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.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

support.symantec.com

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
Available memory, disk space, and NIC information
Operating system
Version and patch level
Network topology
Router, gateway, and IP address information
Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration
If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service
Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:
  - Questions regarding product licensing or serialization
  - Product registration updates, such as address or name changes
  - General product information (features, language availability, local dealers)
  - Latest information about product updates and upgrades
  - Information about upgrade assurance and support contracts
  - Information about the Symantec Buying Programs
  - Advice about Symantec's technical support options
  - Nontechnical presales questions
  - Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan          customercare_apj@symantec.com
Europe, Middle-East, and Africa  seMEA@symantec.com
North America and Latin America  supportsolutions@symantec.com
Chapter 1  Introducing Data Insight for Data Loss Prevention ................................................................. 9
  About this guide ................................................................................................................................. 9
  About Data Insight ............................................................................................................................ 10
  Components of the Symantec Data Loss Prevention integration with
  Veritas Data Insight ......................................................................................................................... 11
  How Data Insight works with Data Loss Prevention ................................................................. 12
  What you can do with Veritas Data Insight and Symantec Data Loss
  Prevention ....................................................................................................................................... 13
  Where to get more information about Veritas Data Insight ..................................................... 15

Chapter 2  Enabling Data Insight to manage risk ................................................................. 17
  Locating and managing data at risk ............................................................................................... 17
  Implementing Data Insight for Data Loss Prevention to manage data
  a risk .............................................................................................................................................. 18
  Configuring the connection between the Enforce Server and Data
  Insight ........................................................................................................................................... 22
  About the Data Insight lookup plug-in ......................................................................................... 23
  Configuring Data Loss Prevention to retrieve attribute values from Data
  Insight ........................................................................................................................................... 25
  Mapping attributes to Data Insight data fields ............................................................................. 26
  Enabling the Data Insight lookup plug-in .................................................................................... 29
  Chaining the Data Insight lookup plug-in ..................................................................................... 29
  Enabling lookup plug-in parameter keys ...................................................................................... 30
  Testing the Data Insight lookup plug-in configuration ............................................................... 31
  Troubleshooting the Data Insight lookup plug-in ........................................................................ 32
  Changing Data Insight refresh intervals ....................................................................................... 34
  Best practices for finding and reporting on data at risk .......................................................... 34
Chapter 3  Finding data users and accesses in incident reports ................................................................. 36

Accessing reports of folders at risk .......................................................... 36
Configuring the risk score and timeframes for the report of folders at risk ...................................................................................... 39
Viewing folders ranked by risk, path, or folder exposure ....................... 40
Viewing details of a folder at risk ............................................................... 41
Filtering the information in the report of folders at risk .......................... 42
Saving a report of folders at risk ............................................................... 45
Finding data users and accesses in incident reports ............................... 46
Viewing Data Insight incident details ...................................................... 48
Accessing the history of a file in the Veritas Data Insight console .......... 49
Selecting custom attributes for data user details ..................................... 50
Creating summary reports for Data Insight .............................................. 51
Creating and distributing aggregated incident reports to data owners ........................................ 52

Chapter 4  Working with the Veritas Data Insight Self-Service Portal ................................................................. 56

About the Veritas Data Insight Self-Service Portal ..................................... 56
Configuring Symantec Data Loss Prevention for use with the Veritas Data Insight Self-Service Portal ................................................................. 57
Configuring the Response Rule Execution Service ................................. 58
Operational logs for the Response Rule Execution Service .................... 60
Introducing Data Insight for Data Loss Prevention

This chapter includes the following topics:

- About this guide
- About Data Insight
- Components of the Symantec Data Loss Prevention integration with Veritas Data Insight
- How Data Insight works with Data Loss Prevention
- What you can do with Veritas Data Insight and Symantec Data Loss Prevention
- Where to get more information about Veritas Data Insight

About this guide

The Symantec Data Loss Prevention Data Insight Implementation Guide describes how Veritas Data Insight can be integrated with Symantec Data Loss Prevention to locate and manage data at risk in your enterprise. This guide describes how to connect the Enforce Server to the Data Insight Management Server, how to configure the Data Insight Lookup Plug-in to retrieve pertinent data and populate incident attributes, and how to configure the risk score and timeframes to report data at risk. This guide also describes how to configure Symantec Data Loss Prevention for use with the Veritas Data Insight Self-Service Portal.

This guide does not address topics related to installing or configuring Veritas Data Insight (including the Self-Service Portal), or topics involving Symantec Data Loss Prevention that are not specific to Veritas Data Insight integration with Symantec Data Loss Prevention.
Symantec is an authorized reseller of the Veritas Data Insight software product and related support and maintenance. The Veritas Data Insight software product is subject to the end user license agreement accompanying the software, and the Veritas support offering details can be found at: https://www.veritas.com/content/support/en_US/terms/support-fundamentals.html, or successor URL. Customers may receive technical support by contacting Symantec Customer Care to verify their entitlement prior to being transferred to Veritas Customer Care for technical assistance.

About Data Insight

Many organizations struggle with identifying data users and owners for their unstructured data. This challenge is compounded with the fact that organizations lack visibility into the types of content and data that is spread across their computing environment.

With Veritas Data Insight, users can monitor file access to automatically identify the data user of a file based on the access history. The usage information then automatically enters into the incident detail of files that violate Symantec Data Loss Prevention policies. This method enables users to identify sensitive data along with the responsible users to enable more efficient remediation and data management.

Veritas Data Insight scans unstructured data systems and collects the full access history of users across the data. Veritas Data Insight helps organizations monitor and report on access to sensitive information.

Veritas Data Insight helps organizations solve the problem of identifying data owners and responsible parties for information in spite of incomplete or inaccurate metadata or tracking information. This helps support large-scale business owner-driven remediation processes and workflows.

See “What you can do with Veritas Data Insight and Symantec Data Loss Prevention” on page 13.

Veritas Data Insight can provide the following information:

- Who owns the data
- Who is responsible for remediation
- Who has seen the data
- Who has access to the data
- What data is most at risk
- Frequency of usage of data
The Veritas Data Insight information that contains the access history of data users is available to Symantec Data Loss Prevention. If the access history on a file is recorded, a data user can be identified in a Network Discover incident.

The **Folder Risk Report** ranks folders based on number of files with policy violations, severity weightings, folder exposure, and actual user accesses on sensitive data. This report provides a mechanism to focus on the folder assets with the largest volume of data and highest risk of data exposure. The report helps Symantec Data Loss Prevention remediators drive down risk in the fastest possible manner.

See “Accessing reports of folders at risk” on page 36.

Symantec Data Loss Prevention queries Veritas Data Insight for the data user of a file and other access history attributes like the last modifying user. This access history information is available in the Symantec Data Loss Prevention incident snapshot as custom attributes.

The data user information from Veritas Data Insight can also be assigned to the **Data Owner Name** field, to enable the automatic distribution of aggregated incident reports to data owners for remediation.

See “Creating and distributing aggregated incident reports to data owners” on page 52.

Data owners and custodians can remediate Symantec Data Loss Prevention Network Discover file-system and SharePoint incidents directly using the Self-Service Portal in Veritas Data Insight. You can configure a workflow in Veritas Data Insight to send email alerts to data owners or custodians about policy violations. They can then log in to the Self-Service Portal to view the policy violations and remediate Symantec Data Loss Prevention incidents using Smart Response rules.

See “About the Veritas Data Insight Self-Service Portal” on page 56.

**Components of the Symantec Data Loss Prevention integration with Veritas Data Insight**

Veritas Data Insight monitors file access to automatically identify the data user of a file based on the access history. The summary of access history information then automatically feeds into the incident detail of files that violate Symantec Data Loss Prevention policies.

These components are integrated to provide data user information for the Network Discover incidents.

See “How Data Insight works with Data Loss Prevention” on page 12.

The following components are integrated to provide data user information for incident remediation.
### Table 1-1  Data Insight integration components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Veritas Data Insight</strong></td>
<td>Veritas Data Insight scans unstructured data systems (Network Attached Storage (NAS) filers, Windows file servers, SharePoint). It reports on the access history of various users across files and folders. Support for SharePoint is available beginning with Veritas Data Insight version 4.0. Using the Self-Service Portal provided by Veritas Data Insight, data owners and custodians can remediate incidents directly, without needing access to the Symantec Data Loss Prevention Enforce Server administration console. The Self-Service Portal is available beginning with Veritas Data Insight version 4.5.</td>
</tr>
<tr>
<td><strong>Symantec Data Loss Prevention Network Discover</strong></td>
<td>Network Discover scans file shares on the unstructured data systems. It identifies confidential information as Network Discover incidents.</td>
</tr>
<tr>
<td><strong>Symantec Data Loss Prevention Enforce Server</strong></td>
<td>Symantec Data Loss Prevention queries Veritas Data Insight for the data user of a file and other access history attributes like the last modifying user. Symantec Data Loss Prevention provides users of the Veritas Data Insight Self-Service Portal with the ability to view and execute incident remediation response rules.</td>
</tr>
</tbody>
</table>

### How Data Insight works with Data Loss Prevention

*Figure 1-1* shows the flow of information between the Veritas Data Insight Management Server and the Symantec Data Loss Prevention servers.

Veritas Data Insight scans unstructured data systems and stores information about the access history across files and folders.

A Network Discover Server scans the files and folders in unstructured data systems to expose confidential data. Information about the exposed confidential data is stored on the Symantec Data Loss Prevention Enforce Server. With the activation of a license for Veritas Data Insight, a lookup plug-in on the Enforce Server pulls data user information from the Veritas Data Insight Management Server. This data user information populates custom attributes for a Network Discover incident at the time the incident is generated.
What you can do with Veritas Data Insight and Symantec Data Loss Prevention

Table 1-2 describes the use cases of Veritas Data Insight to enable more efficient incident remediation. You use the Network Discover incident report options to identify the data owners to notify about these incidents.

