Symantec™ Data Loss Prevention Data Insight Implementation Guide

Version 11.0

Symantec Data Loss Prevention Data Insight Implementation Guide

Documentation version: 11.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

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 automatic software upgrades protection
- 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 Web site at the following URL:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

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 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_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing Data Insight for Data Loss Prevention

This chapter includes the following topics:

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 Symantec 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.

Symantec Data Insight scans Network Attached Storage (NAS) filers and reports on the access history of various users across files and folders. Symantec Data Insight helps security administrators and the information security teams in your

organization to monitor and report on access to sensitive information. It also supports large-scale business owner-driven remediation processes and workflows.

Symantec Data Insight helps organizations solve the problem of identifying data owners and responsible parties for information due to incomplete or inaccurate metadata or tracking information.

See "What you can do with Symantec Data Insight and Symantec Data Loss Prevention" on page 12.

Symantec Data Insight can provide the following information:

- Who owns the data
- Who has accessed the data
- How the data is protected
- Who has seen the data
- Frequency of access to files

The Symantec 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 "About reports of folders at risk" on page 39.

Symantec Data Loss Prevention queries Symantec 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 Symantec 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 56.

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

Symantec 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.

The following components are integrated to provide data user information for incident remediation:

Symantec Data Insight	Symantec Data Insight scans Network Attached Storage (NAS) filers and Windows file servers. It reports on the access history of various users across files and folders.
Network Discover	Network Discover scans file shares on the same Network Attached Storage (NAS) filers and Windows file servers. It identifies confidential information as Network Discover incidents.
Symantec Data Loss Prevention	Symantec Data Loss Prevention queries Symantec Data Insight for the data user of a file and other access history attributes like the last modifying user.

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 11.

How Data Insight works with Data Loss Prevention

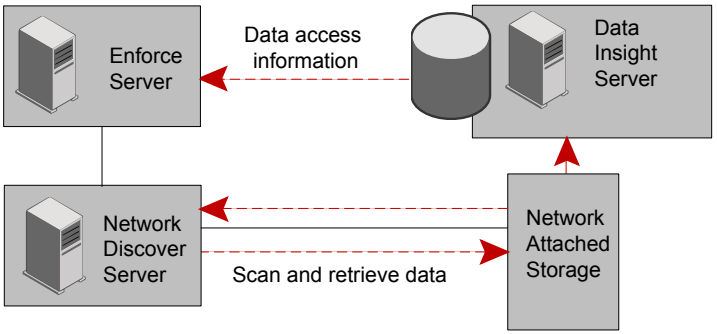
Figure 1-1 shows the flow of information between the Symantec Data Insight Management Server and the Symantec Data Loss Prevention servers.

Symantec Data Insight scans file systems and shares and stores information about the access history across the files and folders in Network Attached Storage.

A Network Discover Server scans the files and folders in Network Attached Storage 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 Symantec Data Insight, a lookup plug-in on the Enforce Server pulls data user information from the Symantec Data Insight Management Server.

This data user information populates custom attributes for a Network Discover incident at the time the incident is generated.

Figure 1-1 Flow of information between Data Insight and the Symantec Data Loss Prevention servers



A process table specifies the installation and configuration of the components in this diagram.

See "Locating and managing data at risk" on page 18.

What you can do with Symantec Data Insight and Symantec Data Loss Prevention

Table 1-1 describes the use cases of Symantec Data Insight to enable more efficient incident remediation:

Table 1-1 What you can do with Symantec Data Insight

Tasks	Description
Prioritize remediation of folders.	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.

Table 1-1 What you can do with Symantec Data Insight *(continued)*

Tasks	Description
Create and automatically distribute aggregated incident reports to data owners for remediation.	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.
Identify the 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. Symantec Data Insight provides information to tie the most active user of a file to a manager or responsible party for remediation steps.
Identify the next-best owner.	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. Symantec Data Insight provides information to drop down to the next resolvable account that names an individual.
Investigate a data leak.	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 Symantec Data Insight Management Server. On the Symantec 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.

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 47.

Where to get more information about Symantec Data Insight

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

- Symantec Data Insight supports specific filers.
  For a list of the supported filers, see the *Symantec 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."

