Symantec Data Loss Prevention 15.7 Maintenance Pack 2 Release Notes

Last updated: February 19, 2021

Table of Contents

Introduction

About these release notes

These release notes include late-breaking information and are updated periodically. You can find the most current version of the release notes at the Broadcom Tech Docs Portal.

Other Symantec products that integrate with Symantec Data Loss Prevention have their own release notes, which you can find at the Broadcom Tech Docs Portal.

About Symantec Data Loss Prevention 15.7 Maintenance Pack 2

Data Loss Prevention 15.7 Maintenance Pack 2 includes important product defect fixes for the Enforce Server, detection servers, and Windows and macOS DLP Agents. Symantec recommends that you apply the maintenance pack as soon as possible to all components.

> **NOTE**
>
> This is a re-release of Symantec Data Loss Prevention 15.7 Maintenance Pack 2 (originally released in December 2020). The names of the ZIP files for Maintenance Pack 2 that you can download from the Broadcom Product Downloads portal have been appended with "_b" to indicate the re-release. Make sure that you download and unzip the correct files before you deploy Maintenance Pack 2.
>
> For more information, see What's changed in the re-release of Data Loss Prevention 15.7 Maintenance Pack 2.

Due to architectural changes introduced in macOS 11, beginning with Data Loss Prevention 15.7 MP2, the macOS DLP Agent uses the Apple Endpoint Security Framework. The change to a new framework requires several important adjustments to Endpoint monitoring and deployment. Updated browser extensions for Google Chrome and Mozilla Firefox are also provided in Maintenance Pack 2. Endpoints that have not been upgraded to macOS 11 can continue to use the previously deployed DLP Agents.

The Enforce Server now reports when monitoring for Google Chrome and Mozilla Firefox has been disabled or tampered with on macOS 11 endpoints. Endpoints on which the Google Chrome extension or the Mozilla Firefox extension is not functional are now indicated to be in the Critical (red) state on the **Agent Overview** page of the Enforce Server administration console.

The Microsoft Outlook monitoring solution has been rearchitected for compatibility with the changes in macOS 11. Maintenance Pack 2 introduces a new Microsoft Outlook add-in that you can deploy from the Microsoft 365 admin center. As of Maintenance Pack 2, Symantec Data Loss Prevention monitors only versions of Microsoft Outlook that support the add-in model. To continue monitoring Microsoft Outlook on endpoints that have upgraded to Maintenance Pack 2, you must install Microsoft Outlook 16.30 or a more recent version.

What's changed in the re-release of Data Loss Prevention 15.7 Maintenance Pack 2

The re-release of Data Loss Prevention 15.7 Maintenance Pack 2 includes the hotfix that is described in the January 30, 2021 update at https://support.broadcom.com/external/content/critical-alerts/DLP-15.7-MP2-Required-Hotfix-for-Windows/16909.

If you have already installed the hotfix or the original Maintenance Pack 2 release (December 2020), see the advisory at https://support.broadcom.com/external/content/critical-alerts/Revised-DLP-15.7-MP2-Available-Soon-and-Actions-All-DLP-15.7-Customers-Can-Take/17194.

If you plan to deploy the re-release, you can follow the deployment instructions that are provided in the *Symantec Data Loss Prevention 15.7 Upgrade Guide*. In the original release of Maintenance Pack 2, the upgrade sequence of Data Loss Prevention components was different from the documented process.

In addition, with the re-release, the re-architected DLP Agent supports macOS 10.14 and 10.15.

Applying Symantec Data Loss Prevention 15.7 Maintenance Pack 2

Before applying Maintenance Pack 2 or installing Symantec Data Loss Prevention 15.7, refer to the system requirements documentation at the Data Loss Prevention 15.7 Help Center for information about system requirements.

The rearchitected DLP Agent in Maintenance Pack 2 supports macOS versions 10.14, 10.15, and 11. Endpoints that have not been upgraded to macOS 11 can continue to use the previously deployed DLP Agent.

If you plan to upgrade endpoints to macOS 11, you must deploy the new DLP Agent on those endpoints immediately after completing the upgrade to avoid any downtime in agent monitoring. If you deploy the re-architected DLP Agent on macOS endpoints, you must also upgrade the Enforce Server and detection servers to Maintenance Pack 2.

The create_package tool is no longer supported. You must generate agent installation packages using the **System > Agents > Agent Packaging** screen of the Enforce Server administration console.

