What's New and What's Changed in Symantec™ Data Loss Prevention 15.7

Last updated: 27 February 2020

Symantec™
A Division of Broadcom

What's New and What's Changed in Symantec™ Data Loss Prevention 15.7

Documentation version: 15.7c

Legal Notice

Broadcom
1320 Ridder Park Drive
San Jose, California
95131

https://www.broadcom.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Introducing Symantec Data Loss Prevention 15.7

This chapter includes the following topics:

About this guide

The *What's New and What's Changed in Symantec Data Loss Prevention 15.7* guide describes new features and capabilities that are associated with the release. It also highlights changes relative to previous releases, including removal of features or supported platforms.

This guide does not contain implementation or configuration details for these new features. It provides an overview of each new feature in Symantec Data Loss Prevention 15.7, including, where appropriate, enough detail to help you understand how this feature is used. It also includes deployment information to help you plan for rolling out these new features to your organization.

Where possible, the guide provides pointers to further information about new and changed functionality.

For the complete Product Documentation Library for Symantec Data Loss Prevention 15.7, see https://support.symantec.com/us/en/article.DOC11597.html. See also the online Help at https://help.symantec.com/home/dlp15.7?locale=EN_US.

Summary of new and changed features

New and changed features in Symantec Data Loss Prevention 15.7 are summarized in the following tables. You can find more deployment details and explanations in chapter 2.

Endpoint features

Table 1-1 New and changed Endpoint features for Symantec Data Loss Prevention 15.7

Feature	Short description
LiveUpdate for keeping DLP Agents up to date	With LiveUpdate, you can easily keep your DLP Agents on Windows up to date with the latest hot fixes as soon as they are available. See "LiveUpdate for keeping DLP Agents up to date" on page 14.
Expanded platform support	The DLP Agent for macOS and Windows includes support for the following operating systems: ■ Windows Server 2019 ■ macOS 10.15 See "New operating system support" on page 15.
Summary data for Endpoint Discover Classification scans	You can view summary details of the numbers of tags used and policy violations for Endpoint Discover Classification scans on the Enforce Server administration console. See "Summary data for Endpoint Discover Classification scans" on page 15.
Support for monitoring file uploads to cloud locations from Microsoft Office 2019 and Office 365	The DLP Agent can monitor files saved from Microsoft Office 2019 applications and Office 365 to OneDrive, SharePoint, and WebDAV locations and edited using Box Edit. See "Support for monitoring file uploads through Microsoft Office 2019 and Office 365" on page 15.

Detection features

Table 1-2 New and changed Detection features for Symantec Data Loss Prevention 15.7

Feature	Short description
New and updated data identifiers and policy templates	Symantec Data Loss Prevention 15.7 includes 53 new data identifiers and four new policy templates, including a policy template for the new California Consumer Privacy Act (CCPA). Also included are updates to the existing GDPR policy templates. See "New and updated data identifiers and policy templates" on page 16.
New incident variables are available for REST response rules	New DLP incident variables are available for the following REST response rules: ■ **Email Notification** ■ **Send to Syslog** ■ **Quarantine** ■ **CSV Export** See "New incident variables are available for REST response rules" on page 18.
Optimized index distribution to endpoints for EMDI	EMDI index distribution to endpoints consumes less bandwidth than previously. See "Optimized index distribution to endpoints for EMDI" on page 19.

Discover features

Table 1-3 New and changed Discover features for Symantec Data Loss Prevention 15.7

Feature	Short description
Easier Symantec Data Access Governance deployment	In Symantec Data Loss Prevention 15.7, you do not have to download and install a separate plugin to integrate with Symantec Data Access Governance. See "Easier Symantec Data Access Governance deployment" on page 19.
Ability of detection servers to join ongoing grid scans	Assigned detection servers automatically join ongoing grid scans as soon as they become available. See "Ability of detection servers to join ongoing grid scans" on page 20.