See “Finding data users and accesses in incident reports” on page 46.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prioritize remediation of folders.</td>
<td>The <strong>Folder Risk Report</strong> ranks folders based on number of files with policy violations, severity weightings, folder exposure, and actual user accesses on sensitive data. This report provides a mechanism to focus on the folder assets with the largest volume of data and highest risk of data exposure. The report helps Symantec Data Loss Prevention remediators drive down risk in the fastest possible manner. The <strong>Folder Risk Report</strong> is only available for file system Discover targets.</td>
</tr>
</tbody>
</table>
Table 1-2  What you can do with Veritas Data Insight (continued)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and automatically distribute aggregated incident reports to data owners for remediation.</td>
<td>Data-owner remediation reports provide a scalable method of remediating large numbers of incidents. You can aggregate incidents into a single incident report for each data owner on an ad hoc or scheduled basis and then email the remediation reports (as a CSV or HTML attachment) to the respective custodians or data owners.</td>
</tr>
<tr>
<td>Identify the data owner.</td>
<td>File owner information may not reflect the responsible party. The responsible party or data owner can be a line manager in the business unit, the head of a department, or an information security officer. Veritas Data Insight provides information to tie the most active user of a file to a manager or responsible party for remediation steps.</td>
</tr>
<tr>
<td>Identify the next-best owner.</td>
<td>The <strong>Data Owner</strong> field may return an unresolvable account for an individual that has left the organization. For example, in Windows Active Directory, every user has an underlying unique identifier that is associated with their account. This identifier is sometimes an unidentifiable string of information. Veritas Data Insight provides information to drop down to the next resolvable account that names an individual.</td>
</tr>
<tr>
<td>Identify the data custodian.</td>
<td>Veritas Data Insight enables assignment of one or more users as custodians of a data repository. Custodian tagging is typically used to determine the person responsible for remediation. The assigned custodian need not have accessed the files and folders. Support for custodian information is available beginning with Veritas Data Insight version 4.0.</td>
</tr>
<tr>
<td>Investigate a data leak.</td>
<td>In the event of a data leak, you may want to know who saw a particular file. You can run a Symantec Data Loss Prevention summary report by the data user custom attribute. Also, incident snapshots provide information to tie the incident back to the Veritas Data Insight Management Server. On the Veritas Data Insight Management Server, you can view detailed information and an audit history of who accessed the data. You can also view correlations to similar incidents. Additional remediation steps can then be taken to report on those individuals or launch subsequent targeted scans on their assets.</td>
</tr>
</tbody>
</table>
Table 1-2  What you can do with Veritas Data Insight (continued)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and automatically distribute</td>
<td>The Veritas Data Insight Self-Service Portal allows you to distribute the remediation workflow directly to data owners and custodians. The Self-Service Portal allows data owners and custodians to view policy violations and apply Smart Response rules without requiring access to the Symantec Data Loss Prevention Enforce Server administration console. The Self-Service Portal is available beginning with Veritas Data Insight version 4.5.</td>
</tr>
<tr>
<td>remediation workflows to data owners and</td>
<td></td>
</tr>
<tr>
<td>custodians</td>
<td></td>
</tr>
</tbody>
</table>

Where to get more information about Veritas Data Insight

You must target a file share on a filer that is supported for both Veritas Data Insight and Symantec Data Loss Prevention. The supported filers and supported client protocols (such as CIFS) are listed in the following documentation:

- Veritas Data Insight supports specific filers.
  For a list of the supported filers, see the Veritas Data Insight Installation Guide.

- Network Discover scans of file systems support specific client protocols.
  For a list of the supported client protocols, see the Symantec Data Loss Prevention Administration Guide, in the section "Supported file share targets."

Veritas Data Insight only scans SharePoint Document and Picture Libraries. Support for SharePoint data is available beginning with Veritas Data Insight version 4.0.

The following documentation provides more information about Veritas Data Insight:

- Veritas Data Insight Installation Guide
  Explains how to install Veritas Data Insight.

- Veritas Data Insight Administrator’s Guide
  Explains how to configure and administer Veritas Data Insight using the management console. Explains how to gather the access history of the data users. Explains how to configure and customize the Self-Service Portal.

- Veritas Data Insight User’s Guide
  Explains the Veritas Data Insight views that display data access information on folders and by users or groups. Explains how to set up Veritas Data Insight reports. Explains how to use the Self-Service Portal to remediate Symantec Data Loss Prevention incidents.
The following documentation provides information about the setup to identify data users in the Symantec Data Loss Prevention product using the information from Veritas Data Insight:

- **Symantec Data Loss Prevention System Requirements Guide**
  Provides the requirements for the disk space for the Veritas Data Insight information on the Enforce Server.

- **Symantec Data Loss Prevention Installation Guide**
  Explains how to install the Symantec Data Loss Prevention product.

- **Symantec Data Loss Prevention Administration Guide**
  Explains how to configure and run the scan of a Network Discover Box cloud storage, file system, or SharePoint target, and how to set up reports. Explains how to configure other lookup plug-ins, including CSV, LDAP, and Script Lookup Plug-ins.
Enabling Data Insight to manage risk

This chapter includes the following topics:

- Locating and managing data at risk
- Implementing Data Insight for Data Loss Prevention to manage data at risk
- Configuring the connection between the Enforce Server and Data Insight
- About the Data Insight lookup plug-in
- Configuring Data Loss Prevention to retrieve attribute values from Data Insight
- Mapping attributes to Data Insight data fields
- Enabling the Data Insight lookup plug-in
- Chaining the Data Insight lookup plug-in
- Enabling lookup plug-in parameter keys
- Testing the Data Insight lookup plug-in configuration
- Troubleshooting the Data Insight lookup plug-in
- Changing Data Insight refresh intervals
- Best practices for finding and reporting on data at risk

Locating and managing data at risk

To locate and manage data at risk using Veritas Data Insight, use the following processes:
- Set up, create, and automatically distribute aggregated incident reports to data owners for remediation. See “Creating and distributing aggregated incident reports to data owners” on page 52. See “Finding data users and accesses in incident reports” on page 46.

- Retrieve the data user from the Veritas Data Insight Management Server into the Data Owner Name field in Discover incidents. Then use the Discover reports to locate and manage the incidents. See Table 2-1 on page 18. See Table 2-2 on page 20.

- Retrieve details about file use from the Veritas Data Insight Management Server into the custom attributes in the Discover incidents, to provide additional fields in the Discover reports to locate and manage the incidents. See Table 2-1 on page 18. See Table 2-3 on page 21.

## Implementing Data Insight for Data Loss Prevention to manage data a risk

To set up the connection to the Veritas Data Insight Management Server, complete the following process:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Install and configure the Veritas Data Insight Management Server. | Make sure that the Veritas Data Insight Management Server has access to the files or file systems of interest. See the following Veritas Data Insight documentation:  
  - Veritas Data Insight Installation Guide  
  - Veritas Data Insight Administrator’s Guide |
| 2    | Install and configure Symantec Data Loss Prevention. | You must install and configure at least one Network Discover Server. See the Symantec Data Loss Prevention Installation Guide. |
Table 2-1 Configuring a Data Insight connection (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3    | Configure a connection between the Enforce Server and Veritas Data Insight. | Veritas Data Insight is a separately licensed option. If Veritas Data Insight is not licensed on the Enforce Server, the menu option to configure the connection to the Veritas Data Insight Management Server does not appear.  
If you add the Veritas Data Insight license onto an existing Enforce Server, you must restart the Incident Persister service to enable incident lookup.  
See “Configuring the connection between the Enforce Server and Data Insight” on page 22. |
| 4    | Test the connection to Veritas Data Insight.                           | Verify the connection between the Enforce Server and the Veritas Data Insight Management Server.  
See “Troubleshooting the Data Insight lookup plug-in” on page 32.                                                                                                                                  |
| 5    | Install and configure the Self-Service Portal.                        | Install and configure the Self-Service Portal on the Veritas Data Insight side. The Self-Service Portal is available beginning with Veritas Data Insight version 4.5.  
See the following Veritas Data Insight documentation:  
- *Veritas Data Insight Administrator’s Guide*  
Configure Symantec Data Loss Prevention for integration with the Self-Service Portal.  
See “About the Veritas Data Insight Self-Service Portal” on page 56.                                                                 |

To retrieve details about file use into the **Data Owner Name** field, first complete the setup in Table 2-1, then complete the following steps:
## Table 2-2 Configuring the Data Insight lookup plug-in to retrieve data owner details from Data Insight

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Configure the Data Insight lookup plug-in to retrieve Data Owner details. | Configure the Data Insight lookup plug-in to retrieve the Veritas Data Insight data user directly into the **Data Owner Name** field in the Discover incidents.  
   See “Configuring Data Loss Prevention to retrieve attribute values from Data Insight” on page 25. |
| 2    | Configure other lookup plug-ins to populate the Data Owner Email field. | Configure other lookup plug-ins as necessary to set the **Data Owner Email Address** field, or other custom attributes.  
   You can chain the LDAP, the CSV, or Script lookup plug-ins with the Data Insight lookup plug-in to set the **Data Owner Email Address** field.  
   Refer to the *Symantec Data Loss Prevention Administration Guide* for details on configuring these plug-ins. |
| 3    | Scan the file systems or SharePoint servers of interest.              | To set up a Network Discover scan of the file systems or SharePoint servers of interest, see the *Symantec Data Loss Prevention Administration Guide*. Support for SharePoint targets is available with Veritas Data Insight version 4.0 or later. |
| 4    | Test the plug-ins.                                                    | Test that the details from the Veritas Data Insight Management Server populate the **Data Owner Name** field.  
   View the incident reports to verify that the expected information is present.  
   See “Finding data users and accesses in incident reports” on page 46. |

To retrieve details from Veritas Data Insight about file use into custom attributes, complete the setup in Table 2-1, then complete the following steps:
### Configuring the Data Insight lookup plug-in to retrieve custom attribute values from Data Insight

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create custom attributes.</td>
<td>On the Enforce Server, create custom attributes for each file detail that you want retrieved from the Veritas Data Insight Management Server. See “About the Data Insight lookup plug-in” on page 23. Refer to the <em>Symantec Data Loss Prevention Administration Guide</em> for details on configuring custom attributes.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the Data Insight lookup plug-in and others you want to implement.</td>
<td>Configure the Data Insight lookup plug-in as well as any other lookup plug-ins you want to implement. See “Configuring Data Loss Prevention to retrieve attribute values from Data Insight” on page 25. Refer to the <em>Symantec Data Loss Prevention Administration Guide</em> for details on configuring the CSV, LDAP, and Script lookup plug-ins.</td>
</tr>
<tr>
<td>3</td>
<td>Map the attributes.</td>
<td>Map the details from the Veritas Data Insight Management Server to the custom attributes that you created. See “Mapping attributes to Data Insight data fields” on page 26.</td>
</tr>
<tr>
<td>4</td>
<td>Scan the file systems, SharePoint servers, or Box accounts you want to protect.</td>
<td>Set up a Network Discover/Cloud Storage Discover scan of the file systems or SharePoint servers of interest. Support for SharePoint targets is available with Veritas Data Insight version 4.0 or later. See the <em>Symantec Data Loss Prevention Administration Guide</em> for configuring Discover scans.</td>
</tr>
<tr>
<td>5</td>
<td>Test the plug-ins.</td>
<td>Test that the details from the Veritas Data Insight Management Server populate your custom attributes. View the incident reports to verify that the expected information is present. See “Finding data users and accesses in incident reports” on page 46.</td>
</tr>
</tbody>
</table>
Configuring the connection between the Enforce Server and Data Insight

Before you can use the information from Veritas Data Insight, you need to configure the connection to the Veritas Data Insight Management Server.