For detailed information about applying the Maintenance Pack, see the chapter "Applying a Maintenance Pack" in the *Symantec Data Loss Prevention Upgrade Guide*.

> **NOTE**
>
> This is a re-release of Symantec Data Loss Prevention 15.7 Maintenance Pack 2 (originally released in December 2020). The names of the ZIP files for Maintenance Pack 2 that you can download from the Broadcom Product Downloads portal have been appended with "_b" to indicate the re-release. Make sure that you download and unzip the correct files before you deploy Maintenance Pack 2.
>
> For more information, see What's changed in the re-release of Data Loss Prevention 15.7 Maintenance Pack 2.

Change in the dependency on Microsoft Visual Studio 2010

As of version 15.7 Maintenance Pack 2, Data Loss Prevention no longer uses Microsoft Visual Studio 2010 Runtime. Instead, Data Loss Prevention has now upgraded to Microsoft Visual C++ 2019. When you deploy 15.7 Maintenance Pack 2, Microsoft Visual C++ 2019 Runtime version 14.25.28508.3 is installed as a necessary dependency. This might overwrite any existing build of Microsoft Visual C++ 2019 Runtime.

If another application uses Microsoft Visual Studio 2015 or later on the same computer that has Data Loss Prevention installed, when you upgrade to Data Loss Prevention 15.7 Maintenance Pack 2, you will be prompted to restart the computer. If you upgrade the Enforce Server or detection servers with the guidance of a user interface, you will be prompted to restart the server at the end of the upgrade. If you perform a silent installation instead, the installation logs will indicate the need to restart. For endpoints, after you upgrade the DLP Agent, you will be prompted to restart the endpoint.

Creating an MDM configuration profile to allow full-disk access for the endpoint security host application (SEHA.app) on macOS endpoints

You must configure an MDM profile to allow full-disk access for the endpoint security host application (`SEHA.app`) on macOS 11 endpoints.

For illustration purposes, the following instructions assume that you plan to use Jamf, an IT management application.

1. In Jamf, select a configuration profile.
2. Navigate to **Privacy Preferences Policy Control**.
3. Under **App Access**, in the **Identifier field**, type `com.symantec.dlp.ext.host.application`.
4. In the **Identifier Type** menu, select **Bundle ID**.
5. In the **Code Requirement** field, enter the following:

```
anchor apple generic and identifier "com.symantec.dlp.ext.host.application"
and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or
certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
Y2CCP3S9W7)
```

   NOTE
   If you copy this information from the documentation, make sure that there are no extra line breaks when you paste it in the **Code Requirement** field.

6. In the **APP OR SERVICE** table, add the following settings:

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow
SystemPolicyRemovableVolumes	Allow
SystemPolicyNetworkVolumes	Allow

7. Click **Save**.

   NOTE
   You can refer to the **System > Agents > Overview** page of the Enforce Server administration console to view and troubleshoot any issues.

Creating an MDM configuration profile to allow full-disk access for the DLP Agent on macOS endpoints

You must configure an MDM profile to allow the full disk access for the DLP Agent on macOS endpoints.

For illustration purposes, the following instructions assume that you plan to use Jamf, an IT management application.

1. In Jamf, select a configuration profile.
2. Navigate to **Privacy Preferences Policy Control**.
3. Under **App Access**, in the **Identifier field**, type `/Library/Manufacturer/Endpoint Agent/edpa`.
4. In the **Identifier Type** menu, select **Path**.
5. In the **Code Requirement** field, enter the following:

```
identifier edpa and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists / and certificate
leaf[field.1.2.840.113635.100.6.1.13] / exists */ and certificate leaf[subject.OU] =
Y2CCP3S9W7
```

   NOTE
   If you copy this information from the documentation, make sure that there are no extra line breaks when you paste it in the **Code Requirement** field.

6. In the **APP OR SERVICE** table, add the following settings:

APP OR SERVICE	ACCESS
SystemPolicyAllFiles	Allow
SystemPolicyRemovableVolumes	Allow
SystemPolicyNetworkVolumes	Allow

7. Click **Save**.

NOTE
You can refer to the **System > Agents > Overview** page of the Enforce Server administration console to view and troubleshoot any issues.

Deploying the on-send web add-in for Outlook on macOS endpoints

The on-send web add-in for Outlook on macOS endpoints enables Symantec Data Loss Prevention to monitor emails and calendar events that are created and sent using Microsoft Outlook and Outlook Web Access.