Table 1-3 New and changed Discover features for Symantec Data Loss Prevention 15.7 *(continued)*

Feature	Short description
Configurable message re-delivery limits for grid scans	Make grid scans more resilient to File Reader restarts by configuring the number of times a message re-delivery can be attempted. See "Configurable message re-delivery limits for grid scans" on page 20.
Detailed reporting of scanned Microsoft Outlook Personal Folders during Network Discover scans	Network Discover scans now provide a more detailed breakdown of the number of scanned Microsoft Outlook Personal Folders (.pst files), including PST sub-items. See "Detailed reporting of scanned Microsoft Outlook Personal Folders during Network Discover scans" on page 20.
Network Discover error messages identify content extraction failures	Administrators can now use Network Discover error messages to determine when conent extraction failures are the reason for failed scans. See "Network Discover error messages identify content extraction failures" on page 21.
Enhanced Network Discover scan statistics	On the Scan Details screen, the **Scan Statistics** section has been updated to provide more useful information. In addition, some previously displayed fields are no longer available. See "Enhanced Network Discover scan statistics" on page 21.
Near real-time grid scan performance feedback	On the Scan Details screen, the **Recent Grid Status** section has been updated to display near real-time performance information about grid server and the participating detection servers in a grid scan. Administrators can use this information to identify and troubleshoot scan performance issues. See "Near real-time grid scan performance feedback" on page 21.

Networking features

Table 1-4 New and changed Networking features for Symantec Data Loss Prevention 15.7

Feature	Short description
Support for Npcap for Network Monitor	Npcap is added as an alternative to WinPcap for Network Monitor. See "Support for Npcap for Network Monitor" on page 23.

Enforce Server and platform features

Table 1-5 New and changed Enforce Server and platform features for Symantec Data Loss Prevention 15.7

Feature	Short description
New incident reporting APIs based on REST	The new Incident Reporting REST API provides easier implementation and expanded functionality compared to the original Incident Reporting and Update API, which was based on SOAP. See "New incident reporting APIs based on REST" on page 24.
Support for Oracle 12c Standard Edition 2 Release 1	You can deploy the Symantec Data Loss Prevention database on Oracle 12c Standard Edition 2 Release 1 (12.1.0.2). See "Support for Oracle 12c Standard Edition 2 Release 1" on page 24.
Support for Oracle multitenant Container Database (CDB)/Pluggable Database (PDB)	You can deploy the Symantec Data Loss Prevention database on Oracle multitenant database systems. See "Support for Oracle multitenant Container Database (CDB)/Pluggable Database (PDB)" on page 24.
Support for Oracle Real Application Clusters (RAC)	You can deploy the Symantec Data Loss Prevention database on Oracle Real Application Clusters (RAC) with Oracle 12.2.0.1 Enterprise Edition. See "Support for Oracle Real Application Clusters (RAC)" on page 25.
Ability to secure messages sent from the Enforce Server to a syslog server	You can secure communication using TLS over TCP encryption for messages sent from the Enforce Server to a syslog server. See "Ability to secure messages sent from the Enforce Server to a syslog server" on page 25.

Table 1-5 New and changed Enforce Server and platform features for Symantec Data Loss Prevention 15.7 *(continued)*

Feature	Short description
Enforce Server user authentication and role assignment using Active Directory	DLP administrators can use Active Directory groups to provide users with access to the Enforce Server administration console. See "Enforce Server user authentication and role assignment using Active Directory" on page 25.
Support for Chrome for Enforce Server access	You can use Chrome to access the Enforce Server administration console. See "Chrome as a supported browser for accessing the Enforce Server" on page 26.

Cloud features

Table 1-6 New and changed Cloud features for Symantec Data Loss Prevention 15.7

Feature	Short description
New Cloud Management Portal page	You can log on to your Cloud Management Portal through the Cloud Management portal page in the Enforce Server administration console. See "Cloud Management Portal" on page 26.

Removed and deprecated platforms and features

The following features are deprecated in or removed from Symantec Data Loss Prevention 15.7.

