

# What's New and What's Changed in Symantec™ Data Loss Prevention 14.6



# What's New and What's Changed in Symantec Data Loss Prevention 14.6

Documentation version: 14.6

Last updated: 05 December 2016

## Legal Notice

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation  
350 Ellis Street  
Mountain View, CA 94043

<http://www.symantec.com>

# Contents

Chapter 1	Introducing Symantec Data Loss Prevention 14.6 .....	6
	About this guide .....	6
	Summary of new and changed features in Symantec Data Loss Prevention 14.6 .....	7
	Endpoint features .....	7
	Cloud features .....	9
	Discover features .....	9
	Enforce Server features .....	10
	Network features .....	11
	Detection features .....	11
	Deprecated features .....	12
Chapter 2	New and Changed Features in Symantec Data Loss Prevention 14.6 .....	14
	Endpoint features .....	14
	Mac and Windows endpoint features .....	14
	Mac endpoint features .....	17
	Windows endpoint features .....	19
	Cloud features .....	20
	Ability to target policies to specific cloud connectors .....	20
	New reporting page for cloud connector incidents .....	20
	Contextual attributes for cloud connector detection rules .....	20
	Discover features .....	20
	Improved authorization for cloud storage targets .....	20
	SharePoint 2016 Discover target .....	21
	Network features .....	21
	Support for using a generic 10 GB Ethernet card with Network Monitor .....	21
	Detection features .....	21
	Form Recognition enabled by default .....	21
	Support for detecting electronically fillable forms .....	22
	Support for monitoring Microsoft Rights Management files .....	22
	New enhancements to regular expressions .....	23

Additional variables for the Log to a Syslog Server and Send Email	
Notification response actions .....	23
New European General Data Protection Regulations (GDPR)	
policy templates .....	24
Updated HIPAA and HITECH (Including PHI) policy	
template .....	24
New and updated data identifiers .....	24
Enforce Server features .....	25
Support for Windows Server 2016 .....	25
Cloud server maintenance alerts available on Enforce Server	
administration console .....	25
Support for managing servers using a domain service user .....	26
Cloud Authorization page .....	26
Oracle 12c database template .....	26
Database space reclamation utility .....	26
Improved Policy List page .....	26
Deprecated features .....	27

# Introducing Symantec Data Loss Prevention 14.6

This chapter includes the following topics:

- [About this guide](#)
- [Summary of new and changed features in Symantec Data Loss Prevention 14.6](#)

## About this guide

The *What's New and What's Changed in Symantec Data Loss Prevention 14.6* guide describes new features and capabilities associated with the release, and 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 14.6, including, where appropriate, enough detail to help you understand how this feature can be 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.

# Summary of new and changed features in Symantec Data Loss Prevention 14.6

## Endpoint features

**Table 1-1** New and changed features for Endpoint for Symantec Data Loss Prevention 14.6

Feature	Description
Support for excluding printers from monitoring	Printers, including local, network, and PDF, can be excluded from monitoring.  See <a href="#">“Support for excluding printers from monitoring”</a> on page 15.
Support for monitoring specific channels using Application Monitoring	Ability to enable or disable specific Application Monitoring channels.  See <a href="#">“Support for monitoring specific channels using Application Monitoring”</a> on page 15.

**Table 1-2** New and changed features for Mac Endpoints for Symantec Data Loss Prevention 14.6

Feature	Description
Support for monitoring macOS 10.11.6	Support for monitoring endpoints running macOS 10.11.6.  See <a href="#">“Support for monitoring Mac OS 10.11.6”</a> on page 17.
Support for monitoring macOS 10.12	Support for monitoring endpoints running macOS 10.12.  See <a href="#">“Support for monitoring macOS 10.12”</a> on page 17.
Support for file restoration on Mac endpoints	Ability to restore the original, non-sensitive, file in the event it is overwritten with a newer file that contains confidential data.  See <a href="#">“Support for file restoration on Mac endpoints”</a> on page 17.
Monitoring Outlook 2016 running on Mac endpoints	DLP Agents can monitor data moved through Outlook 2016 running on Mac endpoints.  See <a href="#">“Monitoring Outlook 2016 running on Mac endpoints”</a> on page 18.

