What's New and What's Changed in Symantec™ Data Loss Prevention 15.1

Last updated: 07 August 2018
What's New and What's Changed in Symantec Data Loss Prevention 15.1

Documentation version: 15.1b

Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, CloudSOC, Blue Coat, the Symantec Logo, the Checkmark Logo, the Blue Coat logo, and the Shield 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.
# Chapter 1
Introducing Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this guide</td>
<td>7</td>
</tr>
<tr>
<td>Summary of new and changed features in Symantec Data Loss Prevention 15.1</td>
<td>8</td>
</tr>
<tr>
<td>Integration with other Symantec Information Protection products</td>
<td>8</td>
</tr>
<tr>
<td>Installation and upgrade features</td>
<td>9</td>
</tr>
<tr>
<td>Enforce Server and platform features</td>
<td>9</td>
</tr>
<tr>
<td>Detection features</td>
<td>11</td>
</tr>
<tr>
<td>Endpoint features</td>
<td>12</td>
</tr>
<tr>
<td>Discover features</td>
<td>13</td>
</tr>
<tr>
<td>Network features</td>
<td>14</td>
</tr>
<tr>
<td>Cloud features</td>
<td>14</td>
</tr>
<tr>
<td>Removed and deprecated features</td>
<td>14</td>
</tr>
</tbody>
</table>

# Chapter 2
New and Changed Features in Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation and upgrade features</td>
<td>15</td>
</tr>
<tr>
<td>Enforce Server and detection server installation enhancements</td>
<td>15</td>
</tr>
<tr>
<td>Enforce Server and detection server upgrade enhancements</td>
<td>16</td>
</tr>
<tr>
<td>Enforce Server and platform features</td>
<td>17</td>
</tr>
<tr>
<td>Support for Oracle 12c Standard Edition 2 Release 2</td>
<td>17</td>
</tr>
<tr>
<td>Secure communication between the Enforce Server and Oracle database</td>
<td>17</td>
</tr>
<tr>
<td>Automatically flag incidents for deletion</td>
<td>17</td>
</tr>
<tr>
<td>Increased limit for Add Note field</td>
<td>18</td>
</tr>
<tr>
<td>Modernized and user-friendly page designs in the Enforce Server</td>
<td>18</td>
</tr>
<tr>
<td>administration console</td>
<td>18</td>
</tr>
<tr>
<td>Updated service names</td>
<td>18</td>
</tr>
<tr>
<td>Guidance for Enforce Server and database sizing and performance</td>
<td>19</td>
</tr>
<tr>
<td>Detection features</td>
<td>19</td>
</tr>
</tbody>
</table>
Tagged content detection using new classification-matching option ............................................................ 19
Single-pass EDM ............................................................................................................................. 19
Single-pass IDM ............................................................................................................................. 20
Incremental IDM Indexing .............................................................................................................. 20
File type matching enhancements ................................................................................................... 20
Enhanced support for the Affordable Care Act ............................................................................. 21
New and updated data identifiers ................................................................................................. 21
Updated General Data Protection Regulation (GDPR) policy templates ........................................ 23
Include email aliases in user groups ............................................................................................. 25
Endpoint features .......................................................................................................................... 26
Single installer for DLP, ICT, and ICE endpoint agents ............................................................. 26
Usability enhancements to endpoint ICE capabilities ..................................................................... 26
Browser monitoring updates ......................................................................................................... 27
Ability to display blocked email recipients in notification pop-ups .............................................. 27
Symantec Information Centric Encryption (ICE) support for cloud storage applications ........... 28
Discover features ............................................................................................................................ 28
Grid scanning for SharePoint targets ........................................................................................... 28
Performance and scalability guidelines for SharePoint grid scanning ........................................ 28
Configure Network Protect to quarantine confidential files in Microsoft SharePoint repositories ... 29
Network features ........................................................................................................................... 29
Secure ICAP for Network Prevent for Web with Blue Coat ProxySG ............................................. 30
Increase in character limits of the Network IP filter and Sender filter for Network Monitor ........... 30
Cloud features ................................................................................................................................ 30
Easier update of email domains for Cloud Service for Email ..................................................... 30
Encrypt email using Symantec ICE with Cloud Service for Email ................................................ 30
Removed and deprecated platforms and capabilities ...................................................................... 31
About deprecated platforms .......................................................................................................... 31
Support for stunnel ......................................................................................................................... 31
Operating system support for servers ........................................................................................... 31
Symantec product integrations ....................................................................................................... 31
Operating system support for endpoint systems ........................................................................... 31
Deprecated operating systems for endpoint systems ...................................................................... 32
Exchange Server targets support .................................................................................................. 32
Deprecated Exchange Server targets ............................................................................................ 32
Deprecated Documentum Content Server targets ......................... 32
OpenText (Livelink) scanner targets support .............................. 32
Virtual desktop support with Endpoint Prevent .......................... 32
Endpoint Prevent application .................................................. 33
Deprecated Endpoint Prevent application ................................. 33
IBM (Lotus) Notes targets ...................................................... 33
SQL database targets ............................................................ 33
Deprecated SQL database targets ............................................. 33
SharePoint server targets ....................................................... 33
Advanced Server settings ....................................................... 34
Introducing Symantec Data Loss Prevention 15.1

This chapter includes the following topics:

- About this guide
- Summary of new and changed features in Symantec Data Loss Prevention 15.1

About this guide

The *What's New and What's Changed Guide* in Symantec Data Loss Prevention 15.1 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 15.1, 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.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 August 2018</td>
<td>Removed reference to SymantecDLPUpdate service.</td>
</tr>
</tbody>
</table>
Summary of new and changed features in Symantec Data Loss Prevention 15.1

New and changed features in Symantec Data Loss Prevention 15.1 are summarized in this chapter. You can find more deployment details and explanations of the features in chapter 2.