Table 1-7 Removed and deprecated platforms and features

Feature	Short description
Folder Risk Report	The Folder Risk Report is deprecated, and will no longer work when Adobe Flash reaches end-of-life in 2020. See "Folder Risk Report" on page 26.
Veritas Data Insight	As of September 30, 2019 customers are no longer able to purchase or renew Veritas Data Insight through Symantec. Our customers who have a valid maintenance contract will be supported through the end of that contract. See "Purchase of Veritas Data Insight from Symantec" on page 26.

Table 1-7 Removed and deprecated platforms and features *(continued)*

Feature	Short description
SOAP-based Incident Reporting API	The SOAP-based version of the Incident Reporting API and the Incident Data Views are deprecated in Data Loss Prevention 15.7. See "SOAP-based Incident Reporting and Update API, and Incident Data Views" on page 26.
Windows 7	DLP Agents are no longer supported on any version of Windows 7. See "Windows 7" on page 27.

Chapter 2

New and changed features in 15.7

This chapter includes the following topics:

Endpoint features

LiveUpdate for keeping DLP Agents up to date

Symantec LiveUpdate provides an easy way for you to obtain the latest hot fixes for DLP Agents on Windows, enabling you to keep your DLP Agents up to date.

You can enable the DLP Agents to receive the updates directly from Symantec, or you can control the update process from within your organization.

The Symantec LiveUpdate Administrator tool, which you can download from the Symantec Support site, is an enterprise web application that lets you manage Symantec updates on multiple internal LiveUpdate servers.

You download the updates from an external Symantec site to internal LiveUpdate Administrator servers, called Distribution Centers. You send the updates either immediately to a production distribution center for LiveUpdate clients to download, or to a testing center to test the updates. Once the updates have passed your testing requirements, they are sent to the production distribution center.

You can distribute the updates on a schedule, letting you create a low-maintenance, reliable system that can be set up once, and then run automatically. Updates can also be manually downloaded and distributed as needed.

For agent configurations, you configure settings for LiveUpdate in the Enforce Server administration console at the **System > Agents > Agent Configuration > Settings** page.

See LiveUpdate settings in the online Help for more information.

New operating system support

The DLP Agent supports the following operating systems:

- Windows Server 2019
- macOS 10.15

Summary data for Endpoint Discover Classification scans

When you run an Endpoint Discover classification scan, Symantec Data Loss Prevention collects the details of the tagging and displays the summary of tags and policy violations on the Enforce Server administration console.

You can also download full reports and view the tags applied, policies violated, and tags versus policy violation distribution details for each agent.

You can view the classification scan summary details for the following on the Enforce Server administration console:

- Top 5 counts of tags applied across all the agents
- Top 5 counts of policies violated across all the agents
- Top 5 tags versus policies violated across all the agents

For details, see the Help topic Endpoint Discover scan.

Support for monitoring file uploads through Microsoft Office 2019 and Office 365

The DLP Agent can monitor files saved from Microsoft Office 2019 applications and Office 365 to OneDrive, SharePoint, and WebDAV locations. Sensitive files that are blocked are saved on the endpoint.

The DLP Agent can monitor Microsoft Office files edited from Box using Box Edit.

Detection features

New and updated data identifiers and policy templates

Symantec Data Loss Prevention includes the following new data identifiers:

- BosniaHerzegovina Unique Master Citizen Number
- Brazil RG Number
- Canada Government Identification Card Number
- Chile Driver License Number
- Driver License Number - CT State
- Driver License Number - Guam
- Driver License Number - IN State
- Driver License Number - KS State
- Driver License Number - KY State
- Driver License Number - MA State
- Driver License Number - MD State
- Driver License Number - MO State
- Driver License Number - MS State
- Driver License Number - MT State
- Driver License Number - ND State
- Driver License Number - NE State
- Driver License Number - NH State
- Driver License Number - OH State
- Driver License Number - RI State
- Driver License Number - VA State
- Driver License Number - VT State
- Driver License Number - WV State
- Driver's License Number - AK State
- Driver's License Number - AZ State