Before you install the on-send web add-in for Outlook on macOS endpoints, review the list of best practices. See Best practices for deploying the on-send web add-in for Outlook on macOS endpoints.

To deploy the on-send add-in for Outlook on macOS endpoints, perform the following actions:

1. Download the macOS agent package from the Broadcom Product Downloads portal and extract it to a temporary directory.
2. Locate the extracted `Outlook-Addin-Manifest.xml` file in the `Endpoint/Mac/x86_64/Add-in` directory. The `Outlook-Addin-Manifest.xml` file contains all of the information required to download and the files that are required to install the add-in.
3. Follow the instructions provided in the Microsoft 365 documentation at https://docs.microsoft.com/en-us/microsoft-365/admin/manage/manage-deployment-of-add-ins?view=o365-worldwide#deploy-an-office-add-in-using-the-admin-center.

NOTE

- You must also deploy the truststore certificate that is used by the on-send web add-in.
  Deploying the truststore certificate for the on-send web add-in for Outlook on macOS endpoints
- To enable monitoring for Outlook Web Access in Mozilla Firefox on macOS endpoints, see Creating an MDM configuration profile to support monitoring in Mozilla Firefox and enable Outlook Web Access monitoring on macOS endpoints.

.

Best practices for deploying the on-send web add-in for Outlook on macOS endpoints

Before you deploy the on-send web add-in for Outlook on macOS endpoints, review the following best practices:

- Make sure that Symantec Data Loss Prevention 15.7 MP2 is successfully deployed on the endpoints and on the Enforce Server.
- Make sure that Microsoft Outlook version 16.30 or later installed on the endpoints.
  Note: The add-in does not support Microsoft Outlook 2016.
- Make sure that you have an active Microsoft Outlook 365 subscription or a Microsoft Exchange Online subscription.
- Make sure that one of the following ports is open and available on the endpoints:

  - 4631
  - 4641
  - 4651
- Make sure that the Symantec add-in server (https://officeapp.endpoint.dlp.protect.symantec.com) is added to the allow list in your organization's Internet firewall. After deployment, the add-in downloads various resources that it needs to function from the Symantec add-in server.
- Make sure that on-send feature for add-ins is enabled in Outlook. For more information, see https://docs.microsoft.com/en-us/office/dev/add-ins/outlook/outlook-on-send-addins?tabs=classic#enable-the-on-send-feature.
- Do not sideload the add-in as the add-in might not function if you deploy it that way.
- Mailbox users should not be allowed to disable or remove the add-in.
- Do not remove the truststore certificate used by the add-in from the keychain. If you remove the truststore certificate from the keychain Outlook monitoring becomes disabled, and it could take up to 75 minutes for the agent state to change to critical in the Enforce Server administration console.

Deploying the truststore certificate for the on-send web add-in for Outlook on macOS endpoints

The following instructions describe the process of creating an MDM configuration profile to deploy the truststore certificate that is used by the on-send web add-in. For illustration purposes, the instructions assume that you plan to deploy the certificate using Jamf, an IT management application.

1. On the **System > Agents > Agent Packaging** screen of the Enforce Server administration console, generate the required agent installation package.
2. Extract the contents of the agent installation package to a temporary folder.
3. Locate the extracted `addin_truststore.pem` file, and rename it to change the file extension to `.cer`. The renamed file should be called `addin_truststore.cer`.
4. In Jamf, select a configuration profile.
5. Navigate to the **Certificate** section and upload the `addin_truststore.cer` file.

After you finish deploying the truststore certificate, on an endpoint, verify that the certificate is present in the system keychain.

Creating an MDM configuration profile to support monitoring in Mozilla Firefox and enable Outlook Web Access monitoring on macOS endpoints

The following instructions describe the process of creating an MDM configuration profile to deploy the new Mozilla Firefox extension as well as a signed certificate to enable Outlook Web Access monitoring in Firefox on macOS endpoints. For illustration purposes, the instructions assume that you plan to deploy the extension using Jamf, an IT management application. The browser extension is supported only on Mozilla Firefox 64.0 and later versions.

Before you begin, make sure that you have completed the following steps:

- Creating an MDM configuration profile to allow full-disk access for the endpoint security host application (SEHA.app) on macOS endpoints
- Creating an MDM configuration profile to allow full-disk access for the DLP Agent on macOS endpoints

1. Create a browser policy (`.plist` file) which you can upload to Jamf. Mozilla provides a template that you can use to define policies for the Firefox browser.