Integration with other Symantec Information Protection products

Table 1-2  New and changed features for Information Protection integrations for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single installer for DLP Agent, Information Centric Tagging (ICT) agent, and Information Centric Encryption (ICE) Utility</td>
<td>You can choose to install all of the agents at the same time, or you can install each one separately. See “Single installer for DLP, ICT, and ICE endpoint agents” on page 26.</td>
</tr>
<tr>
<td>Symantec Information Centric Encryption (ICE) support for cloud storage applications</td>
<td>Use built-in Symantec Information Centric Encryption (ICE) capabilities to encrypt sensitive files that are uploaded and downloaded using monitored cloud storage applications such as Box and Microsoft OneDrive. See “Symantec Information Centric Encryption (ICE) support for cloud storage applications” on page 28.</td>
</tr>
<tr>
<td>Symantec Information Centric Encryption support for Cloud Service for Email</td>
<td>Use Symantec Information Centric Encryption capabilities to encrypt sensitive emails that are sent using monitored email applications such as on-premises Microsoft Exchange, Microsoft Office 365, and Gmail. See “Encrypt email using Symantec ICE with Cloud Service for Email” on page 30.</td>
</tr>
<tr>
<td>Enhanced integration with Symantec Information Centric Tagging (ICT)</td>
<td>Easily configure Data Loss Prevention policies to detect classified content based on the taxonomy from your Symantec Information Centric Tagging deployment. See “Tagged content detection using new classification-matching option” on page 19.</td>
</tr>
<tr>
<td>Symantec ICE usability enhancements</td>
<td>Incident snapshots indicate whether a file has been encrypted or encrypted and blocked; other improvements simplify configuration and end-user interaction. See “Usability enhancements to endpoint ICE capabilities” on page 26.</td>
</tr>
</tbody>
</table>
# Installation and upgrade features

**Table 1-3** New and changed features for installation and upgrade for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved Enforce Server and detection server installation experience</td>
<td>The new installer for the Enforce Server and detection servers enables you to select the components you need for your particular implementation. Selecting only the needed components reduces the installation payload and reduces network bandwidth usage. See “Enforce Server and detection server installation enhancements” on page 15.</td>
</tr>
<tr>
<td>Enforce Server and detection server upgrade enhancements</td>
<td>The new process for upgrading the Enforce Server and detection servers provides performance benefits compared to upgrades in previous versions. In addition, the new upgrade process provides these capabilities:</td>
</tr>
<tr>
<td></td>
<td>■ Allows you to upgrade your two- and three-tier Windows and Linux instances directly from Symantec Data Loss Prevention version 14.x to Symantec Data Loss Prevention 15.1.</td>
</tr>
<tr>
<td></td>
<td>■ Allows you to upgrade while the existing Symantec Data Loss Prevention version continues to run.</td>
</tr>
<tr>
<td></td>
<td>See “Enforce Server and detection server upgrade enhancements” on page 16.</td>
</tr>
</tbody>
</table>

# Enforce Server and platform features

**Table 1-4** New and changed features for the Enforce Server for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
### Table 1-4  
New and changed features for the Enforce Server for Symantec Data Loss Prevention 15.1 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Secure communication between the Enforce Server and Oracle database     | You can create a secure connection between the Enforce Server and the Oracle database using TLS.  
See “Secure communication between the Enforce Server and Oracle database” on page 17.                                                                                                                           |
| Automatically flag incidents for deletion                               | Automatically flag incidents for deletion based on criteria such as incident age.  
See “Automatically flag incidents for deletion” on page 17.                                                                                                                                                        |
| Increased limit for **Add Note** field                                  | The limit for the **Add Note** field for the response rule action and the incident action has been increased from 1024 characters to 4000 bytes.  
See “Increased limit for Add Note field” on page 18.                                                                                                                                                               |
| Modernized and user-friendly page designs in the Enforce Server         | Updated layouts for the Executive Summary dashboards, **Policy Groups** page, and **Cloud Detection Server** page in the Enforce Server administration console.  
See “Modernized and user-friendly page designs in the Enforce Server administration console” on page 18.                                                                                                      |
| Updated service names                                                    | Symantec Data Loss Prevention 15.1 includes a change to all service names; where service names began with ‘Vontu,’ they now begin with ‘SymantecDLP.’ All service names that included "Monitor" now include "DetectionServer" instead.  
The **VontuUpdate** service has been removed from Symantec Data Loss Prevention 15.1.  
See “Updated service names” on page 18.                                                                                                                                                                            |
## Detection features

