Digital Guardian Agent for Windows Release Notes

Copyrights and Trademarks

Corporate Headquarters

Digital Guardian
275 Wyman St., Suite 250
Waltham, MA 02451-1414
Tel: 781 788-8180
Fax: 781 788-8188

www.digitalguardian.com

Trademarks

Patents

Digital Guardian products are protected by one or more patents. Contact Digital Guardian, Inc. for more information.

Contents

Chapter 1

Introduction

This document describes new features and resolved and known issues in the current Digital Guardian Agent for Windows. It also includes important issues affecting the DG Agent for Windows and provides workarounds, where appropriate. Finally, it provides information about software that is no longer supported.

A tracking number accompanies most items. For more information about an item, contact your Digital Guardian Account Representative and refer to the tracking number.

Chapter 2

New Features

These are the new features and enhancements in the last three releases.

DG Agent 7.6.4

Digital Guardian Agent 7.6.4 for Windows supports the latest versions of the following Boldon James user classification software, including

- Email & Office Classifier v3.16.3
- File Classifier v3.16.0
- Classifier Administration Server (CAS) v3.17.0

DG Agent 7.6.3

This release contains no new features.

DG Agent 7.6.2

The Agent for Windows 7.6.2 supports the enhancements described in this section.

Upgrade of Micro Focus Autonomy

The DG Agent 7.6.2 versions of Micro Focus Keyview Filter SDK and Autonomy Eduction Engine SDK have been upgraded to version 12.6.

These components are required for using the DG Adaptive Content Inspection (ACI) feature. The version 12.6 content inspection SDKs are installed by default with DG Agent 7.6.2 for Windows.

DG Agent 7.6.2 for Windows continues to support the 41 DG built-in ACI entities listed on the DGMC Manage Classification - Adaptive Inspection Resources page (Policies > Content Patterns > ACI Resources).

Micro Focus Autonomy documentation is provided with DG Server 8.3 in the Third Party Documentation folder.

Enhancement to DG Rule Engine

DG has enhanced the DG rule engine to allow it to trigger on a nonexistent custom document property.

Previously, the rule engine did not allow the following comparison to be made if the file did not have the custom document property:

```
<equal>
<evtSrcDocPropertyString name="msip_label_4a0952fd-98af-4a15-bbfa-
b9106ff391ff_name"/>
<string value=""/>
</equal>
```

The new behavior effectively allows customers to test whether a document property is present or not. As shown in the example above, the string will have an empty value if the document property is not present.

> **Caution:** This feature applies only to files that have other document properties. It does not apply to files that do not have document properties, such as text files and source code.

The use of the <not> operator invalidates the result of the comparison, which means that the immediate result is ignored.

```
<not>
<equal>
<evtSrcDocPropertyString name="msip_label_4a0952fd-98af-4a15-bbfa-
b9106ff391ff_name"/>
<string value=""/>
</equal>
</not>
```

To use this feature, enable the treatAbsentDocPropAsEmptyString setting in the Agent config.xml file, as shown. The default is off (0).

```
<treatAbsentDocPropAsEmptyString>1</treatAbsentDocPropAsEmptyString>
```

Chapter 3

Important Notes

This section describes important issues affecting the DG Agent for Windows and provides workarounds, where appropriate.

Clear Browser Cache if NTDs Are Not Being Blocked

If Network Transfer Downloads (NTDs) are not being blocked on versions of Google Chrome or Microsoft Edge that use the HTTP3 network protocol, you will need to clear the browser cache. This will resolve the issue. (AG-40446)

Always Configure DG WIP From the DGMC

If you are using DGMC 7.5 or later, always use the DGMC and not the MSI Tool to make configuration changes to the DG web inspection proxy (WIP), such as applying a custom root certificate. If you make configuration changes with the MSI Tool, they might be overwritten by the DGMC later on. (SA-36974)

Firefox Cache Corruption Issue

In environments using the DG Agent for Windows and the DG web inspection proxy (WIP), attempts to access a website that requires a secure (https) connection to secure communication with your Agent computer through Firefox might fail due to corruption of the Firefox certificate store. When you enter the website URL in the Firefox browser, Firefox displays a Secure Connection Failed error page.

If the website connection problem occurs only with the Firefox browser, click the "Learn More..." link on the error page for solutions. (SA-36314)

New Certificate Generated From a Replacement Root Certificate Template Not Active Until Next Agent Reboot

DG provides a default root certificate template (template.pem) that is used to create a root certificate that DG writes into the Windows certificate store to allow browsers supported with the web inspection proxy (WIP) to trust the server certificates signed by DG.

Whenever the Agent receives a new template.pem file — for example, if you overwrite the current default WIP root certificate template with a custom root certificate template — a new root certificate generated from the replacement template does not become active until after the next Agent computer reboot has completed. DG made this change to properly support certain browsers. (SA-27965)

NTUs Not Detected for Files With Zero Bytes

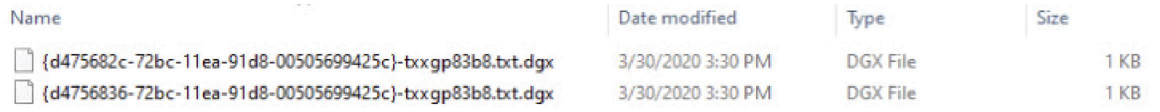
The DG web inspection proxy (WIP) does not detect network transfer uploads (NTUs) for files with zero bytes. No NTU event is shown for such files in the local forensics report. The file type does not matter. This limitation occurs if WIP is enabled for any browser supported by DG. (SA-34172)

Multiple Uploads of Files Captured to SMB Storage

Under some circumstances, multiple uploads of a file captured to SMB storage (an SMB network share) will occur on what may appear to be only one event. This behavior is typically due to file capture occurring when a file operation (copy, move, delete, or network transfer upload) is blocked, because the program performing the action that triggers file capture may automatically retry the action several times, triggering an upload to your SMB network share each time. In some cases, this might affect your disk space, depending on how large the file being captured is and how many duplicates occur.

This issue may not require remediation, because you will already be taking actions to maintain the size of the uploaded files over time (for example, deleting files older than a specific number of days). This should be sufficient to maintain acceptable size limits, even with this issue.

