Symantec Data Loss Prevention 15.7 Maintenance Pack 1 Release Notes

Version 15.7 MP1

Last updated: November 16, 2020

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.

About updates to the Symantec Data Loss Prevention 15.7 MP1 Release Notes

The known issues and workarounds that are described in these release notes are occasionally updated as new information becomes available.

The following table provides the history of updates to this version of the *Symantec Data Loss Prevention Release Notes*.

Table 1: Change history for the Symantec Data Loss Prevention 15.7 MP1 Release Notes

Date	Description
16 November 2020	Added the known issue (DLP-31606) applicable to users upgrading from version 15.5 to 15.7. See Table 7: Installation and upgrade known issues in 15.7.

About Symantec Data Loss Prevention 15.7 Maintenance Pack 1

Maintenance Packs such as 15.7 MP1 do not include new features, though additional platform support may be added for the Enforce Server, detection servers, and DLP Agents.

Because Maintenance Packs are restricted to defect fixes only, with no changes to features or the database schema, Symantec recommends that you apply Maintenance Packs immediately after they are released, and with minimal qualifying (as compared with other types of releases) in a Test environment. Applying a Maintenance Pack ensures that your Symantec Data Loss Prevention environment is up to date, and optimizes technical support for your deployment.

Other release types include the following:

- Major Release: Includes new features and functionality changes. Always includes database schema changes. Includes new SKUs. Example: 15.0.
- Minor Release: Includes new features and functionality changes. Usually includes database schema changes. Includes new SKUs. The scope of change in a Minor Release is typically not as extensive as in Major Releases. Example: 15.7.

Applying Symantec Data Loss Prevention 15.7 Maintenance Pack 1

Maintenance Packs can only be applied to an already installed version of Symantec Data Loss Prevention. This maintenance pack can only be applied to Symantec Data Loss Prevention 15.7 (new or upgraded installation).

> **NOTE**
> After upgrading DLP Agent to version 15.7 MP1 on endpoints running the Microsoft Windows 10 May 2020 (20H1) update, you might need to reboot the endpoints to enable monitoring and blocking for confidential files that are uploaded over HTTPS.

Before applying Maintenance Pack 1 or installing Symantec Data Loss Prevention 15.7, refer to the *Symantec Data Loss Prevention System Requirements and Compatibility Guide* for information about system requirements.

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

Both guides are available at the Broadcom Tech Docs Portal.

Important changes to language support

The Enforce Server management console is currently provided in multiple languages, including:

- English
- Brazilian Portuguese
- Spanish
- French
- Japanese
- German
- Italian
- Chinese (Traditional and Simplified)
- Korean
- Russian

This notice is to inform you that subsequent to Data Loss Prevention 15.7.x, only the following languages will be supported for the Enforce Server user interface and product documentation (online help and PDFs):

- English
- Brazilian Portuguese
- Spanish
- French
- Japanese

Support for other languages is deprecated. While language packs will be available for all languages in the release subsequent to 15.7.x, new text on existing pages or on new pages in the Enforce Server administration console will not be translated, and will appear in English, for these language packs:

- German
- Italian
- Chinese (Traditional and Simplified)
- Korean
- Russian

For those languages that are supported beyond version 15.7.x, as listed previously, all new text will be translated.

Longer term, Symantec may discontinue providing language packs for the deprecated languages.

> **NOTE**
> Product documentation, including online help and PDFs, was not translated for Data Loss Prevention 15.7.x. There will be translations for product documentation in subsequent releases, for the listed supported languages.

Symantec continually assesses customer requirements, so if your organization desires support for one of the deprecated languages, contact the Data Loss Prevention product team through Support or your account team. Symantec will consider your request and reevaluate the list of deprecated languages.

The deprecation of support for Enforce Server administration console languages does not affect other areas of Data Loss Prevention language support. You will continue to have the ability to detect sensitive data in all languages that are currently supported. You will also continue to be able to display the Endpoint notification pop-up dialog in all supported languages.

Updating the Team Identifier on endpoints deployed with MDM profiles

This Maintenance Pack includes DLP Agent drivers with new signatures. As a result, when you install this Maintenance Pack, you must also update the Team Identifier on endpoints that are deployed with Mobile Device Management (MDM) profiles.