- Driver's License Number - DC State
- Driver's License Number - HI State
- Driver's License Number - IA State
- Driver's License Number - ID State
- Driver's License Number - OK State
- Driver's License Number - OR State
- Driver's License Number - U.S. Virgin Islands
- Kosovo Unique Master Citizen Number
- Macedonia Unique Master Citizen Number
- Mexico Passport Number
- Montenegro Unique Master Citizen Number
- Norway Health Insurance Card Number (HICN)
- Russia Cargo Customs Declaration
- Russia Employment Record
- Russia Insurance Account Number (SNILS)
- Russia OMS Number
- Russia Military Identity Number
- Turkey Local Phone Number
- Turkey Mobile PhoneNumber
- Turkey Passport Number
- Turkey Tax Identification Number
- Turkey Value Added Tax (VAT) Number
- US Adoption Taxpayer Identification Number
- US Preparer Taxpayer Identification Number
- Vehicle Identification Number
- Venezuela Driver License Number
- Venezuela Value Added Tax (VAT) Number
- Vojvodina Unique Master Citizen Number

Symantec Data Loss Prevention includes the following new policy templates:

- California Consumer Privacy Act

- Russian Federal Law on Personal Data (No. 152-FZ)
- Turkish Personal Data Protection Law 6698
- US States Driver's License Number

Symantec Data Loss Prevention includes updates to the following policy templates:

- **General Data Protection Regulation (Banking and Finance)**: Added new European data identifiers.
- **General Data Protection Regulation (Government Identification)**: Added new European data identifiers.
- **General Data Protection Regulation (Healthcare and Insurance)**: Added new European data identifiers.

New incident variables are available for REST response rules

New incident variables are available for the following response rules:

- **Send to Syslog**
- **Send Email Notification**
- **Quarantine**
- **CSV Export**

The following new variables are available for the **Send to Syslog** and the **Send Email Notification** response rules:

- **$DOCUMENT_ID$**
- **URL**
- **$AWS_ACCOUNT_ID$**
- **$AWS_PRINCIPAL_ID$**
- **AWS_BUCKET_NAME**
- **$AWS_ACCOUNT_NAME$**
- **AWS_REGION**
- **$ROOM$**
- **$SPACE$**
- **$POLICY DESCRIPTION$**
- **$POLICY_LABEL$**

- **Note:** The variables **$POLICY DESCRIPTION$** and **$POLICY_LABEL$** are not available in the user interface and must be entered manually.

The following new variables are available for the **Quarantine** and the **CSV Export** response rules:

- **$DOCUMENT_ID$**
- **URL**
- **$AWS_ACCOUNT_ID$**
- **$AWS_PRINCIPAL_ID$**
- **AWS_BUCKET_NAME**
- **$AWS_ACCOUNT_NAME$**
- **AWS_REGION**
- **$ROOM$**
- **$SPACE$**

See REST incident variables in the online Help.

Optimized index distribution to endpoints for EMDI

When an EMDI index is updated, the endpoints receive only the data that is different between the old index and the new. This saves bandwidth utilization especially when the index updates are deployed in environments with a large number of endpoints.

For more information see About the Exact Match Data Identifer profile and index in the online Help.

Discover features

Easier Symantec Data Access Governance deployment

Symantec Data Access Governance lets customers manage and control access to structured and unstructured data, systems, and applications. Symantec Data Access Governance StealthAUDIT provides file owner and access information similar to the existing integration with Veritas Data Insight.

In the initial release of Data Access Governance, for Data Loss Prevention 15.1 and 15.5, a separate FlexResponse plugin had to be downloaded and installed. In Data Loss Prevention 15.7, you do not have to download a separate plugin for either installation or upgrade. The plugin is automatically included, although you still need to configure the plugin to use Data

Loss Prevention with StealthAUDIT. As in the previous release of Data Access Governance, you also have to install StealthAUDIT separately.

