monitor an endpoint application other than the ones supplied by Websense, follow the instructions below. The instructions vary depending on the operating system, as well as the type of application.

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 8 Store apps*.

There are 2 ways to import applications onto the Data Security 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're monitoring "winword.exe" on users' endpoint devices, they may change the executable name to "winword.exe" to avoid being monitored.

^{**}Starting in v7.7.3 **Note**: Mac Endpoint only analyzes the File Access operation

2. Using an external utility program, **DSSRegApps.exe**. This method records the application's metadata, so that Websense Data Security can analyze the metadata.

In other words, if the name of the application is modified by an end users, Websense Data 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 Data Security Management Server.

To use the external tool to import applications in the Data Security server:

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

Field	Description
IP Address/ Hostname	Insert the IP Address or Hostname of the Data Security Server.
User Name	Provide the user name used to access the Data Security Server. This is the user name assigned to administrators that have relevant permissions.
Password	Enter the Password used to access the Data Security 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 Data Security Management Server.

3. Click OK.

A message will appear indicating that the application was successfully registered with the Data Security Server. The Get File Properties screen will be re-displayed with the Data Security Server fields completed, but the File Name and Display Name empty. This allows you to select additional applications to register with the Data Security 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 8 Store apps

Starting in Data endpoint v7.7.3.1629, you can import Windows 8 Store apps into your Endpoint Applications list. The following instructions do not apply to Windows 8 desktop applications. For instructions on how to monitor Windows desktop

applications, see the section above, Windows Desktop Applications.

Note: In order 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. However, 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 <u>Endpoint Applications</u>.

Windows 8 Store applications 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 Data Security, you must add the wildcard "*" after the application name (e.g. microsoft.microsoftskydrive*). This method allows for greater flexibility when the app version changes.
 - b. When entering the value from the **PackageFullName** field into Data Security, 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 <u>Endpoint Applications</u>.

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. In order 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.