To update the Team Identifer on endpoints deployed with MDM profiiles, follow these steps:

1. Configure a payload for *Kernel Extensions*.
2. Enable **Allow User Overrides** to allow users to approve kernel extensions.
3. Add the Team Identifier `Y2CCP3S9W7` as an Allowed Kernel Extension to the payload.

   If your environment includes endpoints deployed with an earlier version of the DLP Agent, and if you do not plan to upgrade these endpoints, do not remove the previous Team Identifier.
4. Save the payload.
5. Set the payload to deploy to all endpoints where the DLP Agent is installed.

Python 2.x is deprecated for Server FlexResponse plug-ins

As of this Maintenance Pack, Symantec Data Loss Prevention does not support Python 2.x for Server FlexResponse plug-ins. Administrators must port existing plug-ins to Python 3.x after installing this Maintenance Pack.

Network Discover/Cloud Storage Discover deprecated platforms

As of this Maintenance Pack, Network Discover/Cloud Storage Discover no longer supports scanning and detection for the following platforms:

- Microsoft Outlook Personal Folders (.pst files) that were created with Outlook 2010
- Network shares that reside on Microsoft Windows Server 2008 R2 SP1
- IBM Lotus notes 8.5.x
- Oracle 11.2 databases
- Microsoft SharePoint 2010 SP2
- Microsoft Exchange Server 2010 SP3

In addition, Network Discover/Cloud Storage Discover no longer supports the installation of scanners on 32-bit operating systems.

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.

About Update Readiness Tool failures

The Update Readiness Tool fails in the following scenarios:

- While running the tool after you have updated the Oracle version from 11g to a supported version of Oracle 12c. Confirm that you are running the same Oracle Client version as the Oracle Server version. If the versions do not match, the Oracle Client cannot connect to the database, which causes the Update Readiness Tool to fail.
- During the Update Readiness Tool database account creation process.
  To prevent this issue, reinstall the Oracle Client and select **Administrator** on the **Select Installation Type** panel. Selecting **Administrator** enables the command-line clients, expdp and impdp.

  NOTE

  The Oracle Client, available from the Oracle.com site, is only required for three-tier deployments.

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 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 MP1

This section lists fixed issues in Symantec Data Loss Prevention 15.7 MP1. Unless otherwise noted, all issues are fixed on the server side.

Enforce Server issues fixed in 15.7 MP1

This table lists fixed Enforce Server issues in 15.7 MP1.

Table 2: Enforce Server issues fixed in 15.7 MP1

Issue ID	Description
4254732	Match highlighting in incident snapshots involving a large amount of extracted content no longer cause a Java `OutOfMemoryError` exception.
4255900	While upgrading the Enforce Server on Linux, files in the `EnforceServerInstallationPath/Protect/tomcat/conf/` directory are no longer replaced. Previously, changing the files in this directory caused truststore and keystore issues.
4265972	While exporting a list of Network Discover incidents to a CSV file, all of the incidents that are displayed on the report page are now successfully exported, including any incidents that are related to deleted scans.
4265974	To prevent issues with file persistence, the `fileCreateDate` value and the `fileAccessDate` value of incident files are now limited to an acceptable date range in Oracle Database.
4265976	Improved performance while loading and displaying incident snapshots.
4265978	Deleting multiple policies simultaneously no longer creates orphaned CommandInfo records on the Enforce Server. In addition, performance optimizations in the Monitor Controller stop orphaned CommandInfo records from being sent to detectors and endpoints, which prevents wastage of CPU resources. This fix does not remove existing orphaned CommandInfo records.
4266691	When scheduled reports fail to be sent to certain SMTP recipients, system event reports correctly indicate which recipients did not receive the reports and whether the report succeeded by reaching at least one recipient. This optimized behavior is dependent upon the SMTP relay's ability to reject unknown or incorrect addresses upfront.
4266926	Incidents and their attachments can now be deleted.
4266939	The domains in the drop-down menu on the Enforce Server administration console logon screen are now listed in alphabetical order.
4267369	Resolved a security vulnerability while importing policies to prevent XML external entity injection attacks.
4267500	The Tomcat localhost logs on Microsoft Windows-based Enforce Servers now use the expected CR LF line delimiter instead of the Unix-style LF line delimiter.
4267964	Resolved a security vulnerability related to role-based access control in the Enforce Server administration console.
4268200	Previously, after an upgrade to version 15.1 and then to version 15.7, telemetry schedules prevented the Symantec DLP Manager service from starting. The Symantec DLP Manager service is no longer prevented from starting after the upgrade.