For detailed information about Symantec Data Access Governance and how to implement it with Symantec Data Loss Prevention, see the Product Guides for Symantec Data Loss Prevention Data Access Governance.

Ability of detection servers to join ongoing grid scans

Busy detection servers join ongoing grid scans as soon as they become available. This enhancement reduces the idle time of detection servers, and enables scheduled grid scans to start on time and run at full capacity as much as possible.

If a detection server is assigned to more than one scan target, it joins the ongoing grid scan that started first.

Configurable message re-delivery limits for grid scans

In previous versions of Symantec Data Loss Prevention, if the File Reader restarted during a grid scan, queued items were sometimes not scanned or messages were removed from the queue without being processed. Such occurrences sometimes resulted in errors being generated for those missed files..

To prevent such issues from occurring, administrators can set the following new property in the `crawler.properties` file on each detection server to configure how many times a message re-delivery is attempted following a File Reader restart:

```
crawler.scanqueue.item.max.redeliveries
```

Detailed reporting of scanned Microsoft Outlook Personal Folders during Network Discover scans

Network Discover Drid scans now provide a more detailed breakdown of the number of scanned Microsoft Outlook Personal Folders (.pst files).

On the Scan Details screen, in the **Scan Statistics** section, the number of scanned `.pst` files is now reported by the new **Total PST Items** scan statistic. In addition, the number of scanned PST items is incremented by 1 only after all of the sub-items within a particular PST item are processed.

The number of scanned PST sub-items is reported separately using the **PST Subitems Scanned** scan statistic, and the number of failed PST sub-item scans is reported using the **PST Errors** scan statistic.

See “Enhanced Network Discover scan statistics” on page 21.

Network Discover error messages identify content extraction failures

Network Discover error messages now indicate when content extraction failure is the reason for failed scans.

For example, the following error message is displayed when content extraction fails for a particular file that exceeds the configured size limit:

```
Failed to extract content from truncated file exceeding the maximum file size.
```

Enhanced Network Discover scan statistics

On the Scan Details screen, the **Scan Statistics** section provides a more detailed breakdown of processed items which enables administrators to better understand the scope of a scan as well as its outcome. Some scan statistics have been replaced with more useful information and are no longer provided.

The following scan statistics are no longer displayed:

Scan statistic	Description	Reason for removal
Bytes Scanned	Number of bytes scanned.	Renamed to **Bytes Downloaded**.

The following new scan statistics have been added:

Scan statistic	Description
Total Items Considered	Total number of processed items, including those that could not be scanned.
Total PST Items	Number of `.pst` files processed.
PST Subitems Scanned	Number of PST sub-items scanned.
PST Errors	Number of errors that occurred while scanning PST sub-items.

Near real-time grid scan performance feedback

On the Scan Details screen, the **Recent Grid Status** section now includes additional columns that display near real-time information about the performance of the grid leader and each participating grid follower. Using this information, administrators can troubleshoot the ongoing scan and as well as plan to improve the performance of future grid scans.

The following performance information is displayed about the grid leader:

Performance parameter	Description	Performance impact
Wait Time	The total amount of time elapsed since the start of the scan during which the grid leader pauses file crawling while the grid followers perform detection and remediation on crawled files.	A lower value is better. Non-zero values indicate that there might be too few participating grid followers.
Wait Time (Last Hour)	The average amount of time elapsed over the preceding hour during which the grid leader pauses file crawling while the grid followers perform detection and remediation on crawled files.	
CPU Usage %	The total processor usage.	Used to track the grid leader throughput with respect to filtering.