You can also optionally configure the risk score and other options for the report of folders at risk. The risk score is based on relevant information from the Symantec Data Loss Prevention incidents plus the information from the Veritas Data Insight Management Server.

To configure the connection to the Veritas Data Insight Management Server

1. Click **System > Settings > Data Insight** from the Enforce Server administration console.

   If Veritas Data Insight is not licensed on the Enforce Server, this menu option does not appear.

   If you add the Veritas Data Insight license onto an existing Enforce Server, you must restart the Incident Persister service to enable the Veritas Data Insight lookups and the data owner lookups for incidents.

2. Click **Configure**.

3. Enter the **Host Name** of the Veritas Data Insight Management Server. The **Host Name** may need to match the host name in the certificate.

4. Enter the **Port** number of the Veritas Data Insight Management Server. The default is 443.

5. Click **Retrieve Certificate**.

   This retrieval sends a request to the specified Veritas Data Insight Management Server to obtain its SSL certificate.

6. Click **Yes** to trust the certificate.

   Verify that the certificate is returned from the Veritas Data Insight Management Server and that is the correct certificate.

7. Enter the log on information to the Veritas Data Insight Management Server.

   - Select **Use Saved Credentials** to use a credential that is saved in the credential store.
     
     Then enter the name of the saved credential.

   - Select **Use These Credentials** to enter the credentials here.

   - Enter the **Username and Password**, and **Re-enter Password**.
8 Click **Test Connection** to verify the connection to the Veritas Data Insight Management Server.

This tests the connection to the Veritas Data Insight Management Server using the specified credentials. This **Test Connection** operation is available only after the server certificate is verified. If the test is successful, the system displays the message: "The test connection succeeded." If the test is not successful, verify the connection parameters and credentials.

9 Optionally, you can configure the risk score and timeframes for the report of folders at risk. Generally, the defaults are acceptable.

See “Configuring the risk score and timeframes for the report of folders at risk” on page 39.

10 Optionally, you can also configure the data refresh schedule to retrieve the information from the Data Insight Management Server.

See “Changing Data Insight refresh intervals” on page 34.

---

**About the Data Insight lookup plug-in**

The Data Insight lookup plug-in pulls data from a Veritas Data Insight Management Server. It then uses that data to populate custom attributes for a Network Discover incident at the time the incident is generated. The Data Insight lookup plug-in connects Symantec Data Loss Prevention with Veritas Data Insight to retrieve attribute values. Data Insight can be used to provide granular context to incidents, including up-to-date data owner information.

**Note:** The Data Insight lookup plug-in requires a Data Insight license separate from Symantec Data Loss Prevention licensing. If your system is not licensed for Data Insight, the Data Insight lookup plug-in is not available.

See “About Data Insight” on page 10.

You must create custom attributes for each attribute you want populated from the Veritas Data Insight Management Server. You create only the custom attributes that you need. When an incident is created, the Enforce Server retrieves data regarding that incident. Some of that data is in the form of "attributes." Custom attributes capture and store supplemental data that is related to the incident, such as the name of a relevant manager or department. Refer to the *Symantec Data Loss Prevention Administration Guide* for details on creating custom attributes.

To populate custom attributes with the incident-related data, the Enforce Server uses the Data Insight lookup plug-in to retrieve the additional data from the Veritas Data Insight Management Server. You can chain the Data Insight lookup plug-in
with other plug-ins, such as the LDAP lookup plug-in, CSV lookup plug-in, or Script lookup plug-in. For example, you may want to do this to set the Data Owner Email Address field. If the new lookup returns null or empty values for any custom attribute fields, those empty values overwrite the existing values.

The values for the custom attributes are updated by clicking Lookup in the Attribute section of the Incident Snapshot screen. This action replaces the existing values that are stored in the custom attribute fields with the values returned by the new lookup. Refer to the Symantec Data Loss Prevention Administration Guide for details on using lookup plug-ins to remediate incidents.

The Veritas Data Insight lookup plug-in can retrieve the following information from the Veritas Data Insight Management Server:

- Data user. The data user is the user who most frequently accessed the file.
- Business owner as defined in the Veritas Data Insight product.
- Custodian. The custodian is the user who is responsible for remediation of the file. (Support for custodian information is available with Veritas Data Insight version 4.0 or later.)
- Custodian Folder. The URI of the file system or SharePoint folder to which the custodian is assigned. (Support for custodian folder information is available with Veritas Data Insight version 4.0 or later.)
- Data user last access time. The last time the data user accessed the file.
- Data user access count. The number of times the data user accessed the file.
- Most active users.
- Most active readers.
- Most active writers.
- Read and write counts for each of the most active users, readers, or writers.
- Last modified by.
- Last accessed time.
- Number of read accesses across all users.
- Number of write accesses across all users.
- The first time that access history was collected for this incident.

See “Configuring Data Loss Prevention to retrieve attribute values from Data Insight” on page 25.
Configuring Data Loss Prevention to retrieve attribute values from Data Insight

The System > Incident Data > Lookup Plugins page in the Enforce Server administration console is where you configure the Data Insight lookup plug-in. You can configure one Data Insight lookup plug-in per Enforce Server instance.

Table 2-4  Configuring the Data Insight lookup plug-in

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Create custom attributes. | Configure attribute status values and create custom attributes at the System > Incident Data > Attributes page. Refer to the Symantec Data Loss Prevention Administration Guide for details.  
Note: If you use only the data-owner-name attribute, you do not have to create a custom attribute. The data-owner-name attribute is generated by the system. |
| 2    | Configure a connection to Data Insight. | Set the host name, credentials, and parameters to connect to Data Insight.  
See “Configuring the connection between the Enforce Server and Data Insight” on page 22. |
| 3    | Create a new Data Insight lookup plug-in. | From the Enforce Server administration console, navigate to the System > Incident Data > Lookup Plugins page and select New Plugin > Data Insight. |
| 4    | Enter a Start Date. | If you leave this field empty, the system sets this field to oldest date for history possible, which is 1/1/1970. |
| 5    | Select the Active User Count. | You can specify between 0 and 10 active users. The default is 1. |
| 6    | Select the Active Reader Count. | You can specify between 0 and 10 active readers. The default is 1. |
| 7    | Select the Active Writer Count. | You can specify between 0 and 10 active writers. The default is 1. |
| 8    | Configure the Attribute Mapping. | The system provides you with an attribute mapping template for all the information exposed by Data Insight. A separate entry is made for each custom attribute to be populated. You enter the custom attribute to the right of the equals sign for each entry you want to map. For example, Data_User=attr.data-owner-name which is configured for you.  
See “Mapping attributes to Data Insight data fields” on page 26. |
### Table 2-4  Configuring the Data Insight lookup plug-in (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9    | Enable the plug-in. | See “Enabling the Data Insight lookup plug-in” on page 29.  
If you deploy multiple plug-ins, chain them as well.  
See “Chaining the Data Insight lookup plug-in” on page 29. |
| 10   | Enable the lookup parameter keys. | For example, if you use the `data-owner-name` attribute, select the **Incident** key.  
You can select more than one key, but since each attribute group is a separate hit against the Symantec Data Loss Prevention database, you should only select those keys you need.  
See “Enabling lookup plug-in parameter keys” on page 30. |
| 11   | Test and troubleshoot the plug-in. | See “Testing the Data Insight lookup plug-in configuration” on page 31.  
See “Troubleshooting the Data Insight lookup plug-in” on page 32. |

## Mapping attributes to Data Insight data fields

Custom attributes are mapped to Veritas Data Insight information with entries in the **Attribute Mapping** field for the Data Insight lookup plug-in. Each mapping is entered on a separate line in the field. The order in which these mapping entries appear in the field does not matter.

If you use the Data Insight lookup plug-in to retrieve the data owner, this attribute is mapped for you (`Data_User=attr.data-owner-name`). You can also define a mapping for an arbitrary custom attribute that a subsequent plug-in in the lookup plug-in chain uses. Thus, for all other data fields except `data-owner-name`, you need to create custom attributes.

The syntax for Data Insight attribute mapping is as follows:

\[
\text{Veritas Data Insight property} = \text{attr. Custom Attribute Name}
\]

Where:

- **Veritas Data Insight property**  
The Veritas Data Insight property whose data value is returned to the Enforce Server. This value is used to populate the custom attribute that is specified in the attribute mapping.

- **Custom Attribute Name**  
The name of the custom attribute as it is defined in the Enforce Server.
Note: If the name of the attribute contains white-space characters, you must precede each instance of the white space with a backslash. A white-space character is a space or a tab. For example, you need to enter the `Total Writes` custom attribute as: `attr.Total\ Writes`.

Here are some additional mapping examples:

File_Total_Writes = attr.Total\ Writes  
File_Total_Reads = attr.Total\ Reads  
File_Total_Writes = attr.Total\ Writes  
File_Last_Modified_By = attr.Last\ Modified\ By  
File_Last_Access_Date = attr.Last\ Accessed

All dates are in the `YYYY-MM-DD hh:mm` format (ISO 8601). The date is displayed in the time zone of the Enforce Server.

All names and users are in the format `domain\username`.

The following table describes the attribute mapping details for the Data Insight lookup plug-in.