**Table 1-5** New and changed features for Detection for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-pass EDM and other EDM-related improvements</td>
<td>Single-pass EDM detection performance is improved up to 14 times when a large number of EDM indexes are used. Other EDM changes include enhancements to the behavior of the WHERE clause, stopwords, CJK (Chinese/Japanese/Korean) processing, and multi-token matching. EDM reindexing is required after you upgrade to Symantec Data Loss Prevention 15.1. EDM has new memory requirements and introduces changes to how detection servers are sized. The <em>EDM Memory Requirements Spreadsheet</em> has been updated. See “Single-pass EDM” on page 19.</td>
</tr>
<tr>
<td>Single-pass IDM</td>
<td>Detection performance is improved up to 30% when multiple indexes are used. See “Single-pass IDM” on page 20.</td>
</tr>
<tr>
<td>Incremental IDM Indexing</td>
<td>You can append files to a previously created index without replacing the entire index you’ve deployed. See “Incremental IDM Indexing” on page 20.</td>
</tr>
</tbody>
</table>
| File type enhancements | You can select four different file type matching rules for Outlook. Support for the Outlook file type is expanded to:  
  ■ Outlook Message File: *.msg* file type  
  ■ Outlook Mac Data File: *.olm* file type  
  ■ Outlook Personal Storage Table File: *.pst* file type  
  ■ Outlook Data File: *.ost* file type, newly supported in Symantec Data Loss Prevention 15.1. In Symantec Data Loss Prevention 15.0, only the *.msg* file type was available. See “File type matching enhancements” on page 20. |
### Table 1-5  
New and changed features for Detection for Symantec Data Loss Prevention 15.1 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced support for the Affordable Care Act</td>
<td>Symantec Data Loss Prevention 15.1 enhances support for the Affordable Care Act (ACA) by including a new policy template and three new data identifiers for detecting protected health information associated with the United States Medicare and Medicaid programs.</td>
</tr>
<tr>
<td>Updated General Data Protection Regulation (GDPR) templates</td>
<td>Updates to some GDPR policy templates to reflect the new European Personal Identity data identifiers. The GDPR replaces the EU Data Protection Directives on 25 May 2018.</td>
</tr>
<tr>
<td>Include email aliases in user groups</td>
<td>You can include email aliases in your user group configurations.</td>
</tr>
</tbody>
</table>

### Endpoint features

### Table 1-6  
New and changed features for Endpoint for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser updates</td>
<td>The DLP Agent uses processes that are native to the browser to monitor Windows browsers, which helps to improve performance and to prevent monitoring coverage outages. The DLP Agent uses an extension to monitor Safari to comply with Safari security protocols.</td>
</tr>
</tbody>
</table>
Table 1-6  New and changed features for Endpoint for Symantec Data Loss Prevention 15.1 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Ability to display blocked email recipients in notification pop-ups | You can configure policies to display blocked emails in endpoint notification pop-ups.  
  See “Ability to display blocked email recipients in notification pop-ups” on page 27. |

Discover features

Table 1-7 New and changed features for Discover for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Grid scanning for SharePoint targets         | The grid scanning feature of Network Discover now supports Microsoft SharePoint scan targets. Grid scans improve scan throughput by distributing the workload across multiple detection servers.  
  See “Grid scanning for SharePoint targets” on page 28. |
| Performance and scalability guidelines for SharePoint grid scanning | The documentation for Symantec Data Loss Prevention 15.1 includes scaling and performance recommendations for running grid scans on SharePoint scan targets.  
  See “Performance and scalability guidelines for SharePoint grid scanning” on page 28. |
| Network Protect quarantine of confidential files in SharePoint repositories | Configure Network Protect to automatically quarantine confidential files in Microsoft SharePoint repositories using the Network Protect: Quarantine File response action.  
  Alternatively, configure the SharePoint Quarantine smart response action to resolve incidents manually.  
  See “Configure Network Protect to quarantine confidential files in Microsoft SharePoint repositories” on page 29. |
Network features

Table 1-8  New and changed features for Network for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure ICAP for Network Prevent for Web with Blue Coat ProxySG</td>
<td>Use Secure ICAP for Network Prevent for Web with Blue Coat ProxySG. Use of stunnel is no longer supported.</td>
</tr>
<tr>
<td>Increased character limits for Network IP filter and Sender Filter for Network Monitor</td>
<td>Character limits for the Network IP filter and the Sender filter for the Network Monitor configuration are increased.</td>
</tr>
<tr>
<td></td>
<td>See “Increase in character limits of the Network IP filter and Sender filter for Network Monitor” on page 30.</td>
</tr>
</tbody>
</table>

Cloud features

Table 1-9  New and changed features for Cloud for Symantec Data Loss Prevention 15.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easier update of email domains for Cloud Service for Email</td>
<td>Add and update your email domains for Cloud Service for Email for Microsoft Office 365 in reflecting mode in the Enforce Server administration console.</td>
</tr>
<tr>
<td></td>
<td>See “Easier update of email domains for Cloud Service for Email” on page 30.</td>
</tr>
</tbody>
</table>

Removed and deprecated features

Several features have been removed or deprecated in Data Loss Prevention version 15.1. See “Removed and deprecated platforms and capabilities” on page 31.
New and Changed Features in Symantec Data Loss Prevention 15.1

This chapter includes the following topics:

- Installation and upgrade features
- Enforce Server and platform features
- Detection features
- Endpoint features
- Discover features
- Network features
- Cloud features
- Removed and deprecated platforms and capabilities

Installation and upgrade features

The following installation and upgrade features are new or improved in Symantec Data Loss Prevention 15.1.