If remediation is required, you will need to perform a manual or scripted cleanup task to remove duplicate captured files. In your SMB network share, look for multiple files with the same original filename, the same size, and datetimes created within a few seconds of one another. (SA-35651)



Name	Date modified	Type	Size
{d475682c-72bc-11ea-91d8-00505699425c}-txxgp83b8.txt.dgx	3/30/2020 3:30 PM	DGX File	1 KB
{d4756836-72bc-11ea-91d8-00505699425c}-txxgp83b8.txt.dgx	3/30/2020 3:30 PM	DGX File	1 KB

Browser Upload Retries May Result in Multiple Prompts

On blocked uploads some websites — including Google Drive, Gmail, and others — retry uploading the files. Depending on the site, the retry continues until the browser is restarted or the tab is closed. For every browser upload retry, a new event is generated in the Local Forensic Report. Depending on the rule caching policy, this might result in multiple prompts. If the user sees a prompt for the site they have already denied, they should restart the browser. (SA-29415)

Custom Document Properties

You can create custom document properties for Microsoft Office documents. For information about creating and editing these properties, view Microsoft help for the Office product you are working with.

You can also create custom document properties for PDF documents using an application such as Adobe Acrobat (paid version) to apply new tags to the PDF file. These new tags are stored within the PDF file's custom document properties section.

1. In Adobe Acrobat, select **File > Properties**.
2. In the Document Properties dialog box, select the **Custom** tab. Enter a unique name and value. For example, the unique name might be "DGTAG" and the value to be stored against that tag might be "pi_data".

Once you have created the tags in the PDF file, you can create new DG control rules that look for the specific tag name and then perform various actions based on the associated tag value.

The DG Agent uses the Adaptive Content Inspection (ACI) KeyView engine to read the custom properties contained within a PDF file. To make the KeyView engine aware of which custom document property tags it is allowed to read, you need to manually edit the pdfsr.ini configuration file:

<DGAgentInstallFolder>/Verity/kv/_nti40/bin/pdfsr.ini

By default, the DG Agent installation folder is installed in C:\Program Files\DGAgent\

> **Note:** Before you can edit the pdfsr.ini file, you must first terminate the Agent. After editing the file, restart the Agent.

The default pdfsr.ini file has the following content:

```
#Customer can use this file to set up some customized data such as customized
metadata tags.
#The format of metadata is: 1. <TOTAL> total_item_number </TOTAL>
#                           2. Content: tag_name datatype
# Datatype includes: STRING, INT4, DATETIME, CLIPBOARD, BOOL, UNICODE, IEEE8
   and OTHER.
# DATETIME use YYYYMMDD format
<META>
<TOTAL> 2 </TOTAL>
/bjLabelRefreshRequired UNICODE
/bjDocumentLabelXML UNICODE
</META>
```

You need to make two edits to this configuration file (and repeat the process for each tag to be read).

1. Increment the value on the `<TOTAL> total_item_number </TOTAL>` line by one for each tag being applied.

2. Add a new line defining the new tag to be read and the data type to be used to read the tag's value field.

3. Save your changes.

Example:

The following example shows the configuration file after adding the example tag, DGTAG.

- UNICODE in the example represents the data type of the tags value field.
- The data type should match the type used by Adobe Acrobat.
- Allowable data type values: (STRING, INT4, DATETIME, CLIPBOARD, BOOL, UNICODE, IEEE8 and OTHER).

```
#Customer can use this file to set up some customized data such as customized
metadata tags.
#The format of metadata is: 1. <TOTAL> total_item_number </TOTAL>
#                           2. Content: tag_name datatype
# Datatype includes: STRING, INT4, DATETIME, CLIPBOARD, BOOL, UNICODE, IEEE8
   and OTHER.
# DATETIME use YYYYMMDD format
<META>
<TOTAL> 3 </TOTAL>
/bjLabelRefreshRequired UNICODE
/bjDocumentLabelXML UNICODE
/DGTAG UNICODE
</META>
```

Digital Guardian can enforce rules and record events based on custom document properties, as described in "Using Document Properties in Rules" in *Digital Guardian Rule Implementation Guide*. If you have a document where a custom property shares the same name as a default property, Digital Guardian uses the value of the default document property and ignores the value of the custom property.

Clipboard Read Request by Firefox or Chrome When User Right-Clicks Bookmark May Cause DG to Trigger Classification Rule

If you have a classification rule to detect clipboard activity against Mozilla Firefox or Google Chrome and respond with a prompt, and a user copies classified text to the Windows clipboard, opens the browser and right-clicks a bookmark, your rule will trigger and the user will see a justification prompt. This happens because the browser makes an unnecessary clipboard read request when the user right-clicks the bookmark. In response, DG correctly detects a read of classified data from the clipboard by the browser and triggers the classification rule. Users who are prompted should respond to the prompt and then click the bookmark. (SA-31846)

Adding Process Flags for ChromeDriver

Webdriver for Chrome is an automated test tool that contains the ChromeDriver server (chromedriver.exe). If you are using ChromeDriver and the chromedriver.exe process crashes, add the following entry to your process flags file:

chromedriver.exe, SK + NI

Length Restriction on Component List and Feed List Names

When you create component lists or feed lists in the DGMC, DG now restricts the number of characters allowed in the list name. The names of component lists are limited to 64 characters and the names of feed lists to 50 characters. This ensures that the character limits allowed by the DG Server are consistent with the limits allowed by the DG Agent.

The same restrictions apply to importing XML files containing component lists or feed lists. If the name of the component list within the XML import file is longer than 64 characters, the DGMC will import the list, but the DG Agent will not download it. If the name of the feed list within the XML import file exceeds 50 characters, the DGMC will not import the list. (SA-30415)

File Open Block Events LFR Returns Different Information for Office 2016 32-Bit on Windows 10 V1809, Build 253

After applying a Justification rule with a silent Block action for File Open events to an Agent computer and upgrading Microsoft Windows 10 v1809 to Build 253, when you open a Microsoft Office 2016 file and then run the Local Forensic Report (LFR) for File Open Block events, you will see different information, depending on whether you are running Office 2016 32-bit or Office 2016 64-bit and whether your rule uses a wide policy pattern or a more specific policy pattern. If you wrote the rule with a wide policy pattern, the Local Forensic Report for an Office 2016 32-bit file displays the folder name and the path to the folder name, whereas with Office 2016 64-bit, the Local Forensic Report displays the file name and source file path.

If you want the Local Forensic Report to return a file name instead of a folder name for a file opened with Office 2016 32-bit, create a rule with a very specific policy pattern, for example:

```
<and>
 <regExp expr="open_block\\.+">
  <evtSrcFilePath />
 </regExp>
 <equal>
  <evtOperationType />
  <constOpFileOpen />
 </equal>
</and>
```

(SA-30321)

IPv6 Address Format Not Supported

DG does not support using IPv6 (version 6 of the Internet Protocol) on Agent computers. Only IPv4 is supported.

Using Justification Prompts With NTUs

Before using justification prompts with Network Transfer Download (NTU) operations involving classified files, make sure to test the prompts with the websites you plan to use them with. In some cases, sites might time out while the prompt is active and display a message or dialog box indicating that the page has been unresponsive. If this happens, the user should wait for the page to become active again. The file will upload as expected after the delay. This issue can occur on all versions of the Chrome browser supported by DG.