Note: For more than two users, replace "n" with the user number. For example, enter `Most_Active_Reader_3`.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data_User</td>
<td>Attribute that corresponds to the data user. This person uses the file most frequently. The person who uses the file most frequently may not be the person who created the file.</td>
</tr>
<tr>
<td>Business_Owner</td>
<td>Custom attribute that corresponds to the business owner of the data user as defined in the Veritas Data Insight Management Server.</td>
</tr>
<tr>
<td>Custodian_1</td>
<td>Custom attribute that corresponds to the remediator of the file. (Support for custodian information is available with Veritas Data Insight version 4.0 or later.)</td>
</tr>
<tr>
<td>Custodian_Folder_1</td>
<td>Custom attribute that corresponds to the URI of the file system or SharePoint folder to which the custodian is assigned. (Support for custodian folder information is available with Veritas Data Insight version 4.0 or later.)</td>
</tr>
<tr>
<td>Data&gt;User_Last_Access</td>
<td>Custom attribute that corresponds to the last time that the data user accessed a file. The format is <code>YYYY-MM-DD hh:mm UTC+/−hh</code>.</td>
</tr>
<tr>
<td>Data_User_Reads</td>
<td>Custom attributes that correspond to the read access count of the data user.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Data_User_Writes</td>
<td>Custom attributes that correspond to the write access count of the data user.</td>
</tr>
<tr>
<td>File_Access_History_Start_Date</td>
<td>Custom attribute that corresponds to the first time that access history for the file was collected.</td>
</tr>
<tr>
<td>File_Last_Access_Date</td>
<td>Custom attribute that corresponds to the last time the file was accessed.</td>
</tr>
<tr>
<td>File_Last_Modified_By</td>
<td>Custom attribute that corresponds to the last user who modified the file.</td>
</tr>
<tr>
<td>File_Total_Reads</td>
<td>Custom attribute that corresponds to the total number of read accesses.</td>
</tr>
<tr>
<td>File_Total_Writes</td>
<td>Custom attribute that corresponds to the total number of write accesses.</td>
</tr>
<tr>
<td>Most_Active_Reader_1</td>
<td>Custom attributes that correspond to the most active readers. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_Reader_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Reader_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Reader_Reads_1</td>
<td>Number of reads from the most active readers. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_Reader_Reads_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Reader_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Reader_Writes_1</td>
<td>Number of writes from the most active readers. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_Reader_Writes_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Reader_Writes_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_User_1</td>
<td>Custom attributes that correspond to the most active user. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_User_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_User_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_User_Reads_1</td>
<td>Number of reads from the most active users. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_User_Reads_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_User_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_User_Writes_1</td>
<td>Number of writes from the most active users. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_User_Writes_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_User_Writes_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Writer_1</td>
<td>Custom attributes that correspond to the most active writers. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_Writer_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Writer_n</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-5  
Data Insight attribute mappings (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most_Active_Writer_Reads_1</td>
<td>Number of reads from the most active writers. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_Writer_Reads_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Writer_Reads_n</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Writer_Writes_1</td>
<td>Number of writes from the most active writers. You can add any number of active readers to the mapping.</td>
</tr>
<tr>
<td>Most_Active_Writer_Writes_2</td>
<td></td>
</tr>
<tr>
<td>Most_Active_Writer_Writes_n</td>
<td></td>
</tr>
</tbody>
</table>

### Enabling the Data Insight lookup plug-in

To enable the Data Insight lookup plug-in you must enable it.

**To enable the Data Insight lookup plug-in**

1. Navigate to **System > Incident Data > Lookup Plugins** in the Enforce Server administration console.
2. Click **Modify Plugin Chain** at the **Lookup Plugins List Page**.
3. In the **Dedicated Actions** field, select (check) the **On** option.
4. Click **Save** to apply the configuration.

If the plug-in cannot be loaded the system reports an error and the plug-in state remains **Off**.

### Chaining the Data Insight lookup plug-in

The Veritas Data Insight lookup plug-in can be used in combination with other types of lookup plug-ins. When multiple lookup plug-ins are chained together, output from a previous lookup plug-in can be used as a key to retrieve additional information.

The Data Insight lookup plug-in can be used in combination with other Data Loss Prevention lookup plug-ins. This is known as "chaining." When multiple lookup plug-ins are chained together, output from a previous lookup plug-in is used as a key to retrieve additional information. For example, commonly Data Insight is used to populate the data-owner-name attribute. Another lookup plug-in, such as the LDAP lookup plug-in, is then chained to look up the data-owner-email value which is based on the data-owner-name value. As another example, the Veritas Data Insight lookup plug-in provides the most active user as a custom attribute in the **Incident Snapshot**. Another lookup plug-in (such as the LDAP lookup plug-in)
can then retrieve related information for that user, such as the department or the manager’s email.

See the Symantec Data Loss Prevention Administration Guide for additional information about chaining lookup plug-ins.

To chain the Data Insight lookup plug-in

1. Navigate to System > Incident Data > Lookup Plugins in the Enforce Server administration console.
2. Click Modify Plugin Chain at the Lookup Plugins List Page.
3. In the Execution Sequence field, select the execution order from the drop-down menu.
4. Click Save to apply the chaining configuration.

Enabling lookup plug-in parameter keys

The System > Incident Data > Lookup Plugins > Edit Lookup Plugin Parameters page lists the Lookup Parameter Keys that you select to trigger the lookup of attribute values. Lookup parameter keys are organized into attribute groups. The selections made at this screen apply to all the lookup plug-ins deployed on the Enforce Server.

To perform a lookup, you must map at least one lookup parameter key to a field in your external data source. Each lookup parameter group that you enable is a separate database query for the Enforce Server to perform. All database queries are executed for each incident before lookup. To avoid the performance impact of unnecessary database queries, you should only enable attribute groups that your lookup plug-ins require.

Because the plug-in stops searching after it finds the first matching lookup parameter key-value pair, the order in which you list the keys in your attribute map is significant. Refer to the attribute mapping examples for the specific type of plug-in you implement for details.

Note: Refer to the Symantec Data Loss Prevention Administration Guide for details on lookup plug-in parameter keys.

To enable one or more lookup parameter keys

1. Navigate to System > Incident Data > Lookup Plugins in the Enforce Server administration console.
2. Click Lookup Parameters at the Lookup Plugins List Page.
3 Select (check) one or more attribute groups at the **Edit Lookup Plugin Parameters** page. 

Click **View Properties** to view all of the keys for that attribute group. 

See **Table 2-6** on page 31.

4 **Save** the configuration. 

Verify the success message indicating that all enabled plug-ins were reloaded.

### Table 2-6 Lookup parameter keys

<table>
<thead>
<tr>
<th>Attribute group</th>
<th>Lookup parameter keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>attachment-nameX, attachment-sizeX</td>
</tr>
<tr>
<td>Incident</td>
<td>date-detected, incident-id, protocol, data-owner-name, data-owner-email</td>
</tr>
<tr>
<td>Policy</td>
<td>policy-name</td>
</tr>
<tr>
<td>Recipient</td>
<td>recipient-emailX, recipient-ipX, recipient-urlX</td>
</tr>
<tr>
<td>Sender</td>
<td>sender-email, sender-ip, sender-port, endpoint-user-name, endpoint-machine-name</td>
</tr>
<tr>
<td>Server</td>
<td>server-name</td>
</tr>
<tr>
<td>Monitor</td>
<td>monitor-name, monitor-host, monitor-id</td>
</tr>
<tr>
<td>Status</td>
<td>incident-status</td>
</tr>
<tr>
<td>ACL</td>
<td>acl-principalX, acl-typeX, acl-grant-or-denyX, acl-permissionX</td>
</tr>
</tbody>
</table>

### Testing the Data Insight lookup plug-in configuration

Follow these steps to test the Data Insight lookup plug-in.
Testing the Data Insight lookup plug-in

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a file share Discover Target.</td>
<td>Set up the Discover Target to scan a Data Insight file share. Refer to the <em>Symantec Data Loss Prevention Administration Guide</em> for instructions.</td>
</tr>
<tr>
<td>2</td>
<td>Create a test policy.</td>
<td>For example, you can create a keyword policy that uses the word &quot;secret&quot; as the keyword. Refer to the <em>Symantec Data Loss Prevention Administration Guide</em> for instructions.</td>
</tr>
<tr>
<td>4</td>
<td>Run the Discover Target.</td>
<td>Check the Incident Snapshot for the Discover incident. Verify that for any attributes you mapped, you should see that they are populated. For example, if you mapped the data-owner-name attribute, you should that the Data Owner Name field is populated.</td>
</tr>
<tr>
<td>5</td>
<td>Verify attribute lookup.</td>
<td>Check the Incident Snapshot for the Discover incident. Verify that for any attributes you mapped, you should see that they are populated. For example, if you mapped the data-owner-name attribute, you should that the Data Owner Name field is populated.</td>
</tr>
<tr>
<td>6</td>
<td>Troubleshoot the plug-in as necessary.</td>
<td>To troubleshoot, check the log file SymantecDLP\Protect\logs\tomcat\localhost.latest_date.log.</td>
</tr>
</tbody>
</table>

Troubleshooting the Data Insight lookup plug-in

If the Data Insight lookup plug-in is not working, troubleshoot it as follows.

**To test the connection to the Data Insight Management Server**

1. Configure the connection from the Enforce Server to the Veritas Data Insight Management Server.
   
   See "Configuring the connection between the Enforce Server and Data Insight" on page 22.

2. On the System > Settings > Data Insight page, click Test Connection to verify the connection to the Veritas Data Insight Management Server.
   
   This tests the connection to the specified Veritas Data Insight Management Server using the specified credentials. This connection is available only after the server certificate is verified.

3. Configure and enable all the lookup plug-ins.

4. Click Reload Lookup Plugins to reload all the lookup plug-ins from the Custom Attributes tab of the System > Incident Data > Attributes screen.
5 View an existing incident snapshot. Click the **Lookup** option on the incident snapshot.

6 Make sure that no connection errors are recorded in the **Incident History** section.

**To verify that the custom attributes are correctly populated**

1 Verify that the custom attributes have been created.

   Select **System > Incident Data > Attributes > Custom Attributes**.

   Verify that all the custom attributes exist in the list of custom attributes in the user interface.

2 Click **Reload Lookup Plugins** to reload the plug-in from the **Custom Attributes** tab of the **System > Incident Data > Attributes** screen.

3 Click the **Lookup** option for an existing Incident Snapshot.

4 When the page returns, view the **Attributes** area from the **Incident Snapshot** page.

   - The Custom Attributes should be filled with entries retrieved from the Veritas Data Insight lookup.
   - If the correct values are not populated, or there is no value in a custom attribute you have defined, check the Tomcat log file for mismatched items.

**To check the log files**

1 Open the log file

   `SymantecDLP\Protect\logs\tomcat\localhost.latest_date.log`

2 If the plug-in failed to load, search for a message in the log file similar to the following:

   ```text
   SEVERE
   ```

   Note the "Cause" section that follows this type of error message. Any such entries explain why the plug-in failed to load.

3 If the plug-in loads but attributes are not populated, look in the log for the attribute map. Verify that values are being populated, including for the lookup parameters that you enabled. To do this, search for a lookup parameter key that you have enabled, such as `data-owner-name`. 
Changing Data Insight refresh intervals

To change the schedule for the data refresh from the Veritas Data Insight Management Server, update the properties in the DataInsightDataRefresh.properties file on the Enforce Server.