**Table 1-2**      New and changed features for Mac Endpoints for Symantec Data Loss Prevention 14.6 *(continued)*

Feature	Description
Ability to monitor System Integrity Protection (SIP) on Mac endpoints	<p>Applications protected by System Integrity Protection (SIP) on macOS 10.11 through 10.11.6 and macOS 10.12 endpoints are monitored.</p> <p>See <a href="#">“Ability to monitor System Integrity Protection (SIP) on Mac endpoints”</a> on page 18.</p>

**Table 1-3**      New and changed features for Windows Endpoints for Symantec Data Loss Prevention 14.6

Feature	Description
Support for monitoring endpoints on Citrix 7.9	<p>Support for monitoring endpoints running on Citrix 7.9.</p> <p>See <a href="#">“Support for monitoring endpoints on Citrix 7.9”</a> on page 19.</p>
Increased monitor coverage for Citrix	<p>Support for scanning Microsoft Office files, restoring files on Citrix drives, and monitoring files accessed by applications.</p> <p>See <a href="#">“Increased monitor coverage for Citrix”</a> on page 19.</p>
Support for monitoring Microsoft Windows 10 Anniversary Update Enterprise, Pro 64-bit PC	<p>Support for monitoring the Microsoft Windows 10 Anniversary Update Enterprise, Pro 64-bit PC operating system.</p> <p>See <a href="#">“Support for monitoring Microsoft Windows 10 Anniversary Update Enterprise, Pro 64-bit PC”</a> on page 19.</p>
Support for monitoring Windows 10 endpoints using 64-bit Firefox	<p>Support for monitoring Firefox on Windows 10 64-bit.</p> <p>See <a href="#">“Endpoint Prevent monitor support for Firefox 64-bit”</a> on page 19.</p>
Support for monitoring uploads by Microsoft Edge	<p>Support for monitoring file content uploaded through the Microsoft Edge browser over the HTTPS protocol.</p> <p>See <a href="#">“Support for monitoring uploads to Microsoft Edge”</a> on page 19.</p>



## Cloud features

**Table 1-4** New and changed features for Cloud for Symantec Data Loss Prevention 14.6

Feature	Description
Ability to target policies to specific cloud connectors	<p>You can target policies to specific cloud connectors, such as Gatelets and Securlets provided by Symantec CloudSOC.</p> <p>See <a href="#">“Ability to target policies to specific cloud connectors”</a> on page 20.</p>
New reporting page for cloud connector incidents	<p>You can view incident reports for DIM and DAR cloud connector incidents on the <b>Incidents &gt; Cloud Connectors</b> page.</p> <p>See <a href="#">“New reporting page for cloud connector incidents”</a> on page 20.</p>
Contextual attributes for cloud connector detection rules	<p>You can specify contextual attributes for cloud connector detection rules.</p> <p>See <a href="#">“Contextual attributes for cloud connector detection rules”</a> on page 20.</p>

## Discover features

**Table 1-5** New and changed features for Discover for Symantec Data Loss Prevention 14.6

Feature	Description
Support for Microsoft SharePoint 2016 targets	<p>Network Discover now supports SharePoint 2016 as a scan target.</p> <p>See <a href="#">“SharePoint 2016 Discover target”</a> on page 21.</p>
Improved authorization for cloud storage targets	<p>The authorization procedures for Box and Dropbox Business targets have changed to make them more manageable and secure.</p> <p>See <a href="#">“Improved authorization for cloud storage targets”</a> on page 20.</p>