Discontinued Support for AFE and AME

Effective with the DG 7.5 release, DG no longer sells or supports the Adaptive File Encryption and Adaptive Mail Encryption modules. DG continues to support other encryption options, including Removable Media Encryption (RME) and its variations: Portable Encryption and CD/DVD Encryption.

If you have been using AFE or AME, before upgrading to DG Server 7.5 you should uninstall all pre-7.5 DG Agents that have AFE or AME applied. As part of uninstalling your Agents, select Scan on Uninstall. This will allow the uninstall operation to decrypt all encrypted files. After uninstalling your pre-7.5 DG Agents, you can upgrade to DG Server 7.5 and install 7.5 DG Agents.

If you applied AFE and AME to pre-7.5 Agents, and you upgrade to DG Server 7.5 with valid AFE and AME licenses, you can continue to use AFE and AME, but you can no longer create custom reports using Machine Configuration fields for AFE and AME (Has Adaptive File Encryption and Has Adaptive Mail Encryption). Those fields will not be shown in the Custom Report Wizard.

For information on encryption solutions supported with DG 7.5, refer to “Removable Media Encryption” in the *Digital Guardian Management Console User’s Guide*. RME encryption features are included with the DG product and do not require a license.

Agent Install Cannot Complete With Windows 10 Fast Startup Enabled and Shut down Selected

If Windows 10 Fast Startup is enabled and you select the Shut down (not Restart) option after an Agent install or upgrade, the Agent installation does not complete. For fresh installations, the DGMC Computers page shows "New Agent Needs Reboot" status. For upgrades, the Computers page shows "Upgrade Pending Agent" status.

To complete the Agent install or upgrade, restart the Agent machines using the Windows 10 Restart option.

If you do not need to run your Agent-equipped machines in Fast Startup mode, disabling Fast Startup will allow the install or upgrade to complete. (SA-31967)

Upgrading Agents and Servers To Report User Logon Failed Events

To report User Logon Failed events, DG Agents and DG Servers must be running DG 7.5 and later. If you upgrade your DG Agents to 7.5 or later before you upgrade your servers to 7.5 or later, you will most likely need to reboot your Agent computers to start reporting User Logon Failed events. Rebooting your Agents forces them to register with the Server. Registration enables the new User Logon Failed reporting.

To report User Logon Failed events, you also need to configure the Windows Local Group Policy Object to audit logon attempts on Agent computers. To learn more about configuring DG Agents to report failed logon attempts by users, locate the constOpLogonFailed operation type constant in the “Symbolic Constants” chapter of *Digital Guardian Rule Implementation Guide*.

IoBlockLegacyFsFilters Registry Key Setting

The registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\I/O System\IoBlockLegacyFsFilters must either be set to 0 or not be set (the value is not present). Setting the value to 1 will prevent the DG Agent from functioning properly. (SA-27407)

Enabling Transfer of Diagnostic Artifacts

If you are running a DG release prior to DG 7.3.1 and encounter issues transferring diagnostic artifacts from the DG Agent to the DG Server, it is recommended that you upgrade your Server and your Agent computers to DG 7.3.1 or later to resolve the problems.

Installing User Classification With Microsoft Windows Device Guard

To allow installation of the User Classification (UC) feature in environments with an enforced Windows 10 Device Guard policy in place, you must first use the Microsoft Package Inspector tool (packageInspector.exe) to create a catalog file and integrate it into your Device Guard policy.

Before you begin, set up UC as described in “User Classification” in the *Digital Guardian Management Console User’s Guide*, but do not enable UC on your Agent computers. You will start the Package Inspector on an Agent computer and enable UC on that computer when the Package Inspector is running.

The following procedure provides basic instructions for installing UC on Agent computers that have an enforced Device Guard policy applied. For complete details on using Package Inspector, see Microsoft’s documentation.

1. Apply a Device Guard policy in Audit mode to an Agent-equipped computer. Do not enable the User Classification feature on the Agent computer.

2. Start packageinspector.exe on the Agent computer to which you applied the policy.

3. From the DGMC, enable the User Classification feature on the Agent computer where the Package Inspector is running. When the Upgrade Pending icon ⟲ is displayed, restart the Agent computer.

4. Stop packageinspector.exe.

5. Create a new Device Guard policy from the audit results.

6. Sign the catalog file that was created by packageinspector.exe and add a rule to the audit policy allowing files signed by that certificate.
7. Distribute the catalog file to your Agent computers.
8. Merge the audit policy into your existing Device Guard policies.

DG Scanner Disabled by Default

When you install or upgrade DG Agents to version 7.4 or later, DG Scanner is now disabled by default when the DG Agent starts. The scanner will not perform data-at-rest scans, or classification and encryption scans for data in motion, on any drives. This change ensures that the scanner runs only after you configure it in the DGMC to scan fixed, removable or mapped drives. Selecting any drive and setting a schedule enables the scanner.

In this new default state, the Agent reports an error in the DG log:

```
*ERROR* 00001104 00001188 2017/03/08 15:12:26:546 - CScannerClient::SCStartScannerService:
Service=dgscan Func=StartService error=1058, The service cannot be started, either because it is
disabled or because it has no enabled devices associated with it.

*ERROR* 00001104 00001188 2017/03/08 15:12:26:546 - [CScannerClient::BeginScanner] Could not
start DGScanner service
```

For details about configuring the scanner, refer to "Scanner Settings" in *Digital Guardian Installation and Upgrade Guide*. (SA-19724)

Limitations on Detecting NTU/NTD Events on Websites That Use a Second Level of Encryption

Digital Guardian is not able to detect Network transfer upload and download events on websites that use a second level of encryption in addition to HTTPS. For example, DG cannot detect NTU and NTD events on websites using MTProto Mobile Protocol, where the data is first encrypted between a client, such as a web browser using HTTPS, and then encrypted again by a web server.

Java-Based Uploads Not Supported

Digital Guardian does not support Java-based uploads and downloads due to their advanced functionality, such as uploading multiple files and folders, and uploading using drag and drop.

Propagating UC Information to Microsoft Office Documents Exported as PDF

If you want to propagate user classification information to a Microsoft Office document when the document is saved or exported as a PDF document, you need to add a document property to your Classifier configuration and make a change to the Label Configurations settings file (settings.xml). For detailed instructions, refer to "Propagating UC Information to Microsoft Office Documents Exported as PDF Files" in the *Digital Guardian Management Console User's Guide*.