Enforce Server and detection server installation enhancements

The new installation process for the Enforce Server and detection servers enables you to select the components you need for your particular implementation. Selecting specific installation
components reduces the installation payload and network bandwidth usage compared to the previous installation process.

The new installation process requires that you install the Java Runtime Environment (JRE)—included with the Symantec Data Loss Prevention installer files—before starting the main platform (Enforce Server) installation. Because the Java Runtime Environment is separate from the platform installation, you can update it as Symantec certifies new JRE versions.

**Note:** The graphical user interface portion of the Linux installation is no longer used.

The new installation process includes ease-of-use enhancements. You can use deployment tools to install using MSI on Windows servers and RPM on Linux servers. Example deployment tools that you might use may include the following:

- For RPM, you can use YUM repositories and third-party SMS tools like System Center Configuration Manager.
- For MSI, you can use GPO deployment and third-party SMS tools like System Center Configuration Manager.

**Enforce Server and detection server upgrade enhancements**

The new upgrade process for the Enforce Server and detection server provides the following enhancements:

- Allows you to upgrade your one-, two-, and three-tier instances directly from Symantec Data Loss Prevention version 14.0 and later to version 15.1. You are no longer required to upgrade incrementally from one major or minor release to the next.

**Note:** Upgrade the DLP Agents to at least version 14.0 before you upgrade the Enforce Server to 15.1. DLP Agents earlier than 14.0 cannot communicate with the version 15.1 Enforce Server and detection servers.

- Allows you to upgrade while the existing Symantec Data Loss Prevention version continues to monitor data.
- Allows you to easily roll back to a previous version.
Note: The upgrade process migrates data from the previous instance to a new instance that uses a new directory structure, including plugins located at C:\SymantecDLP\Protect\plugins\ContentExtraction. The migration process does not migrate plugins outside of this location. Refer to the version 15.1 Symantec Data Loss Prevention Upgrade Guide at the following Symantec Support Center article:


If necessary, you can perform a rollback after you have migrated. For details, see the version 15.1 Symantec Data Loss Prevention System Maintenance Guide at the following Symantec Support Center article:


Enforce Server and platform features

The following Enforce Server features are new or improved in Symantec Data Loss Prevention 15.1.

Support for Oracle 12c Standard Edition 2 Release 2

You can use Oracle 12c Standard Edition 2 Release 2 (version 12.2.0.1) with Symantec Data Loss Prevention 15.1 for new installations and upgrades. You can obtain Oracle 12c Standard Edition 2 Release 2 directly from Symantec.

Symantec ends support for Oracle 11g on 25 September 2018. Symantec recommends that you upgrade to Oracle Database 12c Standard Edition 2 Release 2 to continue to receive bug fixes and security patches.

For more information, see the Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2 Installation and Upgrade Guide at the following Symantec Support Center article:


Secure communication between the Enforce Server and Oracle database

You can establish a secure connection between the Enforce Server and Oracle database using TLS 1.2. You can establish certificates to create the connection or use a server certificate that is signed by a public CA.

Automatically flag incidents for deletion

You can automatically flag incidents for deletion on the System > Incident Deleter > Flag Incidents for Deletion page. For example, you might want to automatically flag incidents for
deletion based on their age. Flagging incidents for deletion automatically can save you a significant amount of time and effort, especially if you have a large number of incidents in your system.

To automatically flag incidents for deletion, you create incident reports with your criteria, such as incident age. You can have one report per incident category: Network, Endpoint, Discover, and Applications. You can customize the schedule for incident flagging, or run incident flagging jobs manually.

After you have flagged incidents for deletion, you can schedule them for deletion or delete them manually on the System > Incident Deleter > Delete Incidents page.

For more information, see the Help topic About automatically flagging incidents for deletion.

Increased limit for Add Note field

The limit for the Add Note field for the response rule action and the incident action has been increased from 1024 characters to 4000 bytes.

Modernized and user-friendly page designs in the Enforce Server administration console

Symantec Data Loss Prevention 15.1 includes updated layouts for the Executive Summary dashboards and Policy Groups page in the Enforce Server administration console.

For more information about the Executive Summary dashboards, see the Help topic About dashboard reports and executive summaries.

Updated service names

Symantec Data Loss Prevention 15.1 includes a change to all service names. In previous releases, service names were prepended with Vontu. These service names will now be prepended with SymantecDLP. In addition to this change, the term Monitor is replaced by DetectionServer. The new service names are as follows:

- SymantecDLPDetectionServer
- SymantecDLPDetectionServerController
- SymantecDLPIncidentPersist
- SymantecDLPManager
- SymantecDLPNotifier

Because of changes to the upgrade process for the Enforce Server and detection servers, the VontuUpdate service has been removed from Symantec Data Loss Prevention 15.1.

See "Enforce Server and detection server upgrade enhancements" on page 16.
For more information about working with Symantec Data Loss Prevention services, see the Help topic About Symantec Data Loss Prevention services.

**Guidance for Enforce Server and database sizing and performance**

The documentation for Symantec Data Loss Prevention 15.1 includes sizing and performance recommendations for the Enforce Server and database.

For more information about these recommendations, see the Symantec Data Loss Prevention System Requirements and Compatibility Guide.