## Enforce Server features

**Table 1-6** New and changed features for Enforce Server for Symantec Data Loss Prevention 14.6

Feature	Description
Support for Windows Server 2016	Windows Server 2016 is certified as a supported platform for the Enforce Server.  See <a href="#">“Support for Windows Server 2016”</a> on page 25.
Support for automatic notifications of cloud service issues as alerts	Cloud server maintenance and outage events can be automatically displayed in the Enforce Server administration console as system events.  See <a href="#">“Cloud server maintenance alerts available on Enforce Server administration console”</a> on page 25.
Support for managing servers using a domain service user	You can access and manage the Enforce Server and detection servers using a domain user. Upgrading users can use the ChangeServiceUser utility to update existing local service users to domain servers.  See <a href="#">“Support for managing servers using a domain service user”</a> on page 26.
Cloud Authorization page	You can create and manage authorizations for connecting to cloud storage repositories on the Cloud Authorization page.  See <a href="#">“Cloud Authorization page”</a> on page 26.
Database space reclamation utility	You can use the new database space reclamation utility to reclaim unused tablespaces in the Symantec Data Loss Prevention Oracle database.  See <a href="#">“Database space reclamation utility”</a> on page 26.
Oracle 12c database template	You can use this database template to create the Symantec Data Loss Prevention Oracle database on Oracle 12c Enterprise more quickly and easily.  See <a href="#">“Oracle 12c database template”</a> on page 26.
Improved Policy List page	The improved Policy List page lets you manage you policies more efficiently.  See <a href="#">“Improved Policy List page”</a> on page 26.
Increased character limit for Active Directory domain name list	The Active Directory domain name list now supports domain names up to 2048 characters long.

**Table 1-6**      New and changed features for Enforce Server for Symantec Data Loss Prevention 14.6 *(continued)*

Feature	Description
Increased data limit on syslog messages	Symantec Data Loss Prevention supports syslog messages up to 64 kilobytes.

## Network features

**Table 1-7**      New and changed features for Network for Symantec Data Loss Prevention 14.6

Feature	Description
Support for using a generic 10 GB Ethernet card with Network Monitor	See <a href="#">“Support for using a generic 10 GB Ethernet card with Network Monitor”</a> on page 21.

## Detection features

**Table 1-8**      New and changed features for Detection for Symantec Data Loss Prevention 14.6

Feature	Description
Form Recognition enabled by default	Form Recognition is enabled by default for customers licensed to use Form Recognition, and forms are monitored on demand.  See <a href="#">“Form Recognition enabled by default”</a> on page 21.
Support for detecting forms with electronically fillable fields	The Form Recognition feature detects PDF files that contain electronically fillable fields.  See <a href="#">“Support for detecting electronically fillable forms”</a> on page 22.
Support for monitoring Microsoft Rights Management files	Symantec Data Loss Prevention can detect files that are encrypted using Microsoft Rights Management Services (RMS) and administered through Azure or Active Directory. It can also inspect content within RMS-protected files.  See <a href="#">“Support for monitoring Microsoft Rights Management files”</a> on page 22.

**Table 1-8**      New and changed features for Detection for Symantec Data Loss Prevention 14.6 (*continued*)

Feature	Description
New enhancements to regular expressions	Regular expressions are now evaluated consistently on both the server and on the endpoint. Performance improvements for regular expressions conditions significantly reduce the detection time on the server and on the endpoint. In addition, the new regular expression engine is optimized for the "no match" use case and skips zero-length matches as a valid match.  See <a href="#">"New enhancements to regular expressions"</a> on page 23.
Additional variables for the <b>Log to a Syslog Server</b> and <b>Send Email Notification</b> response actions	Symantec Data Loss Prevention includes several new incident variables that you can use in the <b>Log to a Syslog Server</b> and <b>Send Email Notification</b> response actions.  See <a href="#">"Additional variables for the Log to a Syslog Server and Send Email Notification response actions"</a> on page 23.
New European General Data Protection Regulations (GDPR) policy templates	Symantec Data Loss Prevention includes several policy templates for European GDPR policy detection.  See <a href="#">"New European General Data Protection Regulations (GDPR) policy templates"</a> on page 24.
Updated HIPAA and HITECH (Including PHI) policy template	The <b>HIPAA and HITECH (Including PHI)</b> policy template has been updated to include keywords for ICD 10 codes.  See <a href="#">"Updated HIPAA and HITECH (Including PHI) policy template"</a> on page 24.
New and updated data identifiers	Symantec Data Loss Prevention 14.6 includes several new and updated data identifiers.  See <a href="#">"New and updated data identifiers"</a> on page 24.