Limitation on Extracting Document Properties

The DG Agent cannot properly extract document properties whose values are in a different language from that of the Windows OS. This limitation applies to Microsoft Office documents saved in the older binary file format (.doc, .xls, .ppt). Documents saved using the newer Open XML file format are not affected. (SA-27245)

Content Inspection Engine Compatibility

When you install or upgrade DG Agents to DG 7.2 or later and you use Adaptive Content Inspection (ACI), you must upgrade the Autonomy content inspection engine as well. Do not apply the new Autonomy inspection engine to earlier DG Agent versions. ACI with the new inspection engine will not work properly with pre-7.2 Agents.

Microsoft Windows Upgrades With a DG Agent Installed

Before performing a Windows upgrade to any version of Windows 10 on a computer with a DG Agent installed, upgrade the DG Agent to the latest version. After you upgrade the DG Agent and it is reporting to the DG Server, apply the latest version of the process flags file (prcsflags.dat) to the DG Agent and merge your custom process flags with this file.

When you complete those tasks, review and follow the Microsoft guidelines regarding third party/OEM software running on your previous version of Windows.

Now you are ready to upgrade Windows.

Following this upgrade process prevents you from ending up with an unsupported DG configuration.

Note: If you have Adaptive File Encryption (AFE) enabled, disable it before upgrading the operating system. You may re-enable it after the upgrade is complete.

Installing Symantec Endpoint Protection 12.1.6 or Later

Digital Guardian has removed the `setup.exe,NI+NC+ND` process flag from the default process flags file due to a change in the recommended order of installation of the Symantec package and installation of the DG Agent.

To install Symantec Endpoint Protection 12.1.6 or later, you must do the following:

1. Add the `setup.exe,NI+NC+ND` process flag to the process flags file and save the file. This will allow the Symantec setup.exe file to unpack itself and run.

2. When the installation is complete, remove `setup.exe,NI+NC+ND` from the process flags file and save the file.

Content Classification of Microsoft Word Documents With ACI

To ensure that Close, Open and Save As operations cause Adaptive Content Inspection (ACI) to perform inspections on Microsoft Word .doc and .docx files, set aciProcessDestFileForContent to 1 in the configuration file on your Agents. Add the following syntax to config.xml:

```
<aciProcessDestFileForContent>1</aciProcessDestFileForContent>
```

Using Stealth Mode With Microsoft Windows

To allow stealth mode to work with DG Agents, do not use the SK (Skipped) and TR (Trusted) process flags on the process explorer.exe.

Also, to maintain stealth, do not apply the NI (No Inject) flag to Windows Task Manager (taskmgr.exe).

Configuration Element for IBM Notes

To prevent DG Agents from encrypting mail attachments more than once when you use AME with IBM Notes (formerly IBM Lotus Notes), add the following configuration entry to config.xml:

```
<ameDisableUpdateBodyWithTicketInfo>1</ameDisableUpdateBodyWithTicketInfo>
```

This configuration directs the DG Agent not to append the DG ticket information to the body of the email.

Workaround To Load DG Outlook Plug-In Automatically

If the DG Outlook plug-in is disabled, DG will not be able to monitor or block Send Mail or Attach Mail operations.

To load the DG Outlook plug-in automatically, use the following procedure in the DGMC to set the required Windows registry settings. Alternatively, you can use Group Policy (GPO) or a batch script. (SA-9605)

1. Select **System > Resources.**
2. In the left pane, click **Custom Configuration**.
3. From the ☰▾ menu, select **Create Configuration Resource**. Alternatively, you can edit an existing Custom Configuration resource.
4. For a new configuration resource, enter a resource name and description.
5. Under Custom Configuration File, add the following two entries between the <appSettings> and </appSettings> tags:

```
<appSettings>
<MAPISMIMEAME pushDuringUpdate="1" regHive="HKLM"
regKey="SOFTWARE\Wow6432Node\Microsoft\Office\Outlook\Addins\MAPISMIMEAMEP
rocessor.EventCallbacks" regName="LoadBehavior"
regType="DWOR">3</MAPISMIMEAME>

<MAPISMIMEAME2 pushDuringUpdate="1" regHive="HKLM"
regKey="SOFTWARE\Microsoft\Office\Outlook\Addins\MAPISMIMEAMEProcessor.Eve
ntCallbacks" regName="LoadBehavior" regType="DWOR">3</MAPISMIMEAME2>
</appSettings>
```

6. Click 💾.
7. Assign the Custom Configuration resource to dynamic groups (**System > Dynamic Groups**).

Note: You might need to adjust the Priority Rank if Agent computers belong to multiple dynamic groups and the Custom Configuration Resource file is assigned to multiple dynamic groups.

8. Run a Dynamic Group Sync job (**System > Job Scheduler > Dynamic Group Sync**) and allow the Agent computers to pick up the settings. This might take 30 minutes (default).

9. Restart the Agent computers.

Chapter 4

Resource File Changes

The following changes were made to resource files in the last three DG Agent releases.

DG Agent 7.6.4

The Agent config.xml file and the Directory Control File (DirCtrl.dat) were updated in DG Agent 7.6.4.

Agent Configuration File Changes

The following new config.xml setting is available.

Setting: <aciEnableSoftHyphenFiltering>1</aciEnableSoftHyphenFiltering>

Default Value: 1

Valid Values: 1 - Enabled, 0 - Disabled

In Registry? No

Description:

If a classification rule contains a content pattern with a trailing soft (visible) hyphen (-) character, such as -Highly Confidential- (no spaces), the content inspection engine filters out the trailing soft hyphen when inspecting content patterns in files converted to PDF. This causes the classification rule to fail because the data pattern will never match the rule. No such filtering occurs with other file types. To ensure that a classification rule succeeds when the content pattern contains a trailing soft hyphen, you can create a custom configuration resource in the DGMC, making sure aciEnableSoftHyphenFiltering is enabled (1). Alternatively, you can choose not to use trailing soft hyphens in classified files that you plan to convert to PDF format.

Directory Control File Changes

DG added the following entry to the // Windows 10 Performance Improvements section of the default Agent Directory Control File (dirctrl.dat) to prevent the DgAgent.exe process from consuming CPU due to content inspection of XO Worktime Communicator log files:

%SystemDrive%\Users*\appdata\local\xo communications\worktime*

DG Agent 7.6.3

New process flags are available in DG Agent 7.6.3.

Process Flags File Changes

Microsoft Outlook COM objects are tracked to help detect various network events, so WinINet and WinSock tracking is not needed. You can use the following flags to prevent WinINet and Winsock tracking:

```
outlook.exe,SB+WS+AS+DWNG+DWSP
```

DG Agent 7.6.2

New process flags are available in DG Agent 7.6.2, and the Directory Control File (dirctrl) has been updated.