The following performance information is displayed about each participating grid follower:

Performance parameter	Description	Performance impact
Download Rate	The average file download speed since the start of the scan.	A higher value is better. A low value indicates that the network, a file share server, or a Microsoft SharePoint repository might be experiencing latency.
Download Rate (Last Hour)	The average file download speed over the preceding hour.	
Access Time - Fetch	The average time taken to retrieve the value of the `Last Accessed` attribute of processed files.	A higher value is better. A low value indicates that the network, a file share server, or a Microsoft SharePoint repository might be experiencing latency.
Access Time - Reset	The average time taken to reset the `Last Accessed` attribute of processed items to the original value.	
Access Time (Last Hour) - Fetch	The average time taken to retrieve the value of the `Last Accessed` attribute of processed files over the preceding hour.	A lower value is better. A high value indicates that the network, a file share server, or a Microsoft SharePoint repository might be experiencing latency.
Access Time (Last Hour) - Reset	The average time taken to reset the `Last Accessed` attribute of processed items to the original value over the preceding hour.	

Performance parameter	Description	Performance impact
CPU Usage %	The total processor usage.	A high value is better. Values less than 80% indicate that the grid leader might be affecting grid scan performance.
CPU Usage % Over Last Hour	The average processor usage over the preceding hour.	

Ideally, the grid leader **Wait Time** should be 0 and the **CPU Usage %** for participating grid followers should be close to 80%.

"Last Hour" fields are populated for the first time one hour after the grid scan is initialized. Thereafter, these fields are updated at configurable intervals unless a particular detection server does not report its performance data on time.

Performance data for the participating detection servers is calculated and stored on the individual detection servers before being reported to the grid leader. However, if the grid leader changes during the scan, the values of all "Over Last Hour" fields is are reset to zero.

To set the update intervals for the grid scan performance feedback, administrators can configure the following properties:

- `crawler.gridperformancelog.enabled` — Toggles performance logging for grid scans. The default value is `True`.
- `crawler.gridperformancelog.updatefrequency.millis` — The frequency in milliseconds with which the **Recent Grid Status** section is updated. The default value is `900000` (15 minutes).
- `crawler.gridperformancelog.cpuusage.query.interval.millis` — The frequency in milliseconds with which CPU usage data is collected on the grid followers. The default value is `5000` (5 seconds).
- `crawler.gridperformancelog.cpuusage.reporting.interval.millis` — The frequency in milliseconds with which the grid followers send their CPU usage data to the grid leader. The default value is `30000` (30 seconds).

Networking features

Support for Npcap for Network Monitor

Npcap is added as an alternative to WinPcap for Network Monitor. You can use either WinPcap or Npcap for Network Monitor in Symantec Data Loss Prevention version 15.7.

See Installing WinPcap or Npcap on a Windows platform in the online Help.

Enforce Server and platform features

New incident reporting APIs based on REST

Data Loss Prevention 15.7 makes available a set of public RESTful APIs for incident reporting. You can use the REST APIs to integrate incident data with other applications to provide dynamic reporting, create a custom incident remediation process, or support business processes that rely on DLP incidents.

The new REST APIs replace the capabilities of the Incident Reporting and Update API, which was based on SOAP technology. REST APIs are generally better performing and easier to use that SOAP-based APIs. While the SOAP-based APIs for incident reporting are still supported, new integrations requiring custom incident reporting should leverage the REST-based APIs. The Incident Reporting and Update SOAP APIs are deprecated in Data Loss Prevention 15.7.

For more information about the incident reporting REST APIs, refer to the DLP 15.7 REST API documentation.

Support for Oracle 12c Standard Edition 2 Release 1

You can deploy the Symantec Data Loss Prevention database on Oracle 12c Standard Edition 2 Release 1 (12.1.0.2).

For detailed information about installing and upgrading the Symantec Data Loss Prevention database on Oracle Standard Edition 2 Release 1, see the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Installation and Upgrade Guide* at https://www.symantec.com/docs/DOC10713.