## Deprecated features

**Table 1-9**      Deprecated features for Symantec Data Loss Prevention 14.6

Feature	Description
Mobile Prevent for Web	Mobile Prevent for Web is deprecated in DLP 14.6 and will be removed in a future release.

**Table 1-9** Deprecated features for Symantec Data Loss Prevention 14.6  
(continued)

Feature	Description
Mobile Email Monitor	Mobile Email Monitor is deprecated in DLP 14.6 and will be removed in a future release.

# New and Changed Features in Symantec Data Loss Prevention 14.6

This chapter includes the following topics:

- [Endpoint features](#)
- [Cloud features](#)
- [Discover features](#)
- [Network features](#)
- [Detection features](#)
- [Enforce Server features](#)
- [Deprecated features](#)

## Endpoint features

Symantec Data Loss Prevention enables you to monitor both Windows and Mac OS X endpoints. The following topics describe whether a new or improved feature is common to both Mac and Windows endpoints, specific to Mac endpoints only, or specific to Windows endpoints only.

## Mac and Windows endpoint features

The following Endpoint features apply to both Mac and Windows endpoints and is new in Symantec Data Loss Prevention 14.6.

## Support for excluding printers from monitoring

You can designate specific printers to be excluded from being monitored, including local, network, and PDF printers. You designate printers to ignore in the agent configuration.

For details on configuring printers to ignore, refer to the "Filter by Printer Properties" topic in the Symantec Data Loss Prevention online Help.

## Support for monitoring specific channels using Application Monitoring

The **Application Monitoring** screen selections allow users to enable or disable specific channels individually. For example, in previous versions, enabling the **Write operations** channel monitored files moved to removable storage, local drives, and network shares. Now you can opt to monitor the removable storage channel while leaving the network shares and local drives channel unmonitored.

The following graphic displays the **Application Monitoring Configuration** section of the **Application Monitoring** screen.

Figure 2-1 Application Monitoring channels


### Application Monitoring Configuration

#### Select the channels to monitor:




For 14.5.x and earlier agents, selecting any of Removable Storage, Local Drive, Copy to Network Share, or Application File Share.

Likewise, for 14.5.x and earlier agents, selecting either HTTP or FTP enables monitoring for both HTTP and FTP channels.




#### Destinations

- Removable Storage  
- Printer/Fax 
- Local Drive 

#### Application File Access

- Application File Access
- Open  
- Read 

#### Clipboard

- Clipboard
- Copy 
- Paste  

#### Web

- HTTP 
- FTP 

#### Network Shares



- Copy to Network Share  

Table 2-1 outlines the latest Application Monitoring channels and compares channel monitor coverage provided in previous versions.

**Table 2-1** Application Monitoring channel control

<b>Application monitoring channels</b>	<b>Application monitoring channels in previous versions</b>
<b>Removable Storage</b>	<b>Write operations</b>
<b>Local Drive</b>	
<b>Copy to Network Share</b>	
<b>Printer/Fax</b>	<b>Printer/Fax</b>
<b>Clipboard, Copy; and Clipboard, Paste</b>	<b>Clipboard, Copy; and Clipboard, Paste</b>
<b>HTTP</b>	<b>Network Access</b>
<b>FTP</b>	
<b>Application File Access, Open; and Application File Access, Read</b>	<b>Application File Access, Open; and Application File Access, Read</b>

### Application monitoring upgrade considerations

Upon upgrade from Symantec Data Loss Prevention 14.5.x and earlier, applications that have been added are updated to the new application controls.

For Mac applications, the **Removable Storage** and **Copy to Network Share** channels are enabled in Symantec Data Loss Prevention 14.6 if **Write Operations** or **Application File Access, Open** were enabled when the application was added in a previous Symantec Data Loss Prevention version. The **HTTP** and **FTP** channels are enabled in Symantec Data Loss Prevention 14.6 if **Network Access** was enabled in a previous version.