The DataInsightDataRefresh.properties file is located in folder SymantecDLP\Protect\config in a default Windows installation.

By default, the start time for the data refresh is daily at 1:00 A.M. If the data refresh does not finish by 7:00 A.M. (default), then the data refresh process is interrupted and the reports are built. On the weekends, no cutoff is set by default, to allow the data refresh process to complete over a weekend. The defaults are set to have the reports available at the start of each work day.

If the start value is "none" then no data refresh starts on that day.

The following example contains data refresh start lines in the properties file:

data_refresh.start.sunday = none

data_refresh.start.monday = 1:00 AM

To specify no cutoff, set the value to "none" in the cutoff lines in the file.

The following example contains data refresh cutoff lines in the properties file:

data_refresh.cutoff.sunday = none

data_refresh.cutoff.monday = 7:00 AM

Best practices for finding and reporting on data at risk

The following best practices provide guidelines for implementation:

- Set up the Veritas Data Insight system and allow it to gather user information for a period of time.
  See the Veritas Data Insight Administrator's Guide.
  See “Where to get more information about Veritas Data Insight” on page 15.

- Make sure that the Enforce Server is connected to the Veritas Data Insight Management Server.
  See “Configuring the connection between the Enforce Server and Data Insight” on page 22.
- Configure your schedule to refresh the data from Veritas Data Insight to the Enforce Server.  
  See “Changing Data Insight refresh intervals” on page 34.

- Configure lookup plug-ins to look up and populate attributes in the Discover incidents. Lookup plug-ins can be scripted and chained.  
  See the Symantec Data Loss Prevention Administration Guide.
Finding data users and accesses in incident reports

This chapter includes the following topics:

- Accessing reports of folders at risk
- Configuring the risk score and timeframes for the report of folders at risk
- Viewing folders ranked by risk, path, or folder exposure
- Viewing details of a folder at risk
- Filtering the information in the report of folders at risk
- Saving a report of folders at risk
- Finding data users and accesses in incident reports
- Viewing Data Insight incident details
- Accessing the history of a file in the Veritas Data Insight console
- Selecting custom attributes for data user details
- Creating summary reports for Data Insight
- Creating and distributing aggregated incident reports to data owners

Accessing reports of folders at risk

The **Folder Risk Report** helps information security analysts identify the top folders for investigation. Each folder is assigned a risk score. The risk score is based on the relevant information from the Symantec Data Loss Prevention incidents plus the information from the Veritas Data Insight Management Server. In the default
display, the folders are ranked with prioritized risk. The risk calculation is relative to the other folders in the list after the current filters are applied. The highest risk folder always has a value of 100.

Some setup is required for all the information to appear in the report of folders at risk. Several options are also available to configure the flow of information and parameters.

See “Configuring the risk score and timeframes for the report of folders at risk” on page 39.

To display the folders at risk

1. Click Incidents > Discover.

2. In the Discover Reports on the left side, click Folder Risk Report.

3. If the Folder Risk Report does not appear on the left side, verify that the role for your user name allows access.

4. To display the Folder Risk Report, Adobe Flash Player 10.1 or later is required as a plug-in in the Web browser. You are prompted to install it when you first access the Folder Risk Report, if it is not already installed.

5. Table 3-1 shows the information in the report of folders at risk.

Table 3-1 Information in the report of folders at risk

<table>
<thead>
<tr>
<th>Information and Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>See “Filtering the information in the report of folders at risk” on page 42.</td>
</tr>
<tr>
<td>Folders with risk score</td>
<td>On the left is a list of folders with the highest risk at the top.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing folders ranked by risk, path, or folder exposure” on page 40.</td>
</tr>
</tbody>
</table>
Table 3-1  Information in the report of folders at risk  (continued)

<table>
<thead>
<tr>
<th>Information and Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Data Owners</td>
<td>For the selected folder on the left, the top data owners are listed. The data owners in this report are from the Data Owner Name field in the incident detail. Setup of a lookup plug-in, or a manual process of setting this field, is required to place values into this field. By default, this field does not have values. See “Configuring Data Loss Prevention to retrieve attribute values from Data Insight” on page 25.</td>
</tr>
<tr>
<td>Sensitive Files Access Trend</td>
<td>For the selected folder on the left, the trend for the past 12 months is listed. The number of days for this trend report can be configured. See “Configuring the risk score and timeframes for the report of folders at risk” on page 39.</td>
</tr>
<tr>
<td>User/Group Activity View</td>
<td>For the selected folder on the left, all groups who have access to the folder and their usage. See “Viewing details of a folder at risk” on page 41.</td>
</tr>
</tbody>
</table>

See “Viewing folders ranked by risk, path, or folder exposure” on page 40.

See “Filtering the information in the report of folders at risk” on page 42.

See “Viewing details of a folder at risk” on page 41.

See “Saving a report of folders at risk” on page 45.

See “Locating and managing data at risk” on page 17.
Configuring the risk score and timeframes for the report of folders at risk

You can configure the risk score for the report of folders at risk. The risk score is based on the relevant information from the Symantec Data Loss Prevention incidents plus the information from the Veritas Data Insight Management Server. You can also configure the timeframes that are in the details of the report.

To configure the risk score

1. Navigate to the System > Settings > Data Insight screen.
2. Click Configure.
3. Configure the risk score parameters as described in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access History Timeframe</td>
<td>365</td>
<td>The number of days in the timeframe for user access in the risk score formula.</td>
</tr>
<tr>
<td>Unique Users Timeframe</td>
<td>7</td>
<td>The number of days that is the timeframe for the user access in the formula.</td>
</tr>
<tr>
<td>Formula</td>
<td>Severity and folder exposure</td>
<td>Select one of the following choices for the components in the risk score formula:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Severity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The severity level of the incident in the Symantec Data Loss Prevention incident report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Severity and folder exposure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Folder exposure is the number of users who can read from the folder where the incidents were found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Severity, folder exposure and user access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User access is the number of users who have accessed the item at risk in the past. The timeframe for the past is the number of days in the Unique Users Timeframe parameter.</td>
</tr>
<tr>
<td>Weights (0-100):</td>
<td></td>
<td>The severity weight of the item at risk. The maximum value of any weight is 100.</td>
</tr>
<tr>
<td>High Severity</td>
<td>100.0</td>
<td>Weight of a high severity item at risk.</td>
</tr>
<tr>
<td>Medium Severity</td>
<td>10.0</td>
<td>Weight of a medium severity item at risk.</td>
</tr>
</tbody>
</table>
Table 3-2  Folder risk report configuration options (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Severity</td>
<td>2.0</td>
<td>Weight of a low severity item at risk.</td>
</tr>
<tr>
<td>Info Severity</td>
<td>1.0</td>
<td>Weight of an informational severity item at risk.</td>
</tr>
</tbody>
</table>

Viewing folders ranked by risk, path, or folder exposure

Click **Incidents > Discover**, and click the link to the **Folder Risk Report**.

In the list pane, you can view the folders at risk, and sort them by risk score, path, or folder exposure.

The risk score is based on the relevant information from the Symantec Data Loss Prevention incidents plus the information from the Veritas Data Insight Management Server.

You can filter the information in the display by status, policy, location, and data owner.

See “Filtering the information in the report of folders at risk” on page 42.

A folder is not visible in the list pane if all its incidents are filtered out of the report.

If you click **View Detail**, detailed information for that folder appears in the detail pane.

See “Viewing details of a folder at risk” on page 41.

You can use the arrow controls to jump to the first page, previous page, next page, or last page.

The following fields are visible in the list pane:

- The folder name and the full path of the folder.

- **Top Policies by File Count**
  The top five policies that are violated and the number of files that are violated for each policy is listed in a chart, subject to the filter criteria. The policies are listed in descending order by the number of sensitive files.
  Click **Incidents Summarized by Policy** to open a new browser window or tab with the Symantec Data Loss Prevention incident summary by policy. When you are finished viewing the information in the new browser window or tab, then close it.

- **Total Sensitive Files**
The total sensitive files include all sensitive files in this folder, including those in the top five policies that are violated.

- **Folder Exposure**
  The folder exposure is the number of users in the ACL that have read access to this folder.
  See the details in the User/Group Activity View in the detail pane on the right side.
  See “Viewing details of a folder at risk” on page 41.

To sort the folders at risk

1. To display the folders at risk, click **Incidents > Discover**. In the **Discover Reports** on the left side, click **Folder Risk Report**.
2. In the Folder Risk Report, click one of the following items for the sort:
   - **Risk**
     This sort option is the default. The folders are listed with the most risk at the top.
     The risk score is based on the relevant information from the Symantec Data Loss Prevention incidents plus the information from the Veritas Data Insight Management Server.
     You can configure the weights in the risk score formula.
     See “Configuring the risk score and timeframes for the report of folders at risk” on page 39.
   - **Path**
     The folders are listed in alphabetical order.
   - **Folder Exposure**
     The folder exposure is a count of the number of users who have read access to the folder.
     The folders are listed in descending order.

**Viewing details of a folder at risk**

The left detail pane provides details of the folders at risk.

The following related reports are links to details in a new browser window or tab:

- **DLP: Folder Incident Report**
  The Folder Incident Report links to a new browser window or tab with the list of the Symantec Data Loss Prevention incidents for the selected folder at risk.

- **Data Insight: Top 5 Users**

- **Data Insight: Monthly Access**
Data Insight: Permissions
All of the Veritas Data Insight report links open a new browser window or tab to the Veritas Data Insight management console.
You must log into the Veritas Data Insight management console before you can view these reports.
See “Where to get more information about Veritas Data Insight” on page 15.

To view the details of a specific folder
1. To display the folders at risk, click **Incidents > Discover**. In the **Discover Reports** on the left side, click **Folder Risk Report**.
2. For a folder in the list pane, click **View Detail** to show the details of that folder in the right pane.

   The name of the folder is displayed at the top of the right pane.

   The list pane (left) and details pane (right) have separate scrollbars, so that they can be positioned for the relevant folder to be visible in each pane.

The right pane shows the following details of a folder at risk:

<table>
<thead>
<tr>
<th>Table 3-3</th>
<th>Details of a folder at risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report detail</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Top 5 Data Owners</strong></td>
<td>Top five sensitive file data owners, ranked by the number of sensitive files owned (if data owners have been specified in the incidents).</td>
</tr>
<tr>
<td><strong>Sensitive Files Access Trend</strong></td>
<td>Trend on a monthly basis over the past 12 months. The time period can be configured, for a custom period. See “Configuring the risk score and timeframes for the report of folders at risk” on page 39. This table represents the number of unique users accessing sensitive files in the folder. The list is broken down by month.</td>
</tr>
<tr>
<td><strong>User/Group Activity View</strong></td>
<td>File activity of groups in the folder’s ACL.</td>
</tr>
</tbody>
</table>

Filtering the information in the report of folders at risk

To focus on specific folders at risk, you can filter the information in the report of folders at risk based on the status, policy, location, and data owner.
To filter the information in the report of folders at risk

1. To display the folders at risk, click **Incidents > Discover**. In the **Discover Reports** on the left side, click **Folder Risk Report**.