   NOTE

   For more information about Firefox policy templates, see https://github.com/mozilla/policy-templates/blob/master/README.md.

   To download the policy template, visit https://github.com/mozilla/policy-templates/blob/master/mac/org.mozilla.firefox.plist.

   You can either create a new `.plist` file based on Mozilla's policy template or modify the existing `.plist` file based on your organization's requirements. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>EnterprisePoliciesEnabled</key>
   <true/>
   <key>Certificates</key>
 <dict>
    <key>ImportEnterpriseRoots</key>
     <true/>
  </dict>
<key>ExtensionSettings</key>
  <dict>
    <key>InformationProtection@symantec.com</key>
    <dict>
      <key>installation_mode</key>
       <string>force_installed</string>
      <key>install_url</key>
      <string>file:////Library/Manufacturer/Endpoint Agent/dlp-firefox-addon.xpi</string>
    </dict>
  </dict>
</dict>
</plist>
```

2. In Jamf, select a configuration profile.
3. Navigate to **Application & Custom Settings**, and then click **Add**.
4. Under **Creation Method**, select **Upload File (PLIST file)**.
5. In the **Preference Domain** field, type `org.mozilla.firefox`.
6. Click the **Upload PLIST file** button, and then browse to and select the `.plist` file that you created in Step 1.
7. Click **Save**.

   NOTE
   You can refer to the **System > Agents > Overview** page of the Enforce Server administration console to view and troubleshoot any failed deployments.

Creating an MDM configuration profile to support monitoring in Google Chrome on macOS endpoints

The following instructions describe the process of creating an MDM configuration profile to deploy the new Google Chrome extension for macOS endpoints using MDM settings. For illustration purposes, the instructions assume that you plan to deploy the extension using Jamf, an IT management application.

Alternatively, you can install the extension manually using the Chrome Web Store. Make sure that the Chrome Web Store URL is not blocked by your organization's network firewall.

See https://chrome.google.com/webstore/detail/symantec-extension/egaejpfbkjamgheoingidhokbfnidlpi.

Before you begin, make sure that you have completed the following steps:

- Creating an MDM configuration profile to allow full-disk access for the endpoint security host application (SEHA.app) on macOS endpoints
- Creating an MDM configuration profile to allow full-disk access for the DLP Agent on macOS endpoints

1. Create a browser policy (`.plist` file) which you can upload to Jamf.

   For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>ExtensionSettings</key>
<dict>
 <key>egaejpfbkjamgheoingidhokbfnidlpi</key>
 <dict>
   <key>installation_mode</key>
   <string>force_installed</string>
   <key>update_url</key>
   <string>https://clients2.google.com/service/update2/crx</string>
 </dict>
 </dict>
</dict>
</plist>
```

2. In Jamf, select a configuration profile.
3. Navigate to **Application & Custom Settings**, and then click **Add**.
4. Under **Creation Method**, select **Upload File (PLIST file)**.
5. In the **Preference Domain** field, type `org.google.Chrome`.
6. Click the **Upload PLIST file** button, and then browse to and select the `.plist` file that you created in Step 1.
7. Click **Save**.

> **NOTE**
> You can refer to the **System > Agents > Overview** page of the Enforce Server administration console to view and troubleshoot any failed deployments.

DLP Agent monitoring limitations for macOS 11 endpoints

The following monitoring limitations apply to macOS 11 endpoints:

- Application File Access Control is not supported.
- Paste monitoring is not supported through Application File Access Control.

  NOTE
  When the re-release of 15.7 Maintenance Pack 2 is deployed on macOS 10.14 and 10.15, paste monitoring is not supported for apps that use Hardened Runtime.
- Cloud Storage monitoring is not supported.

Changes to endpoint incident snapshots

Symantec Data Loss Prevention 15.7 Maintenance Pack 2 introduces a new **Agent Response** indicator in endpoint incident snapshots.

A clock icon indicates that the DLP Agent did not block the user's action but the configured response action was not carried out due to a timeout in macOS 11.

Deprecation of legacy integration with Azure RMS

The initial (legacy) Data Loss Prevention integration with Azure RMS, which involves deploying a plug-in, is deprecated, and support will be removed in a release subsequent to Data Loss Prevention 15.8.