For Windows applications, the **Removable Storage**, **Copy to Network Share**, and **Local Drive** channels are enabled in Symantec Data Loss Prevention 14.6 if **Write Operations** or **Application File Access** were enabled when the application was added in a previous Symantec Data Loss Prevention version. The **HTTP** and **FTP** channels are enabled in Symantec Data Loss Prevention 14.6 if **Network Access** was enabled in a previous version.

### Application monitoring upgrade considerations for monitoring Windows apps

If the user entered the package ID in the **Binary Name** or **Original Filename** fields in previous versions of Symantec Data Loss Prevention, the upgrade process may identify the item as a Mac application and converts them accordingly. The conversion prevents the application from being monitored. If this scenario occurs, you must



delete the incorrectly converted application, and then re-add the application to the **Application Monitoring** screen.

## Mac endpoint features

The following Endpoint features apply to Mac endpoints and are new or improved in Symantec Data Loss Prevention 14.6.

### Support for monitoring Mac OS 10.11.6

The DLP Agent provides support for monitoring endpoints running Mac OS 10.11.6, including applications protected by System Integrity Protection (SIP).

---

**Note:** SIP monitor settings added in previous Symantec Data Loss Prevention versions remain after you upgrade to version 14.6. See [“Ability to monitor System Integrity Protection \(SIP\) on Mac endpoints”](#) on page 18.

---

### Support for monitoring macOS 10.12

The DLP Agent provides support for monitoring endpoints running macOS 10.12.

### Support for file restoration on Mac endpoints

The DLP Agent supports restoring the original, non-sensitive, file in case it is overwritten with a newer file that contains confidential data. This support applies to files residing on or saved to removable storage drives or network shares.

The following file restoration scenarios are supported on Mac endpoints:

- Saving a file that contains sensitive data to a removable storage device or network share
- Adding sensitive data to a file that resides on a removable storage device or network share
- Overwriting an existing file residing on a removable storage device or network share with a file that contains sensitive data using Finder (using Copy and Paste or drag-and-drop) or a terminal command
- Overwriting a non-sensitive file by saving, duplicating, moving, or exporting a file containing sensitive data using Text Edit or Preview

## Monitoring Outlook 2016 running on Mac endpoints

The DLP Agent supports monitoring content sent from Microsoft Outlook 2016 running on Mac endpoints. This feature is available on all Mac OS versions currently supported by Symantec Data Loss Prevention 14.6.

This feature provides support for the following:

- Monitoring sensitive information in all fields of email, meeting invitations, tasks, and notes, as well as attachments in each
- Detecting and preventing sensitive information from leaving a Mac endpoint when sent from Outlook
- Detecting and preventing sensitive information in both plain text and HTML formats
- Ability to ignore and monitor attachments based on file type and size
- Ability to monitor data using sender/recipient patterns
- Ability to monitor data whether or not Outlook is connected to the network

## Ability to monitor System Integrity Protection (SIP) on Mac endpoints

Starting in Symantec Data Loss Prevention 14.5, DLP Agents provided monitoring support for System Integrity Protection (SIP)-protected applications on Mac OS 10.11 through 10.11.4 endpoints. Symantec Data Loss Prevention 14.6 agents provide monitoring support through version Mac OS 10.11.6. Support also includes macOS 10.12.

If you upgrade the Mac endpoint OS to a version greater than 10.11.6 or macOS 10.12, SIP-protected applications are no longer monitored. Symantec Data Loss Prevention 14.6 provides Agent Events that notify users when Mac OS applications that are protected by System Integrity Protection (SIP) become un-monitored. Specifically, Agent Events display the SIP-protected application name and Mac OS version when either the DLP Agent version or the Mac OS version do not match the value provided in the `Hooking.SIP_Agent_OSX_VERSION_COMPATABILITY.str` advanced agent setting.