Process Flags File Changes

You can use the following flags to minimize DG Agent involvement in the activities of the following cloud-based processes:

```
googledrivesync.exe,SK+NI
GoogleDriveFS.exe,SK+NI
onedrive.exe,SK+NI
```

Directory Control File Changes

DG added this entry to SECTION DOCPROPS and SECTION AC12 of the Directory Control File (dirctrl.dat) to prevent temporary file scanning of operations related to Microsoft OneDrive :

```
%SystemDrive%\Users*\AppData\Local\packages\microsoft.oneconnect_*\localstate*
```

Chapter 5

Resolved Issues

The following issues were resolved in the last three releases.

DG Agent 7.6.4

The following issues were resolved in DG Agent 7.6.4 for Windows.

AG-40443

Version 7.6.2 and 7.6.3 DG Agents can have a problem with bundle processing under certain conditions. This can affect forensic reporting to the DGMC and to ARC. A code enhancement to the Agent prevents that from happening.

AG-39332

If Webcast.com/webrtc was accessed using Google Chrome or Microsoft Edge, the microphone and camera tests failed with an error due to an issue with Digital Guardian web inspection proxy (DG WIP). DG added code to the DG Agent to resolve this.

AG-39265

The packaged Boldon James software installer provided by DG was updated at the request of a customer.

AG-39241

When a customer using Microsoft Notepad cuts and pastes text from a file that has permanent classification tags to a new file in Notepad, the classification tags are not propagating as they should to the new file when the customer closes and saves the new file. The problem has been rectified by a code change.

AG-39236

An organization that uses a USB whitelist rule to whitelist events captured on employee USB devices found that DG Agent 7.6.2 reported a different serial number (SN) for Elecom External SSD (USB Attached SCSI) devices than the one reported by the Windows USBView UI app. DG addressed this issue, ensuring the existing whitelist rule and component list can still be used as is.

AG-39013

When an email is sent from Microsoft Outlook to a destination user in the same company as the sender, and the email has a file attachment that was previously classified and contains a permanent tag (or tags), the DG Agent embeds the details of the permanent tags into an internal email property (x-dg-ref), which the DG Agent on the destination user's computer uses to decode the details of the permanent tag and apply any tags to the file attachment when it is saved. When the internal email property contained more than 2 KB of data, the destination DG Agent could not detect it. To address this issue, the DG Agent now uses a different API interface that allows the destination DG Agent 7.6.4 or later for Windows to detect data in x-dg-ref regardless of the amount. To ensure that no data is missed, DG recommends upgrading all of your Agent computers to DG Agent 7.6.4 or later.

AG-38906

DG resolved a Google Chrome interoperability issue between the DG Agent and SentinelOne endpoint security software that occurred through named pipes (a FIFO system for interprocess communication).

AG-38867

If you invoke an Agent rule string function with an incorrect parameter, it might cause a system crash. DG has fixed this issue.

AG-38817

When you create a classification rule that includes a content pattern with a trailing soft (visible) hyphen (-) character, such as -Highly Confidential- (no spaces), the ACI content inspection engine filters out the trailing soft hyphen when reading pdf files. This causes the classification rule to fail because the data pattern will never match the rule. No such filtering occurs with other file types. DG added the aciEnableSoftHyphenFiltering custom configuration setting to the DG Agent , which allows you to override the content inspection engine's default behavior and use a trailing soft hyphen in your classification rules. For details, refer to the "Agent Configuration Settings" table in Appendix B of *Digital Guardian Management Console User's Guide*.

AG-38747

A memory leak on DG Agent computers running Windows Server 2016 Core (Standard) resulted in performance issues, which were resolved with an Agent upgrade and configuration changes.

AG-38714

Attempting to extract a file from a zip file failed due to inadvertent, low-level side effects triggered by DG Agent code. DG has eliminated those side effects.

AG-38514

A system failure occurred when DG accessed an object after the object was destroyed due to a reference counting issue. The problem has been rectified by a code change.

AG-38379

When a file on a local drive was dragged into Google Chrome and then saved using Save As to Desktop, the Local Forensic Report incorrectly displayed the source path as "*source file name* - google chrome". The destination file path was correct. DG addressed this with a code fix.

AG-37107

In a few very limited circumstances, the To email recipient address in a message sent from Microsoft Outlook was not being reported in Send Mail events in the Forensic Reports. A code enhancement resolved this.

DG Agent 7.6.3

The following issues were resolved in DG Agent 7.6.3 for Windows.

AG-39332

If Webcast.com/webrtc was accessed using Google Chrome or Microsoft Edge, the microphone and camera tests failed with an error due to an issue with Digital Guardian web inspection proxy (DG WIP). DG added code to the DG Agent to resolve this.

SA-38589

DG fixed a case of a rare crash in a third-party application integrated with Microsoft Excel when document properties were enabled.

SA-38577

When you created a ZIP file to send files collected by the System Scanner to the DGMC, file names that contained a unicode character stopped the zip creation process at the affected file, leaving the zip file incomplete. To address this, DG Agent code now handles opening unicode file names and treating the file names as unicode so they appear in the zip file correctly. Also, if any file fails to be added to the zip file for any reason, the zip creation process continues.

AG-38515

The following scenario occurred in an environment that had many computers with many Agents configured to perform classification on remote network drives used by those computers. Classification recurred frequently, which caused delays, because each Agent performed classification on the same file if it detected that the classification hash value recorded in the ADS stream of the file did not match the expected classification hash value that was computed based on the classification hash algorithm executed against the deployed policies and rules for that specific Agent.

DG altered the Agent classification hash algorithm to allow computers with identical policies and rules to perform classification on a file only as often as necessary.

AG-38379

When a file on a local drive was dragged into Google Chrome and then saved using Save As to Desktop, the Local Forensic Report incorrectly displayed the destination file path as both the source file path and destination file path. DG addressed this with a code fix.

SA-37811

The DG camera control feature, which uses rules to control the Windows Camera utility, failed to block the Camera on DG Agent computers running Windows 10 build 1909 and above due to an error that prevented the DG filter from attaching to the Camera device. This issue was addressed by creating a REQ function to retry the failing MicroSoft API call a specific number of times to allow for the Camera device to finish mounting.

SA-37468

The DG Agent did not track changes to the Windows registry made by its own processes. This issue has been addressed in the Digital Guardian Agent 7.6.3 for Windows release.

SA-37453

DG applied process flags to resolve an issue where Microsoft Outlook intermittently disconnected from Microsoft Exchange Servers.

SA-37428

If a user attempted to mount a USB storage device on a PC, a device control rule prompted the user and blocked the action. If the user left the USB device plugged in, after a reboot, there was a delay in loading the rule, which allowed the user temporary access to the device before a prompt appeared and the device unmounted. DG resolved this issue with a code fix.