Support for Oracle multitenant Container Database (CDB)/Pluggable Database (PDB)

You can deploy the Symantec Data Loss Prevention database on Oracle multitenant database systems. Multitenant databases are supported on the following Oracle versions:

- 12.1.0.2 Standard Edition
- 12.1.0.2 Enterprise Edition
- 12.2.0.1 Standard Edition
- 12.2.0.1 Enterprise Edition

For detailed information about installing the Oracle multitenant database on Oracle 12.1.0.2 or 12.2.0.1 Standard Editions, see the *Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Installation and Upgrade Guide* at https://www.symantec.com/docs/DOC10713.

For detailed information about installing the Oracle multitenant database on Oracle 12.1.0.2 or 12.2.0.1 Enterprise Editions, see the *Symantec Data Loss Prevention Oracle 12c Enterprise Implementation Guide* at https://www.symantec.com/docs/DOC9260.

Support for Oracle Real Application Clusters (RAC)

You can deploy the Symantec Data Loss Prevention database on Oracle Real Application Clusters (RAC) with Oracle 12.2.0.1 Enterprise Edition.

For detailed information about configuring the Symantec Data Loss Prevention Oracle RAC database on Oracle 12.2.0.1 Enterprise Edition, see the *Symantec Data Loss Prevention Oracle 12c Enterprise Implementation Guide* at https://www.symantec.com/docs/DOC9260.

Ability to secure messages sent from the Enforce Server to a syslog server

You can secure communication using TLS over TCP encryption for messages sent from the Enforce Server to a syslog server. Messages include those sent as a result of the Log to a Syslog Server response rule action and when the Enforce Server logs system events.

To enable encryption for the Log to a Syslog Server response rule action, select TCP and enable the TLS client authentication if necessary. To enable encryption for system events, update the `Manager.properties` file (located in the `\config` directory on the Enforce Server) to include the new line:

```
systemevent.syslog.protocol = [ udp | tcp | tls ]
```

See Enabling a syslog server in the online Help for detailed steps for enabling encryption.

Enforce Server user authentication and role assignment using Active Directory

DLP administrators can use Active Directory groups to provide users with access to the Enforce Server administration console.

To use the feature, DLP administrators create a directory connection between the Enforce Server and the company's Active Directory (AD) server. After creating the connection, administrators create a user group that defines the common names that exist in the AD. The group defines the roles that are applied to the users to be added to the Enforce Server. Finally, the administrator imports the AD users defined in the user group using a sync job.

If you are upgrading to Symantec Data Loss Prevention version 15.7, users in previous Symantec Data Loss Prevention versions are reconciled after the DLP administrator creates an AD-managed role and synchronizes users. Symantec Data Loss Prevention automatically converts users to an AD-managed role based on the username.

Note: If a user does not exist in AD, the user is deleted when the AD sync job runs.

For info on setting up user authentication using AD, see the online Help topic Configuring user authentication and role assignment using Active Directory.

For a video that walks through the steps to set up user authentication using AD, see the online help topic Steps to use AD to provide user access to the Enforce Server administration console.

Chrome as a supported browser for accessing the Enforce Server

You can access the Enforce Server administration console using Chrome.

Cloud features

Cloud Management Portal

The Symantec Data Loss Prevention Cloud Management Portal is now available at **System > Settings > Cloud Management Portal** in the Enforce Server administration console. You can log on to your Cloud Management Portal account from this page to perform initial setup and view a list of your purchased cloud services.

See Using the Cloud Management Portal in the online Help.

Removed and deprecated platforms and features

This following features are removed or deprecated in Symantec Data Loss Prevention 15.7, as noted for each item.

Folder Risk Report

The **Folder Risk Report** is deprecated, and will no longer work when Adobe Flash reaches end-of-life in 2020.

Purchase of Veritas Data Insight from Symantec

Symantec no longer sells Veritas Data Insight as of September 30, 2019.

SOAP-based Incident Reporting and Update API, and Incident Data Views

The SOAP-based version of the Incident Reporting and Update API and Incident Data Views are deprecated.

Windows 7

Microsoft ended Windows 7 support on 14 January, 2020. Because Microsoft is ending support, Symantec no longer supports DLP Agents running on Windows 7 systems.