2. Click **Edit Filters** to open the list of filter options.

3. Select the filter options for your report. 
   
   Table 3-4 lists the filter options.

4. At the bottom of the **Filters** window, click **Apply Filters**.

5. After you have a custom report that is set up with selected filters, you can save it.

   See “Saving a report of folders at risk” on page 45.

The following filters can be set for the report of folders at risk:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Statuses</td>
<td>Based on the status filters, individual incidents are filtered out of the data and the risk score, but the folder is still visible. If all the incidents in a folder are filtered out, it is not visible.</td>
</tr>
</tbody>
</table>

   To filter by incident status:

   - Use the drop-down to select **Include** or **Exclude**. The remainder of the steps assumes that you have selected **Include** which is the default.
   - Select one of the status entries from the **All Statuses** list.
   - Click the plus sign to move it to the **Included Statuses** list.
   - Repeat for any other status entries to include.
   - If you want to remove a status entry out of the **Included Statuses**, click the minus sign.
   - You can search for a status entry by typing a string in the box underneath the **Include** label. Initially, this box says **"Search statuses."**
### Table 3-4 Filters for the folder risk report (continued)

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policies</strong></td>
<td>Based on the policy filters, individual incidents are filtered out of the data and the risk score, but the folder is still visible. If all the incidents in a folder are filtered out, it is not visible.</td>
</tr>
<tr>
<td></td>
<td>To filter by policies:</td>
</tr>
<tr>
<td></td>
<td>■ Use the drop-down to select <strong>Include</strong> or <strong>Exclude</strong>. The remainder of the steps assumes that you have selected <strong>Include</strong>, which is the default.</td>
</tr>
<tr>
<td></td>
<td>■ Select one of the policies from the <strong>All Policies</strong> list.</td>
</tr>
<tr>
<td></td>
<td>■ Click the plus sign to move it to the <strong>Included Policies</strong> list.</td>
</tr>
<tr>
<td></td>
<td>■ Repeat for any other policies to include.</td>
</tr>
<tr>
<td></td>
<td>■ If you want to remove a policy out of the <strong>Included Policies</strong>, click the minus sign.</td>
</tr>
<tr>
<td></td>
<td>■ You can search for a policy by typing a string in the box underneath the <strong>Include</strong> label. Initially, this box says &quot;<strong>Search policies</strong>.&quot;</td>
</tr>
<tr>
<td><strong>Locations</strong></td>
<td>The location filter selects the folders to include or exclude from the display. The risk score of a folder does not change.</td>
</tr>
<tr>
<td></td>
<td>An <strong>Include</strong> section specifies the locations to include.</td>
</tr>
<tr>
<td></td>
<td>An <strong>Exclude</strong> section specifies the locations to exclude.</td>
</tr>
<tr>
<td></td>
<td>The method of selecting the locations to include or exclude is the same for both sections.</td>
</tr>
<tr>
<td></td>
<td>To filter by locations:</td>
</tr>
<tr>
<td></td>
<td>■ Choose whether you want an <strong>Exact Match</strong>, <strong>Contains</strong>, or <strong>Starts with</strong> the string in the box.</td>
</tr>
<tr>
<td></td>
<td>■ Enter a string in the box, which can be a full path or a partial path.</td>
</tr>
<tr>
<td></td>
<td>■ Click the plus sign to move the selection to the list of locations to be included or excluded.</td>
</tr>
<tr>
<td></td>
<td>■ If you want to remove a location entry out of the list, click the minus sign.</td>
</tr>
</tbody>
</table>
Table 3-4  Filters for the folder risk report (continued)

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Owners</strong></td>
<td>The data owner filter selects the folders to include or exclude from the display. The risk score of a folder does not change.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the folder contains other data owners, it remains in the report. An excluded data owner may appear in the top data owners list.</td>
</tr>
<tr>
<td></td>
<td>An <strong>Include</strong> section specifies the data owners to include.</td>
</tr>
<tr>
<td></td>
<td>An <strong>Exclude</strong> section specifies the data owners to exclude.</td>
</tr>
<tr>
<td></td>
<td>The method of selecting the data owners to include or exclude is the same for both sections.</td>
</tr>
<tr>
<td></td>
<td>To filter by data owners:</td>
</tr>
<tr>
<td></td>
<td>■ Choose whether you want an <strong>Exact Match</strong>, <strong>Contains</strong>, or <strong>Starts with</strong> the string in the box.</td>
</tr>
<tr>
<td></td>
<td>■ Enter a string in the box.</td>
</tr>
<tr>
<td></td>
<td>■ Click the plus sign to move the selection to the list of data owners to be included or excluded.</td>
</tr>
<tr>
<td></td>
<td>■ If you want to remove a data owner entry out of the list, click the minus sign.</td>
</tr>
</tbody>
</table>

**Saving a report of folders at risk**

After you filter a report, you can save it for continued use. When you save a customized report, Symantec Data Loss Prevention displays the report title in **Incidents > Discover** under **Saved Reports** on the left side. If you choose to share the report, Symantec Data Loss Prevention displays it for any user that is logged on under your role.

**To save a custom report of folders at risk**

1. Set up a customized report with a set of custom filters and optional sort order. See “Filtering the information in the report of folders at risk” on page 42. See “Viewing folders ranked by risk, path, or folder exposure” on page 40.

2. In the display of the report of folders at risk, click **Save > Save As**.

3. Enter a unique report name and describe the report. The report name can include up to 50 characters.
In the **Sharing** section, users other than the administrator can share a custom report.

**Note:** This section does not appear for the administrator.

The **Sharing** section lets you specify whether to keep the report private or share it with other role members. Role members are other users who are assigned to the same role. To share the report, select **Share Report**. All role members now have access to this report, and all can edit or delete the report. If your account is deleted from the system, shared reports remain in the system. After a report is shared, sharing cannot be disabled for that report. Shared reports are associated with the role, not with any specific user account. If you do not share a report, you are the only user who can access it. If your account is deleted from the system, your private reports are deleted as well.

Click **Save**.

To edit a saved report, click **Save > Save** after you have edited the filters or changed the sort order.

To delete a saved report, click **Delete**.

---

**Finding data users and accesses in incident reports**

The Data Insight Lookup Plug-in populates the custom attributes that were defined and mapped during the configuration.

See “**About the Data Insight lookup plug-in**” on page 23.

See “**Mapping attributes to Data Insight data fields**” on page 26.

The names of these custom attributes may be different in your configuration. General names for the custom attributes are in the examples and explanation of possible reports in this section.

**Table 3-5** shows use cases with suggestions for reports.
## Table 3-5

### Use cases for reports

<table>
<thead>
<tr>
<th>Use case</th>
<th>Description</th>
<th>Reports</th>
</tr>
</thead>
</table>
| Data owner                | File owner information may not reflect the responsible party. The responsible party or data owner can be a line manager in the business unit, the head of a department, or an information security officer. Veritas Data Insight provides information to tie the most active user of a file to a manager or responsible party for remediation steps. | Use the summary reports and filters to determine the incidents of interest.  
See “Creating summary reports for Data Insight” on page 51.  
The LDAP Lookup Plug-in, CSV Lookup Plug-in, or a Script Lookup Plug-in can locate the manager or department of the file owner.  
See “Enabling the Data Insight lookup plug-in” on page 29.  
Use the incident snapshot report to determine the responsible party. Use the Attributes section to view the information from the lookup plug-ins. Use the attributes Lookup option to retrieve the information, if it is not present.  
See “Viewing Data Insight incident details” on page 48. |
| Next-best owner identification | The **File Owner** field may return an unresolvable account for an individual that has left the organization. For example, in Windows Active Directory, every user has an underlying unique identifier that is associated with their account. This identifier is sometimes an unidentifiable string of information. Veritas Data Insight provides information to drop down to the next resolvable account that names an individual.  
Veritas Data Insight provides several data user fields.  
See “About the Data Insight lookup plug-in” on page 23. | Use the summary reports and filters to determine the incidents of interest.  
See “Creating summary reports for Data Insight” on page 51.  
Use the incident snapshot report to determine the **File Owner**. If that owner is not identifiable, use the Attributes section to determine the next-best owner. The Attributes section contains the information from the Veritas Data Insight Management Server.  
See “Viewing Data Insight incident details” on page 48.  
See “Selecting custom attributes for data user details” on page 50. |
Use cases for reports (continued)

<table>
<thead>
<tr>
<th>Use case</th>
<th>Description</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data leak investigation</td>
<td>In the event of a data leak, customers want to know who saw a particular file. Symantec Data Loss Prevention incident snapshots provide information to tie the incident back to the Veritas Data Insight Management Server. On the Veritas Data Insight Management Server, you can view detailed information and an audit history of who accessed the data. Additional remediation steps can then be taken to report on those individuals or launch subsequent targeted scans on their assets.</td>
<td>Use the summary reports and filters to determine the incidents of interest. See “Creating summary reports for Data Insight” on page 51. Use the incident snapshot report to view details of an incident. See “Viewing Data Insight incident details” on page 48. Click the go to Data Insight option in the Incident Details section to view additional details. See “Accessing the history of a file in the Veritas Data Insight console” on page 49. In the incident snapshot, click the Correlations tab to view a list of the incidents that share attributes with the current incident.</td>
</tr>
</tbody>
</table>

**Viewing Data Insight incident details**

Symantec Data Loss Prevention incident lists display the individual incident records with information about the incidents. You can click on any incident to see a snapshot containing more details. You can select specific incidents or groups of incidents to modify or remediate.
To view incidents

1. In the Enforce Server administration console, on the **Incidents** menu, select one of the types of reports. For example, select **Discover**. In the left navigation panel, click **Incidents-All Scans**.

   The incident list displays the individual incident records that contain information such as severity, associated policy, number of matches, and status.

2. Optionally, use report filters to narrow down the incident list. Select the custom attributes from the Veritas Data Insight Management Server to filter or summarize the incident list.