**Detection features**

The following detection features are new or improved in Symantec Data Loss Prevention 15.1.

**Tagged content detection using new classification-matching option**

You can create detection rules by choosing ICT tags from the Information Centric Tagging classification taxonomy, which you import and display on the Enforce Server administration console. Use the new **Content Matches Classification** option to detect classified content across all Data Loss Prevention channels (Network, Storage, Endpoint, Cloud). ICT tags are detected in files and emails. Supported file types include Microsoft Office files (legacy Office and Office 2007 and later formats), PNG files, GIF files, and PDF files.

See Synchronizing with Information Centric Tagging and Content Matching Conditions in the Help.

**Single-pass EDM**

Single-pass EDM performance is improved up to 14 times compared to earlier releases when multiple EDM indexes are deployed in a policy set. Other EDM changes include enhancements to the behavior of the WHERE clause, stopwords, CJK (Chinese/Japanese/Korean) processing, and multi-token matching.

New detection server sizing guidelines are reflected in the updated EDM Memory Requirements Spreadsheet. The spreadsheet is located at the Symantec Support Center at: http://www.symantec.com/docs/DOC8255.html.

You must reindex your EDM indexes when you upgrade to Symantec Data Loss Prevention 15.1.

See About upgrading EDM deployments in the Help.
Single-pass IDM

With Single-pass IDM, detection performance is improved up to 30% when two or more IDM rules are configured and you use multiple indexes.

Single-pass IDM is available on the server; it is not available on the endpoint.

You must reindex your IDM indexes when you upgrade to Symantec Data Loss Prevention 15.1.

See Re-indexing IDM profiles after a major upgrade in the Help.

Incremental IDM Indexing

**Always keep files** is a new option in the Remote IDM indexer. When you choose this option, files that are in the previous index, but not in the current data source, are not deleted. Files can now be appended to a previously created index; the entire index does not have to be replaced when you add files.

The **Always keep files** option is available in the command line interface of the Remote IDM Indexer on Windows and Linux, and in the user interface version of the Remote IDM Indexer on Windows.

See Incremental Indexing in the Help.

File type matching enhancements

When you use the File Type Match condition for detection, you can now select one of four different file type rules corresponding to each supported Outlook file type, including the newly supported `.ost` file type:

- **Outlook Message File**: `.msg` file type identification, metadata extraction, and subfile extraction for Outlook message files.
- **Outlook Mac Data File**: `.olm` file type identification and metadata extraction for macOS files.
- **Outlook Personal Storage Table File**: `.pst` file type identification support for iCard.
- **Outlook Data File**: `.ost` file type identification, metadata extraction, and subfile extraction for Outlook data files.

If the Outlook message file format (`.msg`) was selected in Symantec Data Loss Prevention 15.0, when you upgrade to Symantec Data Loss Prevention 15.1, all four file types are selected. If no Outlook file format was selected in 15.0, none of the four file types are selected when you upgrade to 15.1.

See Supported formats for file type identification in the Help.
Enhanced support for the Affordable Care Act

Symantec Data Loss Prevention 15.1 enhances support for the Affordable Care Act (ACA) by including a new policy template: Medicare and Medicaid (including PHI). This policy detects protected health information (PHI) associated with the United States Medicare and Medicaid programs, including Medicare Beneficiary Numbers, Health Insurance Claim Numbers and Current Procedural Terminology codes used by the Healthcare Common Procedure Coding System.

There are three new data identifiers associated with the Medicare and Medicaid (including PHI) policy template:


- **Health Insurance Claim Number:** The Health Insurance Claim Number (HICN) is assigned by the Social Security Administration to an individual for the purpose of identifying them as a medicare beneficiary.

- **Medicare Beneficiary Identifier:** The Medicare Beneficiary Identifier (MBI) is assigned to an individual for the purpose of identifying them as a medicare beneficiary. The MBI will replace the Healthcare Insurance Claim Number (HICN) on all Medicare cards by April 2019.

For more information about the new Medicare and Medicaid (including PHI) policy template, see the Help topic Medicare and Medicaid (including PHI).

New and updated data identifiers

Symantec Data Loss Prevention 15.1 includes many new and updated data identifiers.

New data identifiers:

- Austria Value Added Tax (VAT) Number
- Denmark Tax Identification Number
- Denmark Value Added Tax (VAT) Number
- Finland Driver's License Number
- Finland European Health Insurance Number
- Finland Passport Number
- Finland Tax Identification Number
- Finland Value Added Tax (VAT) Number
- Germany Tax Identification Number
- Greece Social Security Number (AMKA)
- Ireland Passport Number
- Ireland Tax Identification Number
- Ireland Value Added Tax (VAT) Number
- Japan Driver's License Number
- Latvia Personal Identification Number
- Luxembourg Passport Number
- Luxembourg Tax Identification Number
- Luxembourg Value Added Tax (VAT) Number
- Portugal Driver's License Number
- Portugal National Identification Number
- Portugal Passport Number
- Portugal Tax Identification Number
- Portugal Value Added Tax (VAT) Number
- Romania National Identification Number
- Slovakia National Identification Number
- Slovenia Unique Master Citizen Number
- Spain Value Added Tax (VAT) Number
- Sweden Driving License Number
- Sweden Personal Identification Number
- Sweden Tax Identification Number
- Sweden Value Added Tax (VAT) Number
- UK Bank Account Number Sort Code
- UK Value Added Tax (VAT) Number

Updated data identifiers:
- Austrian Social Security Number
- Bulgarian Uniform Civil Number (EGN)
- Canadian Social Insurance Number
- Hong Kong ID
- Italy Driver's License Number
Japanese My Number - Corporate
- Latvia Tax Identification Number
- Polish REGON Number
- Romanian Numerical Personal Code
- Sweden Personal Identification Number

For more information about these new and updated data identifiers, see the Help topic System-defined data identifiers.