SA-37108

When the licensed User Classification (UC) feature is enabled, the DG Agent will install the Boldon James Classifier API so that the Agent can read UC metadata that may reside within a file. The Classifier API is installed as part of the DG Agent install and is packaged within a zip file. The installation process makes a backup copy of the zip file and extracts the original zip file. If the installation fails, additional attempts to enable the UC feature will fail because the original zip was lost during the extraction process. Without the original zip file, additional attempts to reenable the UC feature fail. DG made changes to the Agent so that now it recreates the original zip from the backup, if necessary.

SA-35136

If ACI was enabled, and Microsoft Office 365 Excel was used to open a file residing in the OneDrive folder, the DG Agent performed content inspection every time the file was opened, which the customer saw as a delay. DG made code changes to the Agent so that it only performs content inspection when required.

DG Agent 7.6.2

The following issues were resolved in DG Agent 7.6.2 for Windows.

SA-38590

When the DG Agent attempted to hook the Firefox process in order to capture events, Firefox 82 shut down. To resolve this issue, DG removed the hooking code used when the DG web inspection proxy (WIP) is disabled. Note that when WIP is disabled, some features of DG protection will not work due to the removal of the hooking code. DG strongly recommends leaving WIP enabled to protect against data loss occurring through the Firefox browser.

SA-38102

In a few test cases, if you started Microsoft Outlook and created a new email, either with or without populating the Subject line, and then copied some text from a different application but did not paste it into the message, an Application Data Exchange (ADE) paste event was incorrectly generated and sent to the DGMC. This was fixed so that now the DG Agent detects these scenarios and filters out the ADE paste event so that it is not sent to the DGMC.

SA-38034

When a rule was deployed to take action based upon the curProcessAddressBar (the address bar of the currently active browser tab), and you accessed a website and performed an NTU or NTD using a Firefox browser configured to use a display language other than English, the rule failed to work as intended and the address bar was blank instead of showing the expected value of curProcessAddressBar. DG fixed this issue so that the address bar shows the expected value in any display language Firefox is set to.

SA-37987

If you used the Outlook application from Microsoft Office 365 to create a new email and then used drag and drop to add a classified file as an attachment, a control rule to display a block prompt when a user attaches a classified file to email failed. The failure was caused by the DG Agent not reporting an Attach Mail event to the DGMC. DG made code changes to address this issue.

SA-37894

A system failure occurred on some DG Agent computers due to an infinite loop caused by a malformed DNS packet. DG resolved the issue with a code fix and enhancement of the DNS packet processing.

SA-37818

When DgUpdate is run to enable a feature or update DG Agent, it may need to shut down and restart DgService as part of the update. Under some circumstances, DgService can hang while being shut down. This prevents the update from successfully completing, and will leave the Agent terminated until the computer is rebooted. One example is enabling the User Classification (UC) feature. To prevent this problem, DG added code to ensure that DgService is shut down. With the service shut down properly, updates are now able to complete successfully.

SA-37783

DG fixed an issue that was preventing the DG Agent from detecting and capturing NTU and NTD data for the DocuSign e-sign website and reporting it in the Local Forensic report.

SA-37437

Event bundling sequence errors resulted in a great many random operational alerts in the DGMC. This occurred due to heavy activity on DG Agent computer shutdown, causing two STORE files to be left behind. Further, on reboot, storage was initialized with the two STORE files in the wrong order due to sorting based on a timestamp. DG resolved the issues by serializing file I/O activity against the STORE files and sorting the STORE files by sequence number.

SA-37402

A control rule with justification prompt should have resulted in a block event in the DGMC and ARC when the copy operation was canceled by the user. Instead, the DG Agent reported the file copy operation as successful. This issue only occurred when a control rule did not have an alert enabled (event only) and a filter rule was present. DG resolved this with a code fix. A block event is now properly reported.

SA-37166

After Boldon James software (DG User Classification) was added to a system, various applications hung or failed to open when the DG Agent attempted to determine whether the window that was open was a Boldon James User Classification selection window that DG needed to inspect when doing Boldon James processing. DG resolved this issue by using a different API to get the window title text.

SA-37157

When you created an email in Microsoft Outlook 365 and attached a cloud file from OneDrive using the Outlook Insert File dialog, the dialog would hang near completion. To resolve this issue, DG has improved its detection of cloud files and added entries to the default Process Flags File (prcsflgs.dat) and the Directory Control File (dirctrl.dat). For details, refer to "DG Agent 7.6.2" on page 23.

SA-37152

DG WIP required up to a 24-hour delay when a website certificate was updated before the change would become effective, leading to transient certificate errors in certain circumstances. To resolve this issue, DG now removes the changed certificate from its cache if a website certificate changes during the cache period. This ensures that certificate updates are propagated to the user's browser without delay.

SA-36776

An exception resulted in DG Agent computers failing when a second solid-state drive (SSD) or hard disk drive (HDD) was attached to the physical HDD socket, and the computers were rebooted. The exception was caused by DG code improperly processing an internal NT File Sytem (NTFS) metadata file, which conflicted with Microsoft Windows Distributed Link Tracking Client (TrkWks) service. To resolve this problem, DG now forwards internal NTFS metadata files without processing them.

SA-35564

A user with a remote drive path that was mapped to an actual drive (for example, V:) and whitelisted for data transfers to certain network locations was blocked intermittently from completing network data transfer operations. This occurred because the full remote destination (UNC) path exceeded the maximum length supported by the DG Agent code, so the Agent used the path of the actual drive (V:) to determine whether to block the user. DG altered the Agent code so that the Agent now truncates long destination paths to the maximum supported length.

SA-34981

Frequent "Unsolicited incoming ARP reply detected" warning messages appeared on DG Agent computers due to Symantec Endpoint Protection software detecting the DG Agent performing an ARP (Address Resolution Protocol) request to retrieve the gateway MAC address. DG altered the Agent code so that it no longer sends an ARP request to retrieve the gateway MAC address when no DG rules are using the agentGatewayMac property.

SA-34285

When you took a screen capture on a high-resolution monitor or screen through the DG Investigation Module (IM), the resulting screenshot only showed part of the screen because the IM module was not able to make itself aware of the system-wide change in screen resolution (DPI), as required by Microsoft. As a result, the IM could not correctly calculate the screen capture's resolution. DG added code to allow the IM to become aware of the change in screen resolution and calculate the screen capture's resolution correctly.

SA-33773

The DG Agent installer returned success code 0 for a successful DG Agent installation when a customer was expecting error code 3010, which indicates that a manual post-installation reboot is required. Because many customers rely on exit code 0, DG resolved this issue by providing the optional EXITCODES="yes" parameter to the msiexec command to support updated return codes.

Along with EXITCODES="yes", you may also want to use the standard /norestart option.