The initial integration supports file decryption and inspection only, and there is no support for decrypting and inspecting email. The initial integration is superseded by AIP Insight for Data Loss Prevention in DLP 15.7, and integration with Microsoft Information Protection in 15.8.

What's new and what's changed in Symantec Data Loss Prevention 15.7

For information on new and changed features, see *What's New and What's Changed in Symantec Data Loss Prevention 15.7* at the Broadcom Tech Docs Portal.

About the latest Update Readiness Tool version

The latest version of the Update Readiness Tool includes important fixes and improvements, and should be the version that you use before attempting an upgrade.

For more information, see Preparing to run the Update Readiness Tool at the Symantec Data Loss Prevention Help Center.

Installing or upgrading to Symantec Data Loss Prevention 15.7

Before installing or upgrading to Symantec Data Loss Prevention 15.7, see the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about system requirements.

When you are ready to install Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Installation Guide*.

Alternatively, when you are ready to install or upgradeSymantec Data Loss Prevention, see the *Symantec Data Loss Prevention Upgrade Guide*.

Both guides are available at the Broadcom Tech Docs Portal.

Oracle Database 19c migration advisory

Oracle has announced that Oracle Database 12c Release 2 (12.2.0.1) has a Patching End Date of November 20, 2020, followed by Limited Error Correction. Oracle strongly recommends migrating to Oracle 19c for product longevity and continued patching.

For Oracle support details, see https://support.oracle.com/knowledge/Oracle%20Database%20Products/742060_1.html.

Symantec will continue to support Oracle Database 12.2.0.1 for use with Data Loss Prevention 15.7 and previous releases. However, the support limitations for Oracle Database 12.2.0.1, as specified by Oracle, will be applicable.

Oracle Database 12.2.0.1 will not be supported for use with the next major release of Data Loss Prevention.

Oracle Database 19c is supported for use with Symantec Data Loss Prevention 15.1, 15.5, and 15.7. Symantec strongly recommends that you migrate your Symantec Data Loss Prevention database to Oracle Database 19c as soon as possible.

Fixed issues in 15.7 MP2

This section lists fixed issues in Symantec Data Loss Prevention 15.7 MP2.

Enforce Server fixed issues in 15.7 MP2

This table lists the fixed Enforce Server issues in 15.7 MP2.

Table 1: Enforce Server fixed issues fixed in 15.7 MP2

Issue ID	Description
None	Detection did not work correctly because of a redundant dependency on Microsoft Visual Studio 2010 Runtime.
DLP-31479	The response rule editor in the Enforce Server administration console took a long time to load when the database contained a large number of policies and response rules.
DLP-31501	Improved the performance of statistics reporting in JDBCLogger.
DLP-31741	After you edited and saved a policy group, the Enforce Server administration console would become unresponsive.
DLP-35191	The Enforce Server failed to communicate with the Network Discover ScanManager, which resulted in performance degradation.

Endpoint fixed issues in 15.7 MP2

This table lists the fixed Endpoint issues in 15.7 MP2.

Table 2: Endpoint fixed issues in 15.7 MP2

Issue ID	Description
DLP-35416	On Windows endpoints, the EDPA service stopped running if the Microsoft Edge Chromium browser extension was not installed because of environmental factors such as a corrupted local Group Policy Object (GPO).
DLP-34689	When you renamed a file in DropBox, a 0 KB file with the original file name was created.
DLP-34834	The certificates that are used by the DLP Agent installer for Windows and other executable files are now signed by Broadcom.
DLP-34849	HTTP/S incidents displayed an 'Unknown' URL when IBM Lotus Expeditor was running on endpoints.
DLP-34387	HTTPS incidents were created for file uploads in Microsoft Edge Chromium.
DLP-34030	HTTP/S incidents displayed an 'Unknown' URL for file uploads in Internet Explorer 11.
DLP-34662	Added support for HTTP/S monitoring in Microsoft Edge Chromium.
DLP-33907	Improved the tamper protection so that users cannot delete the the EDPA.exe service and the WDP.exe service.
DLP-33982	HTTP/S incidents displayed an 'Unknown' URL for file uploads when users draged and dropped files into Internet Explorer 11.

Detection fixed issues in 15.7 MP2

This table lists the fixed Detection issues in 15.7 MP2.