Updated General Data Protection Regulation (GDPR) policy templates

The General Data Protection Regulation (GDPR) is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the EU. It also addresses export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The GDPR replaces the EU Data Protection Directives as of 25 May 2018.

Symantec Data Loss Prevention 15.1 includes updates to some GDPR policy templates to incorporate the new European Personal Identity data identifiers.

The General Data Protection Regulation (Banking and Finance) policy template includes these new data identifiers:

- Austria Value Added Tax (VAT) Number
- Denmark Tax Identification Number
- Denmark Value Added Tax (VAT) Number
- Finland Driver's License Number
- Finland Passport Number
- Finland Tax Identification Number
- Finland Value Added Tax (VAT) Number
- Germany Tax Identification Number
- Ireland Passport Number
- Ireland Tax Identification Number
- Ireland Value Added Tax (VAT) Number
- Latvia Personal Identification Number
- Luxembourg Passport Number
The General Data Protection Regulation (Government Identification) policy template includes these new data identifiers:

- Austria Value Added Tax (VAT) Number
- Denmark Tax Identification Number
- Denmark Value Added Tax (VAT) Number
- Finland Driver's License Number
- Finland Passport Number
- Finland Tax Identification Number
- Finland Value Added Tax (VAT) Number
- Germany Tax Identification Number
- Ireland Passport Number
- Ireland Tax Identification Number
- Ireland Value Added Tax (VAT) Number
- Luxembourg Passport Number
- Luxembourg Tax Identification Number
- Luxembourg Value Added Tax (VAT) Number
- Portugal Driver's License Number
- Portugal Passport Number
- Portugal National Identification Number
Portugal Tax Identification Number
Portugal Value Added Tax (VAT) Number
Sweden Driving License Number
Sweden Tax Identification Number
Sweden Value Added Tax (VAT) Number

The General Data Protection Regulation (Healthcare and Insurance) policy template includes these new data identifiers:

Finland Driver's License Number
Portugal Driver's License Number
Portugal National Identification Number

The General Data Protection Regulation (Travel) policy template includes these new data identifiers:

Finland Driver's License Number
Finland Passport Number
Ireland Passport Number
Luxembourg Passport Number
Portugal Driver's License Number
Portugal National Identification Number

For more information about GDPR policy templates, see the Help topic General Data Protection Regulation (GDPR) policy templates.

Include email aliases in user groups

You can configure user groups to include email aliases. For example, if a user has the primary email address "robert_smith@company.com" and an email alias "bob_smith@company.com," in Microsoft Active Directory, selecting Include Mail Aliases adds both email addresses for that user to your DGM index. Be aware that indexing email aliases will increase your index size.

For more information about including email aliases in user groups, see the Help topic Configuring User Groups.
Endpoint features

Symantec Data Loss Prevention enables you to monitor both Windows and macOS endpoints. Unless otherwise noted, the features described here apply to both macOS and Windows endpoints.

The following endpoint features are new or improved in Symantec Data Loss Prevention 15.1.

Single installer for DLP, ICT, and ICE endpoint agents

In addition to the DLP Agent, the Windows endpoint installer packaging process can include the ICT and ICE Agents, and the macOS endpoint installer packaging process can include the DLP and the ICE Agents.

You can choose to install all of the agents at the same time, or you can install each one separately.

Including these endpoint agents in a single package facilitates the deployment of integrated solutions involving Symantec Data Loss Prevention, Symantec Information Centric Tagging, and Symantec Information Centric Encryption.

To learn more about the installation process for each product, see the Symantec Data Loss Prevention Installation Guide for version 15.1 at the following Symantec Support Center location:

http://www.symantec.com/docs/DOC9257

Usability enhancements to endpoint ICE capabilities

The following enhancements simplify and improve the way in which Enforce Server administrators and endpoint users interact with Symantec ICE:

- The Prevent: Encrypt response rule works on Microsoft Windows endpoints that are running in Safe Mode.

- Incident snapshots display two new agent responses:
  - **Action Encrypted** - Indicates that a managed user tried to copy or move a sensitive file using a supported channel and the file was automatically encrypted.
  - **Action Encryption Blocked** - Indicates that a user action was blocked and a file was not encrypted either because an unmanaged user attempted to copy or move it using a supported channel, or because a managed user attempted to copy or move the file using an unsupported channel.

*Note:* Enforce Server administration console users can also select these agent responses while configuring filters in **Advanced Filters & Summarization** section of Endpoint Incidents reports.
While configuring the Prevent: Encrypt response rule, you configure only two alert messages instead of three:

- Block alert
- Encrypt alert

Note: A Block alert is displayed either when an unmanaged user attempts to copy or move a sensitive file using a supported channel, or when a managed user attempts to copy or move a sensitive file using an unsupported channel.