---

**Note:** For additional information on SIP and Mac OS compatibility, refer to the "Monitoring applications on Mac OS 10.11.5 or later where SIP is enabled" article. The article is available at the Symantec Support Center at:

<http://www.symantec.com/docs/TECH235226>

---

## Windows endpoint features

The following Endpoint features apply to Windows endpoints and are new or improved in Symantec Data Loss Prevention 14.5.

### Endpoint Prevent monitor support for Firefox 64-bit

Support for monitoring 64-bit Firefox on Windows 10.

### Support for monitoring Microsoft Windows 10 Anniversary Update Enterprise, Pro 64-bit PC

Support for monitoring endpoints running Microsoft Windows 10 Anniversary Update Enterprise, Pro 64-bit PC operating system. This support was added at the release of Symantec Data Loss Prevention version 14.5 MP1.

### Support for monitoring endpoints on Citrix 7.9

Symantec supports deploying the Symantec DLP Agent software directly on version 7.9 XenApp application servers and Citrix XenDesktop virtual machines.

### Increased monitor coverage for Citrix

Updates provide expanded monitor support for DLP Agents running in Citrix virtualized environments.

New monitor support includes the following:

- Ability to scan Microsoft Office files
- File restoration for Citrix drives
- Monitoring using the Application File Access feature, including monitoring files uploaded to browsers

### Support for monitoring uploads to Microsoft Edge

Support for monitoring file content uploaded through the Microsoft Edge browser, including files moved over the HTTPS protocol.

---

**Note:** If you are upgrading from a previous version of Symantec Data Loss Prevention, and you monitored the Microsoft Edge browser using the Application Monitoring feature, the entry remains enabled. Symantec recommends that you disable Application Monitoring for Microsoft Edge to prevent duplicate incidents.

---

## Cloud features

The following cloud features are new or improved in Symantec Data Loss Prevention 14.6.

### Ability to target policies to specific cloud connectors

You can target policies to specific cloud connectors, such as Gatelets and Securlets provided by Symantec CloudSOC, or the Symantec Blue Coat Web Security Service cloud web proxy. You assign policy groups to your cloud connectors on the **Manage > Cloud Connectors** page.

Symantec CloudSOC and Symantec Blue coat Web Security Service are sold separately.

### New reporting page for cloud connector incidents

You can view incident reports for data-in-motion (DIM) and data-at-rest (DAR) Cloud Connector incidents on the **Incidents > Cloud Connectors** page.

### Contextual attributes for cloud connector detection rules

You can specify contextual attributes in detection rules for cloud connectors, such as Symantec CloudSOC Securlets and Symantec Blue Coat Web Security Service cloud web proxies.

Contextual attributes let you add attributes to detection requests from cloud connectors. Symantec Data Loss Prevention passes these additional attributes along with the original detection request to the Cloud Service Connector. For example, you can add the **User Threat Score** attribute to a detection request to create incidents for all users above a threat score threshold you define.

You specify contextual attributes on the **Configure Policy - Add Rule** page.

## Discover features

The following Discover features are new or improved in Symantec Data Loss Prevention 14.6.

### Improved authorization for cloud storage targets

The authorization procedures for Box and Dropbox Business targets has changed. Rather than signing in to Box or Dropbox Business targets using an administrative account, you create a Box or Dropbox Business application, then authorize your

scans using the client ID and client secret for those applications. The client IDs and secrets are stored securely in Symantec Data Loss Prevention.

If you have already authorized Box and Dropbox Business cloud storage targets, your existing targets will no longer work. You must create new cloud authorizations after upgrading to Symantec Data Loss Prevention 14.6. To minimize potential downtime for such cloud storage targets, Symantec recommends that you create and register your Box and Dropbox Business applications before upgrading to Symantec Data Loss Prevention 14.6. For details about creating and registering Box and Dropbox applications, see the topic titled "Managing cloud storage authorizations" in the *Symantec Data Loss Prevention Administration Guide*.

You can create and manage authorizations for Box, Dropbox Business, and OneDrive for Business cloud storage targets using the Cloud Authorization page.

See "[Cloud Authorization page](#)" on page 26.