Table 3: Detection fixed issues in 15.7 MP2

Issue ID	Description
None	Detection did not work correctly because of a redundant dependency on Microsoft Visual Studio 2010 Runtime.
DLP-31740	During upgrades, LDAP and detection indexes (for IDM and EDM, for example) were not correctly replicated to cloud detectors.
DLP-33744	EDM policies failed to detect sensitive data that used Hebrew characters.
DLP-33973	If the subject line of an outgoing email contained an odd number of double quotation marks ("), any incident that was generated for that email contained invalid values.
DLP-33801	Under certain conditions, the EDM Prefilter would crash during replication. As a result, EDM profiles did not get updated.
DLP-33802	Pushing large Reusable Recipient/Sender Patterns to detection servers took a long time. This further resulted in long restart times for the detection servers.
DLP-35126	When an IDM profile was re-indexed, Endpoint Partial Matching would get disabled for all other IDM profiles.

Known issues in 15.7 MP2

Endpoint known issues in 15.7 MP2

This table lists the Endpoint known issues in 15.7 MP2.

Table 4: Endpoint known issues in 15.7 MP2

Issue ID	Description	Workaround
Multiple	Due to design limitations within the Microsoft Outlook add-in API, the new Outlook add-in is not invoked in certain situations which prevents emails from being monitored. The following issues on macOS endpoints describe the situations in which Outlook monitoring is not available: • DLP-27045: When you accept, decline, or tentatively accept a meeting invitation, the contents of your reply are not monitored. • DLP-27087: When you cancel a meeting, text contents of the cancellation and any attachments are not monitored. • DLP-27098: When you send an email with the **Draft > Encrypt > Do Not Forward** option enabled, the contents of the email are not monitored. • DLP-27131: When you share a document from Microsoft Word by clicking **File > Share > Send as HTML**, the generated email is not monitored. • DLP-27217: Error messages do not indicate when there is a network connectivity issue. • DLP-27218: If you edit an outgoing email while it is still in the Outbox folder, the updated email is not monitored. • DLP-27596: While using Microsoft Outlook Web Access (OWA), if you open the **Calendar** pane, click an existing meeting, and then forward it, the contents of the forwarded meeting invitation are not monitored. • DLP-27737: While replying to emails using OWA, if you do not click the ellipsis to expand the quoted conversation, the quoted conversation is not monitored. • DLP-27818: While using OWA, if you open the Calendar pane, click a date, and then create a meeting invitation using the dialog box that appears, the contents of the meeting invitation are not monitored. • DLP-27819: If you delete some attachments from an outgoing email while the add-in is still processing it, the contents of the remaining attachments are not monitored. • DLP-31871: After you enable the **New Outlook** option, monitoring is disabled.	For issue DLP-31871, see https://support.broadcom.com/external/content/product-advisories/DLP-not-monitoring-new-Outlook-for-Mac-with-workaround/16308. All of the issues have been reported to Microsoft, and a support ticket has been opened.

Table 5: Endpoint known issues in 15.7 MP2 continued...

Issue ID	Description	Workaround
DLP-29897	On macOS endpoints, when you save a .doc file to a network share using the Save As option, multiple empty folders are created in the file location.	Delete the empty folders that were created.
DLP-30011	On macOS endpoints, if you disable and then re-enable the Symantec Extension in Google Chrome, the DLP Agent becomes unable to monitor Chrome.	
DLP-30012	On macOS endpoints, when you use Google Chrome in incognito mode or guest mode or Mozilla Firefox in private mode, monitoring is unavailable. This behavior is expected because third-party browser extensions, such as Symantec Data Loss Prevention's browser extensions, are not loaded in incognito mode and private mode.	To resume monitoring, disable incognito mode and guest mode in Google Chrome and private mode in Mozilla Firefox via MDM settings.
DLP-35531	On macOS endpoints, the following warning message appears continuously in the `edpa_ext0.log` file: Crash Report is missing	
DLP-35560	On Windows endpoints, after the DLP Agent prevents you from uploading or dragging and dropping a sensitive file using Google Chrome or Microsoft Edge Chromium, if you close the web browser and then try to launch it again, the browser is terminated abruptly.	
DLP-35561	On Windows endpoints, print monitoring does not work when you try to print a web page or document from Google Chrome or Microsoft Edge Chromium.	

Known issues in 15.7

Enforce Server known issues

This table lists the Enforce Server known issues in 15.7.