For more information, see Configuring the Endpoint Prevent: Encrypt action.

- Prevent: Encrypt response rule now displays notifications to Endpoint users, and does not require any user action.
- ICE-encrypted files are not decrypted when users copy them using Explorer from USB storage devices to network shares or to the local disk.
- ICE-encrypted files are not blocked when users try to copy them from USB storage devices to network shares.
- File encryption is supported on USB storage devices that are formatted with the FAT32 file system.

Browser monitoring updates

The DLP Agent uses processes native to the browser to monitor the Microsoft Edge, Firefox (on Windows), and Internet Explorer browsers. The updates help to improve performance and to prevent monitoring coverage outages after browser architecture updates. Updates to Microsoft Edge monitoring adheres to new Microsoft security standards.

To monitor Safari, the DLP Agent uses an extension. This method complies with Safari security protocols introduced with the Apple patch Security Update 2018-001. Endpoint users must enable the extension to allow monitoring on the endpoint. The Agent Overview screen identifies endpoints where the extension is not yet enabled.

For more information, see About application monitoring in the Help.

Ability to display blocked email recipients in notification pop-ups

You can configure policies to display blocked emails in endpoint notification pop-ups. The feature is supported on the following platforms and applications:

- Windows using Outlook 2013 and 2016 and IBM Notes 9.0.x
- macOS using Outlook 2011 and 2016
This feature uses the new Matching Recipients rule in policies to identify single emails or entire email domains in notification pop-ups.

Symantec Information Centric Encryption (ICE) support for cloud storage applications

The Symantec Information Centric Encryption (ICE) capabilities for Endpoint Prevent have been expanded so that you can more easily apply ICE encryption to sensitive files that are uploaded using monitored cloud storage applications such as Box and Microsoft OneDrive. You use the Prevent: Encrypt action in your response rule to automatically apply ICE to sensitive files that are monitored through the Cloud channel on endpoints. You need to deploy the ICE Cloud Console to view and manage user access to protected files.

For more information, see Configuring the Endpoint Prevent: Encrypt action.

Discover features

The following discover features are new or improved in Symantec Data Loss Prevention 15.1.

Grid scanning for SharePoint targets

The grid scanning feature in Network Discover now supports Microsoft SharePoint server scan targets. Grid scanning enables Symantec Data Loss Prevention to run scans more efficiently by distributing the workload across multiple detection servers.

When you configure grid scanning, you must select least at two detection servers for the grid scanning feature to function. When you initiate a grid scan, one detection server is designated as the grid leader, which locates all of the items in the SharePoint repository and sends their URLs to the other detection servers in the grid. The other detection servers then attempt to download the contents of the repository and attempt to discover confidential information in the scan target. When a violation is detected, the detection servers submit an incident to the Enforce Server. The grid leader sends updates about the status of the scan to the Enforce Server, manages the incremental index, and updates all scan statistics.

For more information see these Help topics:

- About grid scanning
- Configuring grid scanning
- Configuring and running SharePoint server scans

Performance and scalability guidelines for SharePoint grid scanning

The documentation for Symantec Data Loss Prevention 15.1 includes performance and scalability guidelines for running grid scans on SharePoint scan targets.
Configure Network Protect to quarantine confidential files in Microsoft SharePoint repositories

You can configure Network Protect to quarantine of Microsoft SharePoint files directly in the Enforce Server administration console. In previous versions of Symantec Data Loss Prevention, you had to install and configure a FlexResponse plug-in to quarantine SharePoint files. You no longer need to install, configure, and use the FlexResponse plug-in.

To quarantine SharePoint files using an Automatic Response rule, you choose the Network Protect: Quarantine File response action. In addition, when you configure a SharePoint scan target, you provide details about the quarantine location on the Protect tab of the scan target.

To quarantine SharePoint files using a Smart Response rule, select the Network Protect: SharePoint Quarantine action.

The Symantec Data Loss Prevention SharePoint Quarantine FlexResponse plug-in is no longer supported as of this release. Beginning with version 15.1, you must use the Network Protect: Quarantine File response action in Network Protect to automatically quarantine confidential files instead of the SharePoint Quarantine FlexResponse plug-in.

To quarantine SharePoint files using Network Protect, existing users must first uninstall the Symantec Data Loss Prevention SharePoint Quarantine FlexResponse plug-in.

To release confidential SharePoint files from quarantine, you must continue to install and use the Symantec Data Loss Prevention SharePoint Release from Quarantine FlexResponse plug-in.

For information about installing and uninstalling the FlexResponse plug-ins, refer to the Symantec Data Loss Prevention SharePoint Quarantine FlexResponse Plug-in Implementation Guide.

For more information, see these topics:

- Configuring and running SharePoint server scans
- Configuring Network Protect for SharePoint servers
- Configuring the SharePoint Quarantine smart response action

Network features

The following network features are new or improved in Symantec Data Loss Prevention 15.1.
Secure ICAP for Network Prevent for Web with Blue Coat ProxySG

Secure ICAP is now available for Network Prevent for Web with Blue Coat ProxySG; it replaces stunnel.

You can configure Secure ICAP on the Configure Server page by selecting Secure ICAP when you add a Network Prevent for Web Server. You also must have a keystore configured and provide the keystore password. You set up the client configuration in Blue Coat ProxySG.