Using EXITCODES= yes with /norestart, returns code 3010 (ERROR_SUCCESS_REBOOT_REQUIRED), and you must manually initiate the post-installation reboot.

```
start /wait msiexec /I "DGBaseAgent.msi" EXITCODES="yes" /qn /l*v
"C:\testInstall.log" /norestart
```

Using EXITCODES="yes" without /norestart, returns code 1641 (ERROR_SUCCESS_REBOOT_INITIATED), and the system immediately reboots post-installation.

```
start /wait msiexec /I "DGBaseAgent.msi" EXITCODES="yes" /qn /l*v
"C:\testInstall.log"
```

For details on msiexec command-line options available beginning with Windows Installer 3.0, refer to https://docs.microsoft.com/en-us/windows/win32/msi/standard-installer-command-line-options.

SA-31853

The DG Agent did not capture the product ID (PID) and vendor ID (VID) for an SSD external SCSI device attached to a DG Agent computer through a USB port. Also, different serial numbers were displayed for FileCopy and DeviceAdded events in the Device Details dialog box. DG added support for UAS (USB attached SCSI) devices to properly retrieve the VID, PID, and Serial Number.

SA-19262

A rule using constOpNetwork to block outbound network connections failed to display a justification prompt requiring a user response before continuing. Although DG does not support prompts that require a delay in network traffic while waiting for a user response, DG code was preventing any prompts for network events. To resolve the issue, DG made code changes that allow prompts that do not have to wait for user input to continue, including a warn prompt that lets the user go on and a block prompt that prevents additional user action. These code changes apply to any prompts that cannot wait for user input before continuing, not only prompts for network events. If a prompt cannot be displayed, the default action for the prompt is taken.

Chapter 6

Known Issues

This section describes issues that have not been resolved in a Digital Guardian Agent for Windows release and provides workarounds when available.

AG-40198

A customer experienced a system failure while closing a file in Microsoft Windows. The close operation caused the failure when it interacted with the Windows file clean up routine.

Workaround: To prevent the system failure, deploy these configuration settings to the Agent and reboot the computer.

```
<dgfsmon_useAssocFileInOpenFileOrStream regHive="HKLM"
regKey="SYSTEM\CurrentControlSet\Services\DGMaster\Parameters\dgfsmon"
regName="dgfsmon_useAssocFileInOpenFileOrStream" regType="DWOR">1</dgfsmon_
useAssocFileInOpenFileOrStream>
```

```
<dgfsmon_UseCreateForAll regHive="HKLM"
regKey="SYSTEM\CurrentControlSet\Services\DGMaster\Parameters\dgfsmon"
regName="dgfsmon_UseCreateForAll" regType="DWOR">1</dgfsmon_UseCreateForAll>
```

AG-38429

When SentinelOne software is running on an Agent computer, a Customer reports frequent Microsoft Excel application hangs, mostly when when trying to save files to local or mapped drives. Canceling the operation or restarting Excel on the Agent computer restores computer operation.

Workaround: To prevent Excel from hanging, deploy these configuration settings to the Agent and reboot the computer.

```
<dgfsmon_useAssocFileInOpenFileOrStream regHive="HKLM"
regKey="SYSTEM\CurrentControlSet\Services\DGMaster\Parameters\dgfsmon"
regName="dgfsmon_useAssocFileInOpenFileOrStream" regType="DWOR">1</dgfsmon_
useAssocFileInOpenFileOrStream>
```

```
<dgfsmon_UseCreateForAll regHive="HKLM" regKey-
y="SYSTEM\CurrentControlSet\Services\DGMaster\Parameters\dgfsmon" regName-
e="dgfsmon_UseCreateForAll" regType="DWOR">1</dgfsmon_UseCreateForAll>
```

SA-37016

After you install a DG Agent, reboot, log on to Windows, and the OneDrive cloud service app starts and tries to sync, you will see an error message stating that OneDrive could not connect to Windows. You will not be able to access your on-demand files, and new files will not be backed up when placed in the OneDrive folder. DG will have a permanent fix for this issue in a future release.

Workaround: Use either of the following methods as an interim fix.

- Open a Windows command prompt and run the following command:

```
reg add HKLM\System\CurrentControlSet\Services\Cldflt\instances /f /v
DefaultInstance /t REG_SZ /d "CldFlt"
```

- Edit your existing config.xml file on the DGMC Custom Configuration Resources page or create a new custom configuration resource if you are not already using one.

```
<appSettings>
<CldFlt_Instances pushDuringUpdate="1" regHive="HKLM"
regKey="SYSTEM\CurrentControlSet\Services\CldFlt\Instances"
regName="DefaultInstance" regType="STRI">CldFlt</CldFlt_Instances>
</appSettings>
```

Note: The <appSettings> and </appSettings> tags are already present if you are editing an existing resource definition. You need to add these elements when you create a new custom configuration resource.

SA-36873

USB Add Device events coming from DG Agent computers running Windows 10 version 2004 might be missing the source file name. This is because Windows 10 version 2004 does not return the friendly name for the device. Other details about the device can be found by clicking on the Device Details icon for the event.

SA-36151

When you copy files from a local DG Agent computer to a remote computer via a Remote Desktop (RDP) session, only the source file directory is reported for the copy events in the Local Forensic Report. The file name and the destination path are not captured. No event is shown for the file copy from the RDP session to the local machine.

SA-27076

Uninstalling the DG Agent using the Control Panel's Programs and Features while the Boldon James User Classification software is enabled causes the uninstallation process to appear that it never completed. It does complete, however. Restart the computer to complete the process.

Workaround:

If the Boldon James software is enabled, always uninstall the DG Agent from the DGMC.

SA-19295

Improper use of the rule DG_SetTimerEvent can cause a system crash.

Workaround: DG has disabled this rule to prevent its improper use. If you need to use this rule, please contact Customer Support for assistance.

SA-19194

Adaptive Content Inspection (ACI) does not work when DG Agents are installed or upgraded from the DGMC (System> Computers > Actions > Install Agents).

Workaround: Installation of DG Agents from the DGMC is intended only for test and demo environments. Remove the DG Agent and reinstall it using a supported installation method. For more information, refer to the *Digital Guardian Installation and Upgrade Guide*.

SA-17335

On computers with DLP, user classification, and ACI enabled, user classification tags are not propagated to a Microsoft Office document (Word, PowerPoint, or Excel) saved as an XPS (XML Paper Specification) file.

SA-17334

On computers with DLP, user classification, and ACI enabled, user classification tags are not propagated to a Microsoft Word document saved as an RTF file.

SA-17253

On computers with DLP, user classification and ACI enabled, if you send a non-classified email message with an attachment that has a user classification, the Send Mail action erroneously triggers a warning prompt. You can still send the email.

SA-17252

On computers with DLP, user classification and ACI enabled, if you use a DG rule to prevent a user from saving a newly created Microsoft Excel, Word, or PowerPoint file, and the file does not have a user classification, even if the user specifies a user classification before saving the new file, the rule still triggers. This prevents the user from applying the classification and from saving the file.