   All custom attributes are all alphabetic fields. Sorting is alphabetic for the summary information for any custom attribute. For example, in a summary of the read values, the value "15" comes after "1" and before "2." Numeric filters, such as greater-than or less-than are not available for the custom attribute values that seem to be numbers or dates.

   See the *Symantec Data Loss Prevention Administration Guide*.

3. To view more details of a particular incident, click the incident.

   The incident snapshot appears, displaying general incident information, matches detected in the intercepted text, and details about policy, attributes, and incident history. You can also search for similar incidents from the **Correlations** tab.

4. Optionally, click through the incident snapshot to view more information about the incident.

   The data user information from Veritas Data Insight is in the **Attributes** section.

5. When you finish viewing incidents, you can exit the incident snapshot or incident list, or you can choose one or more incidents to remediate.

6. To view additional details about file access, you can jump directly to the Veritas Data Insight console.

   See “**Accessing the history of a file in the Veritas Data Insight console**” on page 49.

**Accessing the history of a file in the Veritas Data Insight console**

To view additional details about file access, you can jump directly to the Veritas Data Insight console from a Symantec Data Loss Prevention incident snapshot.
To view additional details about accesses for a particular file

1. Navigate to the incident snapshot for the file of interest.
2. In the Key Info tab, in the Incident Details section, File Location, click **go to Data Insight console**.

   A browser screen opens with file access details for that particular file. The data user information includes an access summary of the primary users of this file. The audit logs provide details about each access of the file, and a chart of the access pattern.

For information about navigating in the Veritas Data Insight console, see the *Veritas Data Insight Administrator’s Guide*.

## Selecting custom attributes for data user details

You must define and configure a set of custom attributes before you can get information about data users.

See "About the Data Insight lookup plug-in" on page 23.

See “Mapping attributes to Data Insight data fields” on page 26.

Initially, you can define the data user, the read count, write count, and one or two active readers and writers.

For a particular file of interest, the incident snapshot and Veritas Data Insight details provide the information to determine who uses a file.

For example, to determine the data users of a cluster of files, perform the suggested steps in the following procedure. If all the files in a folder do not have appropriate access permissions, you can determine who has accessed those files.

### To determine the data users of a cluster of files

1. Define a set of custom attributes for the Data Insight Lookup Plug-in.
   
   See "About the Data Insight lookup plug-in" on page 23.
   
   See “Mapping attributes to Data Insight data fields” on page 26.

2. Set up and run a Network Discover scan of the folder of interest in the file share.

   See the *Symantec Data Loss Prevention Administration Guide*.

3. After the scan has run, display the incident list. The **File Owner** is one of the columns. However, this field does not provide the access pattern for these files.
You can select Advanced Filters & Summarization. Then run a summary by the Veritas Data Insight data user. This summary lists the users who most frequently accessed the files in the folder of interest.

After an analysis of incidents, you can determine if additional custom attributes are needed from the information that Veritas Data Insight provides. Then new custom attributes can be defined, configured, and looked up. See “About the Data Insight lookup plug-in” on page 23.

After you define any new custom attributes, click the Lookup option on the incident snapshot. Then make sure that no connection errors are recorded in the Incident History section.

The values that appear in the incident snapshot Attributes section are the new ones.

Any deleted custom attributes and values are no longer present.

If the mapping of any custom attribute is changed and a new lookup is run, the new mapping overrides any old values in the reports.

Creating summary reports for Data Insight

You can create a summary report for a summary of the data user activity for the files identified in an incident report.

To create a summary report from an incident list

1 In the Enforce Server administration console, on the Incidents menu, select one of the types of reports, and then click an incident list. For example, select Discover, and then the report Incidents-All Scans.

2 Click the Advanced Filters & Summarization bar (near the top of the report).

In Summarize By section, a primary listbox and secondary listbox appear. Symantec Data Loss Prevention displays all Symantec-provided criteria in alphabetical order. These criteria precede any custom criteria the administrator has defined.

3 Select a criterion from the primary listbox, and an optional criterion from the secondary listbox. For example, select the custom attribute for the Veritas Data Insight parameter for Data User and then Total Reads. This report shows the read activity by user.

Options in the secondary listbox appear only after you choose an option from the primary listbox.
4. To create the summary report, click **Apply**.

   Summary reports take their name from the primary summary criterion. If you rerun a report with new criteria, the report name changes accordingly.

5. Save the report.

### Creating and distributing aggregated incident reports to data owners

You can create and automatically distribute aggregated incident reports to data owners for remediation.

An automatic workflow can be set up for the following use cases:

- Automatically or manually set the **Data Owner Name** and **Data Owner Email Address** for new incidents.
- Set a custom status value or custom attribute to mark that the **Data Owner Name** for an incident has been verified. Custom attributes and custom status values can also mark incidents for other workflow steps.
- Set up a recurring email schedule. Reports can be configured to be sent on a recurring schedule, sending only the incidents that have not yet been distributed.
- Mark the incident as sent. After the report is sent, the status attributes and custom attributes can optionally be set, to flag the incidents for the next stage of the workflow.
- Automate the tasks. Lookup plug-in scripts and chained lookup plug-ins can automate the tasks in the workflow sequence.

The following process describes a complex use case that includes the setup tasks, and suggestions to automate some steps in the process.

<table>
<thead>
<tr>
<th>Table 3-6</th>
<th>Setting up, creating, and distributing aggregated incident reports to data owners</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step</strong></td>
<td><strong>Action</strong></td>
</tr>
</tbody>
</table>
| 1         | Install and set up the Veritas Data Insight Management Server.  
Make sure that the Veritas Data Insight Management Server has access to the files or file systems of interest. | See the following Veritas Data Insight documentation:  
- *Veritas Data Insight Installation Guide*  
- *Veritas Data Insight Administrator's Guide* |
### Table 3-6 Setting up, creating, and distributing aggregated incident reports to data owners (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Install the Symantec Data Loss Prevention product, including at least one Network Discover Server.</td>
<td>See the Symantec Data Loss Prevention Installation Guide.</td>
</tr>
<tr>
<td>3</td>
<td>Set up the connection between the Enforce Server and the Veritas Data Insight Management Server.</td>
<td>See “Configuring the connection between the Enforce Server and Data Insight” on page 22. <strong>Note:</strong> Veritas Data Insight is a separately licensed option. If Veritas Data Insight is not licensed on the Enforce Server, the menu option to configure the connection to the Veritas Data Insight Management Server does not appear.</td>
</tr>
<tr>
<td>4</td>
<td>Test the connection from the Enforce Server to the Veritas Data Insight Management Server.</td>
<td>See “Troubleshooting the Data Insight lookup plug-in” on page 32.</td>
</tr>
<tr>
<td>5</td>
<td>On the Enforce Server, create a custom status value or custom attribute for the Data Owner Name verification, and any workflow status attributes.</td>
<td>See “About the Data Insight lookup plug-in” on page 23.</td>
</tr>
<tr>
<td>6</td>
<td>Map the details from the Veritas Data Insight Management Server into the custom attributes that you created.</td>
<td>Edit the properties file for Veritas Data Insight on the Enforce Server, to map the details from the Veritas Data Insight Management Server into the custom attributes that you created. See “Mapping attributes to Data Insight data fields” on page 26.</td>
</tr>
<tr>
<td>7</td>
<td>Map any of the Veritas Data Insight attributes directly into the <strong>Data Owner Name</strong> field.</td>
<td>To map the Veritas Data Insight data user (the person who uses the file most frequently) to the <strong>Data Owner Name</strong>, set the <code>Data_User</code> parameter. See “Configuring Data Loss Prevention to retrieve attribute values from Data Insight” on page 25.</td>
</tr>
</tbody>
</table>
Table 3-6  Setting up, creating, and distributing aggregated incident reports to data owners (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Set up all your lookup plug-ins.</td>
<td>For example, you may want to chain the LDAP Lookup Plug-in to take the <strong>Data Owner Name</strong> and set the <strong>Data Owner Email Address</strong> as either the data owner or the manager of the data owner. No built-in capability provides consistency between the data owner and email address. This action must be customized. The <strong>Data Owner Email Address</strong> can have multiple email addresses that are separated with commas. <strong>Note:</strong> If duplicate attribute names exist between these names and custom attributes, then both fields are updated. See “Configuring Data Loss Prevention to retrieve attribute values from Data Insight” on page 25.</td>
</tr>
<tr>
<td>9</td>
<td>Verify that the Enforce Server general settings are set up to send email notifications.</td>
<td>Set up the SMTP notification settings. Set the option <strong>Send report data with emails</strong>.</td>
</tr>
<tr>
<td>10</td>
<td>Verify that the incident responder has the privileges to run the reports.</td>
<td>The <strong>Remediate Incidents</strong> privilege is required to configure and run the reports. The <strong>Lookup Attributes</strong> privilege is required to set attributes from the lookup plug-ins. The User Privilege <strong>CSV Attachment in Email Reports</strong> is required to attach the CSV report to the email.</td>
</tr>
<tr>
<td>11</td>
<td>Set up a Network Discover and run a sample scan of the file systems of interest.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-6 Setting up, creating, and distributing aggregated incident reports to data owners (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12   | Set up any custom reports. | Set up a filtered report, or set up any report that you want to distribute. For example, you can filter based on the new incidents.  
Select the option **Change Incident Status / Attributes** of the reports scheduling to set incident status or attributes when the email is sent.  
You can also manually set the custom attribute that indicates these incidents were verified. Select any or all incidents in the list. Use the drop-down **Incident Actions** and select **Set Attributes**. You can also set a custom status from this drop-down menu. |
| 13   | Save the custom reports and set up a distribution schedule. | |

*Finding data users and accesses in incident reports*

*Creating and distributing aggregated incident reports to data owners*
Working with the Veritas Data Insight Self-Service Portal

This chapter includes the following topics:

- About the Veritas Data Insight Self-Service Portal
- Configuring Symantec Data Loss Prevention for use with the Veritas Data Insight Self-Service Portal
- Operational logs for the Response Rule Execution Service

About the Veritas Data Insight Self-Service Portal

The Self-Service Portal allows your central information security team to distribute the Data Loss Prevention remediation workflow directly to data owners and data custodians. Using the portal, data owners and custodians can take Network Discover Box cloud storage, file-system, and SharePoint incident remediation actions at the file or the folder level without needing access to the Enforce Server administration console. These remediation actions are Smart Response rules that are executed by Symantec Data Loss Prevention on behalf of the Self-Service Portal user. For detailed information about the configuration and use of the Self-Service Portal, see the Veritas Data Insight Administration Guide and the Veritas Data Insight User Guide. For detailed information about Smart Response rules, see the Symantec Data Loss Prevention Administration Guide. The Self-Service Portal is available beginning with Veritas Data Insight version 4.5.