Issue ID	Description
4268240	Added the following role-based access control changes (RBAC): • Administrators with the Policy Author and User Administrator roles can access the **User Groups** page. However, policy authors cannot access user groups for roles that are managed through Microsoft Active Directory. • On the **User Groups** page, policy authors can view only the groups which are not currently associated with any role, policy,or policy rule, while user administrators can view all existing groups. • On the **Configure Role** page which is accessible only to user user administrators, only the groups which are not currently associated with any role, policy, or policy rule are displayed. • For Directory Group-based policies, on the **Configure Policy – Edit Rule** page, groups for roles that are managed through Microsoft Active Directory are not displayed, regardless of the administrator role. In addition, the **User Groups** page has been moved back under the **Manage > Policy** menu.
4268277	When a user logs on with multiple concurrent sessions using Kerberos Authentication, only failed authentications update the user record version number. Successful authentications no longer modify the version number and successive logins succeed.
4268515	While upgrading the Enforce Server on Linux, all of the files in the `EnforceServerInstallationPath/Protect/tomcat/webapps/ProtectManager/WEB-INFdirectory` are no longer replaced. Only the `struts-config- policy.xml` file is replaced. Previously, if the `springSecurityContext.xml` file was also replaced, administrators were unable to log on to the Enforce Server administration console.
4268517	You can now successfully add a DLP Agent to a group when the context involves an ON_CORPORATE_NETWORK EndpointLocation and PRINT_SCREEN DeviceType.
4268520	Added compatibility with Python 3.x for Server FlexResponse plug-ins.Note: Symantec Data Loss Prevention 15.7 MP1 does not support Python 2.x for Server FlexResponse plug-ins. Administrators must port existing plug-ins to Python 3.x after installing this Maintenance Pack.

Detection fixed issues in 15.7 MP1

This table lists fixed Enforce Server issues in 15.7 MP1.

Table 3: Detection fixed issues in 15.7 MP1

Issue ID	Description
4265302	If detection using OCR - Sensitive Image Recognition fails due to network connectivity or server communication issues, another attempt is now made automatically.
4265304	Connectivity issues with the OCR Server no longer generate authorization errors instead of connection errors.
4266003	Fixed an issue with the detector info update function so that the following error message no longer appears: Cloud Service is not available because of an account issue Added support for Adobe Extensible Metadata Platform (XMP) metadata extraction on detection servers.
4266454	Added support for Adobe Extensible Metadata Platform (XMP) metadata extraction on detection servers.
4266715	Improved the accuracy of detection for the Taiwan ROC ID data identifier.

Endpoint fixed issues in 15.7 MP1

This table lists fixed Endpoint issues in 15.7 MP1.

Table 4: Endpoint fixed issues in 15.7 MP1

Issue ID	Description
4263108	Resolved `edpa.exe` startup failures due to unhandled data identifier exception.
4264827	Added support for monitoring uploads to Microsoft OneDrive cloud storage from within Microsoft Office applications.
4267773	Kernel panics no longer occur on macOS 10.15.2 systems while using Apple Xcode.
4267856	When sensitive files are uploaded to remote shares over HTTPS using Internet Explorer, the incidents that are generated display **unknown** as the URL.
4268345	When Print channel monitoring is enabled in the agent configuration, web browsers and the Adobe PDF printer no longer crash when users attempt to print web pages to PDF files.
4268422	DLP Agent upgrades no longer fail on Microsoft Windows systems with `Access Denied` errors during the pre-installation cleanup step.
4268469	The Safari web browser on macOS 10.14 systems no longer generates incidents when users clear their browsing history,
4268595	Improved performance while opening files using the Safari browser on macOS endpoints.

Known issues in 15.7 MP1

Endpoint known issues in 15.7 MP1

This table lists the Endpoint known issues in 15.7 MP1.

Table 5: Endpoint known issues in 15.7 MP1

Issue ID	Description	Workaround
4263638	When you try to use the `create_package` utility on macOS 10.15.2 endpoints, the following error message appears: `Package creation failed!`	Copy the DLP Agent installer, certificates and the `create_package` utility to a directory other than the default installation directory, and then run the `create_package` utility.

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