Table 6: Enforce Server known issues in 15.7

Issue	Description	Workaround
4231954	As of version 15.0, Symantec Data Loss Prevention no longer supports anonymous logins to the SMTP server that is used for sending out alerts and reports. You must enter a valid user name and password.	Don't use anonymous login to the SMTP server that you use to send out alerts and reports.
4233351	Using a custom configuration file to change logging in **System > Servers and Detectors > Logs > Configuration** fails.	Don't use a custom configuration file to change logging in **System > Servers and Detectors > Logs > Configuration**.
4250348	An exception is returned when you select a duplicate column to query while authoring JSON for an incident list query with the REST API.	Use `filter` or `orderBY` with duplicate field names in the select part of the query.
4255382	If a user is already present when you run the script that sets up the user for DB Views, you will see this error: `DROP USER incident_view CASCADE * ERROR at line 1: ORA-01918: user 'INCIDENT_VIEW' does not exist`	Ignore this error.
4259399	Unsuccessful logins to the Enforce Server using the SOAP API are tagged "Authentication failed," but they do not appear in the audit log table. Successful logins do appear in the audit log table.	None.
4259685	The `krb5.ini` file does not include the additional domain details after upgrade from 14.6 to 15.7. Only the default domain value shows up in the `krb5.ini` file. Additional domains only show up in the list box on the **Settings** page.	Depend on the list box on the **Settings** page for the definitive list of additional domains.

Installation and upgrade known issues

This table lists the installation and upgrade known issues in 15.7.

Table 7: Installation and upgrade known issues in 15.7

Issue	Description	Workaround
DLP-31606	If an un-configured version of Symantec Data Loss Prevention 15.5 exists on a Linux server and you install version 15.7 (for the Enforce Server or detection servers), the services for version 15.7 do not start after you run the version 15.7 Configration Utility.	Complete the following to start services: 1. Uninstall the Symantec Data Loss Prevention 15.7 and 15.5 versions from servers. 2. Reinstall 15.7. 3. Run the Configuration Utility for the 15.7 system.
4173107	Running the Update Readiness Tool returns no errors but the upgrade process fails at the precheck phase.	Revert permissions changes made to the public role to their original state before running the Update Readiness Tool.
4227844	Uninstalling Symantec Data Loss Prevention does not remove it from the **Add/Remove Programs** list.	Complete the removal process on the **Add/Remove Programs** screen a second time to remove Symantec Data Loss Prevention from the list.
4247291	Users who use a custom `data_pump_dir` cannot run the Update Readiness Tool from the Enforce Server.	You can manually set the `data_pump_dir` location at the command line. Refer to the version 15.7 *Symantec Data Loss Prevention Upgrade Guide* for steps.
4247895	If you migrate Symantec Data Loss Prevention 14.0 to a PDB and RAC architecture and you convert LOB data from basicfile to securefile, the Enforce Server no longer connects to the database.	None.
4252447	Comments added to property files are not migrated during the upgrade process.	None.
4254666	If you upgraded to Symantec Data Loss Prevention 15.7 from version 14.6 and you use the same service user, you uninstall previous DLP versions, then attempt to restart services, services fail to start.	Complete the following to start services: 1. Right-click the version 15.7 service name and select **Properties**. 2. Click the **Log On** tab. 3. Enter (and re-enter) the service user password and click **OK**. 4. Restart the services.
4255764	If Symantec Data Loss Prevention 15.5 RPMs were installed for the Enforce Server or detection server, but the Update Configuration utility was not run, Symantec Data Loss Prevention 15.7 cannot be installed.	Uninstall version 15.5, and then perform a fresh installation of version 15.7.
4260204	Upgrading to Symantec Data Loss Prevention 15.7 causes the `wrapper.java.additional.18` property in `SymantecDLPManager.conf` to be commented out.	Update the property to include the original settings.

Solution Pack known issues

This topic describes known issues that you might face while importing Solution Packs as well as their workarounds.

State Data Privacy policies are not imported along with Solution Packs

When you import the following solution packs, State Data Privacy policies do not get imported:

- Financial Services Solution Pack
- Insurance Solution Pack
- Retail Solution Pack
- Media and Entertainment Solution Pack

To resolve the issue, you can manually import the State Data Privacy policies using the Enforce Server administration console after you finish importing all of the Solution Packs.