See Network Prevent for Web Server - basic configuration in the Help.

Increase in character limits of the Network IP filter and Sender filter for Network Monitor

There is an increase in the number of characters that can be used for the Network IP source filter, the IP destination filter, the L7 Sender filter, and the L7 Recipient filter for protocols used by the Network Monitor configuration. The old limit was 2048 characters; the new limit is 2800 characters.

Cloud features

The following cloud features are new or improved in Symantec Data Loss Prevention 15.1.

Easier update of email domains for Cloud Service for Email

You can quickly update the email domains of the corporate emails that you want Cloud Service for Email to scan without contacting Symantec Support to make the changes. This new capability only applies to emails sent from Microsoft Office 365 in reflecting mode.

When you add or remove a domain in the Enforce Server administration console, the new list is immediately sent to Symantec. All domains are verified and updated every 15 minutes by the Symantec Cloud Service.

See Updating email domains in the Help.

Encrypt email using Symantec ICE with Cloud Service for Email

Use Symantec Information Centric Encryption (ICE) capabilities to encrypt sensitive emails that are sent using monitored email applications such as on-premises Microsoft Exchange, Microsoft Office 365, and Gmail. ICE provides the capability to encrypt just the attachment, or the email and the attachment.

You set up ICE for email in the Enforce Server administration console and use the Encrypt action in your response rule. Incidents show up on the Incident Details page with links to the
ICE Cloud Console. You view and manage user access to protected files in the ICE Cloud Console.

For more information on deploying the ICE Cloud Console and setting up ICE, see the Symantec Information Centric Encryption Deployment Guide at http://www.symantec.com/docs/DOC9707.html.

See also Configuring the Enforce Server to connect to the Symantec ICE Cloud in the Help.

### Removed and deprecated platforms and capabilities

#### About deprecated platforms

Certain platforms are indicated as “deprecated.” That indicates that while the deprecated platform is supported in the current release, Symantec plans to remove support in an upcoming release. If your Symantec Data Loss Prevention environment includes a deprecated platform, you should plan on updating the platform to a later supported version or a different supported platform as soon as possible.

#### Support for stunnel

Support for stunnel is deprecated in version 15.1 and will be removed in a subsequent release. Beginning with Symantec Data Loss Prevention 15.1, you can reconfigure your system to use integrated Secure ICAP for Network Prevent for Web instead of stunnel.

#### Operating system support for servers

The following server operating systems are no longer supported:

- Red Hat Enterprise Linux 6.7.
  Windows Server 2012 R2 remains supported.

#### Symantec product integrations

Symantec Encryption Management Server (DLP Encryption Insight) version 3.3 is no longer supported.

#### Operating system support for endpoint systems

The following endpoint operating systems are no longer supported:

- Windows 7 Enterprise, Professional, Ultimate (32-bit) (initial release)
  Windows 7 Service Pack 1 remains supported.
Windows 7 Enterprise, Professional, Ultimate (64-bit) (initial release)
Windows 7 Service Pack 1 remains supported.

Windows 8 Enterprise PC operating system (64-bit)

macOS 10.10 (64-bit)

Deprecated operating systems for endpoint systems
The following endpoint operating systems are deprecated:

- Windows 10 Update Enterprise and Professional (64-bit) [1511]
- Windows 10 Red Stone Update Enterprise and Professional (64-bit) [1607 - RS1]

Exchange Server targets support
The following Exchange server targets are no longer supported:

- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2010 SP1
- Microsoft Exchange Server 2010 SP2

Deprecated Exchange Server targets
Microsoft Exchange Server 2007 SP3 is deprecated.

Deprecated Documentum Content Server targets
The following Documentum Content server targets are deprecated:

- 5.3.x
- 6.6.x
- 6.7

OpenText (Livelink) scanner targets support
Scanning support for OpenText (Livelink) Server 9.x targets is deprecated in 15.1.

Virtual desktop support with Endpoint Prevent
The following virtual desktops with Endpoint Prevent are no longer supported:

- Citrix XenDesktop 5.6
- VMware Workstation 6.5.x

**Endpoint Prevent application**

The following applications are no longer supported with Endpoint Prevent:
- Safari 9.1
- Internet Explorer 9
- Microsoft Office 2007

**Deprecated Endpoint Prevent application**

The Edge RS1 browser is deprecated.

**IBM (Lotus) Notes targets**

Lotus Notes versions 7.0 – 8.0 targets are no longer supported with Network Discover.

**SQL database targets**

DB2 9.1, 9.2, and 9.5 are no longer supported with Network Discover.

**Deprecated SQL database targets**

Oracle 10g is deprecated.

**SharePoint server targets**

The following SharePoint server targets are no longer supported:
- Microsoft Office SharePoint Server 2007 (all service packs)
- Microsoft Office SharePoint Server 2010
- Microsoft Office SharePoint Server 2010 SP1
- Microsoft Office SharePoint Server 2013
- Microsoft Office SharePoint Online 2010 (Dedicated mode)
- Microsoft Office SharePoint Online 2013 (Dedicated mode)
- Microsoft Office SharePoint Online 2016 (Dedicated mode)
Advanced Server settings

The following Advanced Server settings for configuring EDM policies are no longer supported:

- Lexer.MaxTokensPerMultiToken
- Lexer.StopwordLanguages