## SharePoint 2016 Discover target

Network Discover now supports SharePoint 2016 as a target for Discover scans. You can select SharePoint in the drop-down list of scan targets in the Enforce Server administration console when configuring a scan.

## Network features

The following network features are new or improved in Symantec Data Loss Prevention 14.6.

### Support for using a generic 10 GB Ethernet card with Network Monitor

You can now deploy Symantec Data Loss Prevention Network Monitor on a computer with a generic 10 GB Ethernet interface card to monitor data loss on your 10 GB Ethernet network.

## Detection features

The following detection features are new or improved in Symantec Data Loss Prevention 14.6.

### Form Recognition enabled by default

In previous versions of Symantec Data Loss Prevention, you enabled Form Recognition detection on the **Server Settings** page. In Symantec Data Loss Prevention 14.6, Form Recognition is enabled by default for customers licensed to

use Form Recognition. The Form Recognition detection rule must be enabled for a policy for the Form Recognition capability to take effect.

## Support for detecting electronically fillable forms

The Form Recognition feature detects PDF files that contain electronically fillable fields that use AcroForms formatting.

A data match occurs and an incident is created if something is entered on at least one electronic field and the form matches one of the indexed forms in the collection.

You do not perform configuration steps in addition to implementing Form Recognition. However, when creating a Form Recognition profile, you must segregate multi-page PDF files using a PDF editor that retains the AcroForms formatting, such as Acrobat Pro.

## Support for monitoring Microsoft Rights Management files

Symantec Data Loss Prevention can detect files that are encrypted using Microsoft Rights Management Services (RMS) administered through Azure or Active Directory. It can also inspect the content within those files.

The following RMS-encrypted file types can be detected:

- Microsoft Rights Management protected files (PFILE)
- Microsoft Office 2003 and older files
- Microsoft Office 2007 and newer (Office Open XML files) files

This feature can be used with the following Symantec Data Loss Prevention products:

- Network Prevent
- Cloud Prevent for Email
- Network Discover
- Network Monitor
- Network Prevent for Web
- Cloud Storage Discover

---

**Note:** Only Windows detection servers can perform RMS-encrypted file detection. Refer to the *Symantec Data Loss Prevention Installation Guide for Windows* or the *Symantec Data Loss Prevention Upgrade Guide for Windows* for details.

---

## New enhancements to regular expressions

Regular expressions are now evaluated consistently on both the server and on the endpoint. Performance improvements for regular expressions conditions significantly reduce the detection time on the server and on the endpoint. The new regular expression engine is optimized for the "no match" use case, and skips zero-length matches as a valid match.

The performance improvements take effect when you upgrade your detection servers and agents to Symantec Data Loss Prevention 14.6.

For more information about performance enhancements to regular expressions and for troubleshooting regular expressions created in Symantec Data Loss Prevention 14.5 for use in Symantec Data Loss Prevention 14.6, see the chapter "Detecting content using regular expressions" in the *Symantec Data Loss Prevention Administration Guide*.

## Additional variables for the Log to a Syslog Server and Send Email Notification response actions

You can include additional incident field variables in the **Log to a Syslog Server** and **Send Email Notification** response actions to provide more meaningful context to your syslog messages and email notifications.

You can now use the following variables for all incidents:

- Application Name
- Attachment File Name
- Reported On
- Destination IP
- Status
- Server or Detector
- Occurred On
- URL

For Endpoint incidents, you can use the following additional variables:

- Application user
- User Name
- Machine IP (Corporate)
- Endpoint Location

- User Justification

For a complete list of available response action variables, see the topic "Response action variables" in the *Symantec Data Loss Prevention Administration Guide*.

## New European General Data Protection Regulations (GDPR) policy templates

Symantec Data Loss Prevention includes several policy templates for European GDPR policy detection. Each GDPR policy template is pre-configured with keywords and data identifiers to detect GDPR compliance violations.