Symantec Data Loss Prevention provides two web services to Veritas Data Insight for incident remediation: the Response Rule Listing Service and the Response Rule
Execution Service. The Response Rule Listing Service provides a list of the available response rules for a given incident, such as delete or quarantine. The Response Rule Execution Service takes response rule requests from Veritas Data Insight and executes them in Symantec Data Loss Prevention. By default, the Response Rule Execution Service is disabled. You must enable the service to allow Self-Service Portal users to remediate incidents.

See “Configuring the Response Rule Execution Service” on page 58.

You can view the operational logs for the Response Rule Execution Service in the responseruleservice_operational_0.log file within the SymantecDLP/Protect/logs directory. The operational logs may be helpful for troubleshooting issues with the Veritas Data Insight Self-Service Portal.

See “Operational logs for the Response Rule Execution Service” on page 60.

Configuring Symantec Data Loss Prevention for use with the Veritas Data Insight Self-Service Portal

Configuring Symantec Data Loss Prevention for use with the Veritas Data Insight Self-Service Portal involves the following steps.

Table 4-1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>If you have not already done so, configure Smart Response rules for your Network Discover Box cloud storage, file-system, and SharePoint incidents.</td>
<td>For detailed information about Smart Response rules, see the Symantec Data Loss Prevention Administration Guide.</td>
</tr>
<tr>
<td>2</td>
<td>Create an Symantec Data Loss Prevention Enforce Server user with the appropriate role-based access control permissions for incident remediation.</td>
<td>Ensure that the user for the Self-Service Portal has Response Rule Execution and Incident Update privileges for Discover incidents, as well as Incident Modification privileges for the incidents being remediated. For detailed information about setting up users, including configuring role-based access control, see the “Managing roles and users” chapter in the Symantec Data Loss Prevention Administration Guide.</td>
</tr>
</tbody>
</table>
Table 4-1  (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Configure the Response Rule Execution Service.</td>
<td>By default, the Response Rule Execution Service is disabled. To enable and configure the Response Rule Execution Service, modify the appropriate parameters in the SymantecDLP/Protect/config/manager.properties file. After you have modified the parameters in the manager.properties file, restart the Vontu Manager service. The only parameter you are required to configure is com.vontu.enforcewebservices.responserules.execution.service.schedule. This parameter is set to NEVER by default, which means that Symantec Data Loss Prevention never processes response rule requests from Veritas Data Insight. To schedule the Response Rule Execution Service, specify a start and end time in Quartz Cron format. The Quartz Cron format differs from the standard Cron format slightly. For details about the Quartz Cron format, see the Quartz Cron tutorial page.</td>
</tr>
</tbody>
</table>

Configuring the Response Rule Execution Service

By default, the Response Rule Execution Service is disabled. To enable and configure the Response Rule Execution Service, modify the appropriate parameters in the SymantecDLP/Protect/config/manager.properties file. After you have modified the parameters in the manager.properties file, restart the Vontu Manager service.

The only parameter you are required to configure is com.vontu.enforcewebservices.responserules.execution.service.schedule. This parameter is set to NEVER by default, which means that Symantec Data Loss Prevention never processes response rule requests from Veritas Data Insight.

To schedule the Response Rule Execution Service, specify a start and end time in Quartz Cron format. The Quartz Cron format differs from the standard Cron format slightly. For details about the Quartz Cron format, see the Quartz Cron tutorial page.
Table 4-2  Configuration parameters for the Response Rule Execution Service

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Minimum value</th>
<th>Description</th>
</tr>
</thead>
</table>
| com.vontu.enforcewebservices.responserules.execution.service.schedule | NEVER              | N/A           | Specifies the schedule on which Symantec Data Loss Prevention executes response rule requests from the Veritas Data Insight Self-Service Portal. Possible values are:  
|                                                        |                     |               | ■ NEVER: Symantec Data Loss Prevention does not execute response rule requests from the Veritas Data Insight Self-Service Portal.  
|                                                        |                     |               | ■ ALWAYS: Symantec Data Loss Prevention executes response rule requests from the Veritas Data Insight Self-Service Portal immediately upon receipt of the request.  
|                                                        |                     |               | ■ BY_SCHEDULE: Symantec Data Loss Prevention executes response rules from the Veritas Data Insight Self-Service Portal according to the schedule specified in the startHour and endHour parameters. |
| com.vontu.enforcewebservices.responserules.execution.service.startHour | 0 0 2 ? * *       | N/A           | Specifies the start time of the response rule execution process in Quartz Cron format.                                                   |
| com.vontu.enforcewebservices.responserules.execution.service.endHour   | 0 0 7 ? * *       | N/A           | Specifies the end time of the response rule execution process in Quartz Cron format.                                                    |
| com.vontu.enforcewebservices.responserules.execution.request.  
maxIncidentsInWaitingQueue                                      | 5,000,000          | 1             | The maximum number of incidents held in the waiting queue.                                                                                  |
| com.vontu.enforcewebservices.responserules.execution.request.  
maxIncidentsPerRequest                                           | 10,000             | 1             | The maximum number of incidents per response rule execution request.                                                                     |
| com.vontu.enforcewebservices.responserules.execution.request.  
maxRequestQueueSize                                               | 10,000             | 1             | The maximum number of response rule execution requests held in the request queue.                                                           |
Operational logs for the Response Rule Execution Service

The operational logs for the Response Rule Execution Service are useful for troubleshooting any issues you might experience. All messages are logged at the INFO level, with the exception of `RESPONSE_RULE_SERVICES_LOG_23`, which is logged at the FINE level.

You can set the Response Rule Execution Service operational log levels in the `SymantecDLP/Protect/config/ManagerLogging.properties` file:

```
com.vontu.enforcewebservices.
domain.responserules.logging.
ResponseRulesServicesLogHandler.level = INFO
```

<table>
<thead>
<tr>
<th>Log code</th>
<th>Log message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_1</td>
<td>The Response Rule Request Processing Service has started.</td>
<td>This message is logged when the service starts at its scheduled time.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_2</td>
<td>The Response Rule Request Processing Service has stopped.</td>
<td>This message is logged when the service stops at its scheduled time.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_3</td>
<td>Database connection is lost while the service is executing the requests. The Response Rule Request Processing Service will stop processing the requests until the database connection is restored.</td>
<td>This message is logged if the database connection is lost while the service is executing response rules.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_4</td>
<td>Database connection is lost. The Response Rule Request Processing Service will not process the requests as per the schedule until the database connection is restored.</td>
<td>This message is logged if the database connection is lost before the scheduled response rule execution start time.</td>
</tr>
<tr>
<td>Log code</td>
<td>Log message</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_5</td>
<td>Database connection is restored. The Response Rule Execution Request Processing Service will start processing the requests now.</td>
<td>This message is logged if the database connection is restored before the end of the scheduled response rule execution period.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_6</td>
<td>Database connection is restored. The Response Rule Execution Request Processing Service will start processing the requests as per the schedule.</td>
<td>This message is logged if the database connection is restored before the response rule execution service is started.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_7</td>
<td>The Response Rule Execution Request Processing Service has shutdown.</td>
<td>This message is logged during the shutdown of the service, usually as part of the Vontu Manager shutdown.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_8</td>
<td>Error encountered while shutting down the Response Rule Execution Request Processing Service. Reason: Error Message</td>
<td>This message is logged during the shutdown of the service if an error occurs during shutdown.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_9</td>
<td>Database connection is lost. The Response Rule Execution Request Processing Service will not process the requests until the database connection is restored.</td>
<td>This message is logged during the scheduled start of the service if the database connection is not available.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_12</td>
<td>The new schedule mode provided is invalid. Execution schedule will not be updated. Will remain with current schedule type as &quot;NEVER&quot;.</td>
<td>This message is logged by the service if the user an invalid value for the property com.vontu.enforcewebservice.responserules.execution.service.schedule.</td>
</tr>
<tr>
<td>Log code</td>
<td>Log message</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_13</td>
<td>The schedule mode provided is invalid. Execution schedule will be set to default type &quot;NEVER&quot;.</td>
<td>This message is logged by the service during startup. The user entered an invalid value for the property <code>com.vontu.enforcewebservices.responserules.execution.service.schedule</code>.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_14</td>
<td>The Response Rules Execution Request Resource received a GET request from the user &quot;USER&quot; and IP address &quot;IP Address&quot; and UUID &quot;UUID&quot; with no RBAC permission for response rule IDs [1,2].</td>
<td>The user does not have RBAC permissions for the response rules provided in the request. Change the user credentials to a user that has appropriate permissions for the incidents. Returns a 403: Forbidden HTTP status.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_15</td>
<td>The Response Rules Execution Request Resource received a BAD request from the user &quot;USER&quot; and IP address &quot;IP Address&quot; and UUID &quot;UUID&quot;. Reason &quot;Reason&quot;</td>
<td>The user made the POST request with an invalid set of parameters, causing a 400: Bad Request HTTP return status. The Reason section explains the cause of the problem. Possible reasons are missing response rule IDs, non-existent response rule IDs, missing incidents IDs, or invalid or duplicate UUIDs.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_16</td>
<td>The Response Rules Execution Request Resource received a POST request from the user &quot;USER&quot; and IP address &quot;IP Address&quot; and UUID &quot;UUID&quot; with no RBAC permission for response rule IDs [1,2].</td>
<td>The user does not have RBAC permissions for the incidents provided in the response rule ID. Change the user credentials to a user that has appropriate permissions for the incidents.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_19</td>
<td>Error encountered in creating the Response Rules Execution Request for the POST request from the user &quot;USER&quot; and IP address &quot;IP Address&quot; and UUID &quot;UUID&quot;. Reason &quot;Reason&quot;.</td>
<td>This message indicates that the service encountered an error in creating the request. The Reason section explains the cause of the error.</td>
</tr>
<tr>
<td>Log code</td>
<td>Log message</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_21</td>
<td>The schedule mode is changed from NEVER to ALWAYS.</td>
<td>This message is logged by the service after the service mode changed when the service was running.</td>
</tr>
<tr>
<td>RESPONSE_RULE_SERVICES_LOG_23</td>
<td>The Response Rule with ID &quot;ID&quot; is executed on the incident with ID &quot;ID&quot; for the Response Rule Execution Request with the ID &quot;ID&quot; as requested by the user &quot;USER&quot;.</td>
<td>This message is logged when the service has run the response rule on the incident with ID provided in the message. This message is logged in verbose/fine mode only.</td>
</tr>
</tbody>
</table>