1. Navigate to **Manage > Policies > Policy List**.
2. On the Policy List screen, click **New**.
3. On the New Policy screen, select **Add a policy from a template** and click **Next**.
4. On the New Policy - Template List screen, select **State Data Privacy** in the **US Regulatory Enforcement** section and click **Next**.
5. On the Template State Data Privacy screen, click **Next** without changing any settings.
6. On the Configure Policy screen, click the **Policy Group** menu and select **Regulatory Enforcement**.
7. Click **Save**.

Detection known issues

This table lists the Detection known issues in 15.7.

Table 8: Detection known issues in 15.7

Issue	Description	Workaround
4247992	Importing newer policies into older DLP systems is unsupported. Importing new policies in old systems may result in inconsistent detection results and may also lead to database corruption if the policy uses rules or features that were introduced in the new release.	Don't import new policies into older DLP systems. For example, don't import policies created in 15.7 to 15.5 or 15.1 systems.
4257891	It is no longer possible to import a specific policy if the template was exported with data identifiers that have changed in a newer version of the Enforce Server. The Florida Drivers License data identifier is an example.	Don't import a specific policy into a new version of the Enforce Server if that template was created with an older version of the Enforce Server.

Discover known issues

This table lists the Discover known issues in 15.7.

Table 9: Discover known issues in 15.7

Issue	Description	Workaround
4254509	A user who does not have RBAC permissions to see Discover roots is logged out of the Enforce Server administration console in the following scenario: They drill down the Angular dashboard by navigating to **Discover incidents > Content Roots at Risk > Content Root**. There is no data loss or damaging behavior.	Users who do not have permission to access this data should not use this link.
4256325	After upgrading Symantec Data Loss Prevention to version 15.7, File System server scan targets that are assigned a Symantec ICE response action do not have pre-defined exclusion filters.	Edit the scan target and manually add the pre-defined exclusion filters.

Issue	Description	Workaround
4262818	After upgrading Symantec Data Loss Protection to version 15.7, the **Network Protect: SharePoint Release from Quarantine** smart reponse action does not release SharePoint List Items which were quarantined prior to 15.7. "Quarantine" and "Release from Quarantine" work fine in fresh installations of all versions of Data Loss Prevention Discover where "Quarantine" and "Release from Quarantine" are supported.	

Endpoint known issues

This table lists the Endpoint known issues in 15.7.

Table 10: Endpoint known issues in 15.7

Issue	Description	Workaround
4151955	On Windows endpoints, if a user attempts to upload multiple sensitive files to Firefox using drag and drop to a site that does not support drag and drop, then performs the same action with the same files to a site that supports drag and drop, block pop-ups display twice for each file and two incidents are logged for each upload attempt.	None.
4208190	On Windows endpoints, filters for HTTPS are not applied to files saved using a **Save As** operation from Microsoft Office applications to SharePoint or OneDrive.	Add * to the beginning and end of the HTTPs filter. For example, if the existing HTTPS filter is *-dav.box.com*, which correctly applies a filter to Internet Explorer and Firefox, add another filter to monitor **Save As** operations from Office apps: **dav.box.com**.
4248826	Users are unable to paste content to Internet Explorer from the Clipboard when Edge is monitored using the Application Monitoring feature.	None.
4248828	Opening a Microsoft Office file that contains sensitive data residing on a network share triggers an incident.	None.
4249161	Symantec Data Loss Prevention Endpoint Discover now supports the **Limit Incident Data Retention** response rule for eDAR scans on Microsoft Windows endpoints; however, you cannot use the **Limit Incident Data Retention** response rule in combination with any other response rule.	None.
4250243	If a user launches an application while logged on as another user (**Run as different user**) and attempts to upload sensitive information, an incident is generated as expected. However, no pop-up alert is displayed to the user, even if the response rule is configured to display a pop-up alert.	None.
4268115	If a user running macOS 10.15.4 saves a `.doc` file that contains sensitive data to a removable storage device, detection does not occur.	None.
4268116	If a user running macOS 10.15.4 uploads a sensitive file to Box using Safari, detection occurs, and a file with a zero byte size is uploaded to Box.	None.

Issue	Description	Workaround
4267712	If a user installs Firefox 74 for the first time with the DLP Agent running, URL filters do not work and Block and notify pop-ups display unknown for the URL when sensitive files are uploaded.	Complete the following to enable URL filters and URL information: 1. Uninstall Firefox 74. 2. Confirm that the DLP Agent is running on the endpoint and install Firefox 73. 3. Upgrade to Firefox 74.

Copyright statement


Symantec
A Division of Broadcom