Workaround: To require a user to apply a user classification on a new document before saving it, use the Boldon James software to create a policy. Once the user classification has been applied, you can use DG rules to control the movement of the files based on the user-applied classification tags.

SA-13225

If you copy content from a Microsoft PowerPoint document to a different PowerPoint document with the same name but a different file path, the Agent does not block the copy operation as expected when you have rules that should block the copy.

SA-10932

Applying a Block Send Mail rule does not block sending a message that contains a file that is attached or inserted from the Outlook Drafts folder.

SA-10761

Under certain circumstances, a rule to block FileArchive of certain classified files fires and the DGMC shows the action as blocked, but the zip file is still created and the classified file is added to the zip archive.

SA-10759

If you apply a classification rule to classify image files based on specific extensions (for example, bmp, jpg, gif) and you use the Insert tab on the ribbon to insert the classified image file into a Microsoft Word or PowerPoint file, the classification tag is not propagated to the Word or PowerPoint file, and the action is not captured in the Forensic Report.

SA-10572

The DG Agent does not capture and control many events correctly on devices that use media transfer protocol (MTP). As a result, rules do not fire when expected.

SA-10571

The DG Agent does not report device-added events for devices that use media transfer protocol (MTP).

SA-10365

If you rename a file using file transfer protocol (FTP) with Microsoft Windows Explorer or a Command Prompt, the Agent does not report the operation. You do not see the file rename event in the forensic reports in the console.

SA-10165

If you create a PowerPoint Presentation CD using a classified PowerPoint file, when you use the Export option to save the package to a USB device or SD card, DG does not generate a prompt or log the event.

SA-10149

After copying files to the CD/DVD Explorer window and clicking the Encrypt button, the files are encrypted in the Staging Directory. When you then burn the files to the CD-RW drive, all of the files are correctly encrypted on the drive. However, the Local Forensic Report erroneously lists some files as Not Encrypted, and a message indicates that there are files waiting to be burned to disc. You can ignore the erroneous message. All of the files are successfully burned to the CD-RW drive and encrypted as expected. This issue occurs on CD-RW format only when CD RME is enabled and the file size exceeds 50 KB.

SA-9994

When users send emails in rich text format (RTF) or HTML format, the attached image size appears to be 0 KB in the forensic reports. Users might encounter this issue when they send emails with Microsoft Outlook 2007 or 2010.

SA-9907

When you remove a DG Agent from the DGMC with Scan on Uninstall selected, the DG Agent is removed from the target computer successfully, but the DGMC might initially report the status of the DG Agent as terminated. This happens because the status updates every 30 minutes to prevent overloading the DG Server. In a short time, the console will report the DG Agent status correctly.

Chapter 7

Discontinued Support

The following features, options, and systems are no longer supported.

DG Agent 7.4.x for Windows

Effective with the DG Agent 7.6.2 release, DG no longer provides mainstream support for DG Agent for Windows, versions 7.4, 7.4.1, and 7.4.2. These Agents have transitioned out of mainstream support to Extended Support. Customers on Extended Support for DG Agent 7.4.2 will receive best-effort critical updates, subject to any limitations imposed by the Microsoft environment. Critical updates are provided to resolve security defects in the DG Agent that might enable code execution by an adversary without user interaction. For more information, refer to the Digital Guardian Agent for Windows Support Notice entitled "Notice of End of Support for Digital Guardian Agents for Windows, v7.4.x."

Microsoft Edge Legacy

Effective with the Agent 7.6 for Windows release, the Agent no longer supports the Microsoft Edge Legacy web browser.

constOpDocumentRepository

Effective with the Agent 7.6 for Windows release, the Agent no longer supports the constOpDocumentRepository operation type.

Location-Based Trends

Effective with the DG Server 8.2 release, DG no longer supports creating location-based custom trends.

Windows Server 2012 R2

Effective with the DG Server 8.1 release, DG no longer supports Windows Server 2012. Microsoft removed mainstream support for Windows Server 2012 in October 2018.

SQL Server 2012

Effective with the DG Server 8.1 release, DG no longer supports SQL Server 2012. Microsoft removed mainstream support for SQL Server 2012 in October 2018.

Support Discontinued for SQL Server 2014

Effective with the DG Server 8.1 release, DG no longer supports SQL Server 2014. Microsoft removed mainstream support for SQL Server 2014 in October 2017.

Microsoft OS Versions

Effective with the DG Server and Agent 7.5 release, the Agent for Windows does not support Windows 7, 8.x, 10 Threshold 1, Server 2012 R2 operating system computers.

Classification API

Effective with the DG Server and Agent 7.5 release, DG no longer offers or supports the Classification API.

IOS Mobile

Effective with the DG Server and Agent 7.5 release, DG no longer sells or supports the Digital Guardian Mobile App for iOS devices.

AFE and AME

Effective with the DG Server and Agent 7.5 release, DG no longer sells the Adaptive File Encryption (AFE) and Adaptive Mail Encryption (AME) features. Customers with a valid AFE or AME license can upgrade to DG 7.5 Server and continue using AFE and AME with their pre-DG 7.5 Agents. DG continues to support other encryption options, including Removable Media Encryption, Portable Encryption, and CD/DVD Encryption.

Memory Forensics

Effective with the DG Server and Agent 7.4 release, DG no longer sells or supports the Memory Forensics add-on module.

URL List Properties

DG no longer supports the following URL list properties:

- curProcessURLList
- parentProcessURLList

- evtSrcProcessURLList

These properties do not return the URL list of the current or parent process or of the source process. Rules that use these properties will compile correctly in this release if the properties are used in a rule with an "OR" and the rule executes correctly for other properties in the "OR" clause. The URL list properties will be removed from a future release of the DG Agent, and rules using these properties will not compile and will not execute on the endpoint. Rules using these properties should be rewritten without them.

DG NetComm (Fidelis Network DLP)

Effective with the DG Server and Agent 7.4 release, DG no longer supports DG NetComm (Fidelis Network DLP) for managing Network DLP. Instead, Digital Guardian provides the Network Data Loss Prevention (DG Network DLP) solution, which offers both virtual machine and DG Appliance deployment options.

DG Network DLP monitors and controls network communications to prevent sensitive data from leaving your network and support compliance efforts for your sensitive and regulated data. DG inspects all network traffic and then enforces policies to ensure protection. Policy based actions include: allow, prompt, block, encrypt, reroute, and quarantine. Digital Guardian monitors and controls all communications channels, including email, Web, File Transfer Protocol, Secure Sockets Layer, and applications such as webmail, blogs and other social media.

For more information, refer to the Digital Guardian website, digitalguardian.com, or contact your Digital Guardian representative.