GDPR templates include:

- **General Data Protection Regulations (Banking and Finance)**
- **General Data Protection Regulations (Digital Identity)**
- **General Data Protection Regulations (Government Identification)**
- **General Data Protection Regulations (Healthcare and Insurance)**
- **General Data Protection Regulations (Personal Profile)**
- **General Data Protection Regulations (Travel)**

For details about GDPR policy templates, see the topic "UK and International Regulatory Enforcement policy templates" in the *Symantec Data Loss Prevention Administration Guide*.

## Updated HIPAA and HITECH (Including PHI) policy template

The **HIPAA and HITECH (Including PHI)** policy template has been updated to include keywords for ICD 10 codes.

## New and updated data identifiers

Symantec Data Loss Prevention 14.6 includes the following new data identifiers:

- **China Passport Number**
- **French Passport Number**
- **Indian Aadhaar Card Number**
- **Japan Passport Number**
- **Korea Passport Number**
- **Korea Residence Registration Number for Foreigners**



- **Korean Residence Registration Number for Koreans**
- **Mexican Personal Registration and Identification Number**
- **Mexican Tax Identification Number**
- **NIB Number Validation Check (validator)**
- **Spanish Passport Number**
- **Swedish Passport Number**
- **US Passport Number**
- **US ZIP+4 Postal Codes**

Symantec Data Loss Prevention 14.6 includes the following updated data identifiers:

- **Credit Card Number**
- **CUSIP Number**
- **Hong Kong ID**
- **Randomized US Social Security Number (SSN)**

## Enforce Server features

The following Enforce Server features are new or changed in Symantec Data Loss Prevention 14.6.

### Support for Windows Server 2016

You can install and run the Symantec Data Loss Prevention Enforce Server and detection servers on Windows Server 2016 systems. Oracle does not currently support Oracle 11g Standard or One on Windows Server 2016. If you are using Oracle 11g, you must run the database on another supported operating system. If you are using a different version of Oracle, refer to your Oracle documentation for server support information.

### Cloud server maintenance alerts available on Enforce Server administration console

Notifications of cloud service maintenance and outage events are now automatically displayed at the Enforce Server administration console as system events.

## Support for managing servers using a domain service user

You can access and manage the Enforce Server and detection servers using a domain user. For example, by configuring a domain user, you can access Active Directory (AD) Rights Management Services (RMS) from the Enforce Server to detect RMS-encrypted files.

Upgrading users can use the ChangeServiceUser utility to update existing local service users to domain users. The utility is located in the Enforce Server installation directory, for example *C:\SymantecDLP\Protect\bin*.

Refer to the *Symantec Data Loss Prevention Installation Guide for Windows* or the *Symantec Data Loss Prevention Upgrade Guide for Windows* for details.

## Cloud Authorization page

You can create and manage authorizations for connecting to Box, Dropbox Business, and OneDrive for Business cloud storage repositories on the Cloud Authorization page.

## Oracle 12c database template

You can use this database template to create the Symantec Data Loss Prevention Oracle database on Oracle 12c Enterprise more quickly and easily. The template includes the Symantec Data Loss Prevention database schema and a response file that simplifies the database creation process. For more information about using Oracle 12c Enterprise with Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Oracle 12c Enterprise Edition Implementation Guide*.

## Database space reclamation utility

You can use the new database space reclamation utility to reclaim unused tablespaces in the Symantec Data Loss Prevention Oracle database. Using this utility enables you to use the memory in your Oracle database more efficiently, increasing performance and reducing the overall size of your database.

## Improved Policy List page

You can manage your policies more efficiently on the improved Policy List page. You can now apply actions such as **Export**, **Download Details**, **Activate**, **Suspend**, and **Delete** to a selection of policies. You can also filter your policies by **Status**, **Name**, **Description**, and **Policy Group**.

# Deprecated features

**Table 2-2**      Deprecated features in Symantec Data Loss Prevention 14.6

<b>Feature</b>	<b>Description</b>
Mobile Prevent for Web	Mobile Prevent for Web is deprecated and will be removed in a future release. Users of the product should plan accordingly.
Mobile Email Monitor	Mobile Email Monitor is deprecated and will be removed in a future release. Users of the product should plan accordingly.