The following documentation provides more information about Symantec Data Insight:

- *Symantec Data Insight Installation Guide*
  Explains how to install Symantec Data Insight.
- *Symantec Data Insight Administrator's Guide*
  Explains how to configure and administer Symantec Data Insight using the management console. Explains how to gather the access history of the data users.
- *Symantec Data Insight User's Guide*
  Explains the Symantec Data Insight views that display data access information on folders and by users or groups. Explains how to set up Symantec Data Insight reports.

The following documentation provides information about the setup to identify data users in the Symantec Data Loss Prevention product using the information from Symantec Data Insight:

- *Symantec Data Loss Prevention System Requirements Guide*
  Provides the requirements for the disk space for the Symantec 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 file system target, and how to set up reports.
- *Symantec Data Loss Prevention Data Insight Implementation Guide*

Explains the Symantec Data Loss Prevention implementation, configuration, and uses of the information that is gathered from Symantec Data Insight.

- *Symantec Data Loss Prevention Lookup Plug-in Guide*
  Explains the configuration of lookup plug-ins.
- Symantec Data Loss Prevention online Help
  Explains how to configure the connection between the Symantec Data Loss Prevention Enforce Server and the Symantec Data Insight Management Server.

Chapter 2

Enabling Symantec Data Insight to manage risk

This chapter includes the following topics:

Locating and managing data at risk

To locate and manage data at risk, you can 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 56.
- Retrieve the data user from the Symantec 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.
  See "Finding data users and accesses in incident reports" on page 47.
- Retrieve details about file use from the Symantec 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.
  See "Finding data users and accesses in incident reports" on page 47.

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

Table 2-1 Setting up the Symantec Data Loss Prevention system to connect to the Symantec Data Insight Management Server

Step	Action	Description
Step 1	Install and set up the Symantec Data Insight Management Server. Make sure that the Symantec Data Insight Management Server has access to the files or file systems of interest.	See the following Symantec Data Insight documentation: ■ *Symantec Data Insight Installation Guide* ■ *Symantec Data Insight Administrator's Guide*
Step 2	Install the Symantec Data Loss Prevention product, including at least one Network Discover Server.	See the *Symantec Data Loss Prevention Installation Guide.*

Table 2-1 Setting up the Symantec Data Loss Prevention system to connect to the Symantec Data Insight Management Server *(continued)*

Step	Action	Description
Step 3	Set up the connection between the Enforce Server and the Symantec Data Insight Management Server.	See "Configuring Symantec Data Loss Prevention for Symantec Data Insight" on page 21. **Note:** Symantec Data Insight is a separately licensed option. If Symantec Data Insight is not licensed on the Enforce Server, the menu option to configure the connection to the Symantec Data Insight Management Server does not appear. If you add the Symantec Data Insight license onto an existing Enforce Server, you must restart the Incident Persister service to enable the Symantec Data Insight lookups and the data owner lookups for incidents.
Step 4	Test the connection from the Enforce Server to the Symantec Data Insight Management Server.	See "Testing the Symantec Data Insight lookup plug-in" on page 35.

To retrieve details about file use into the **Data Owner Name** field, first complete the setup in Table 2-1, and then complete the following steps:

Table 2-2 Setting up the Symantec Data Loss Prevention system to retrieve details about file use from the Symantec Data Insight Management Server into the data owner field

Step	Action	Description
Step 1	Retrieve the Symantec Data Insight data user directly into the **Data Owner Name** field in the Discover incidents.	To map the Symantec Data Insight data user (the person who uses the file most frequently), to the **Data Owner Name**, set the `Data_User` parameter. See "Configuring the Symantec Data Insight lookup plug-in to populate the Data Owner fields" on page 33. **Note:** You can map any other fields into the **Data Owner Name** field, or set it manually from the Discover incident reports.
Step 2	Set up all your lookup plug-ins. You can also chain the LDAP Lookup Plug-In or the CSV Lookup Plug-In to set the **Data Owner Email Address** field.	Edit the `Plugins.properties` file to set up all your lookup plug-ins. See "Editing the plug-ins properties file to enable the Symantec Data Insight lookup plug-in" on page 27. See the *Symantec Data Loss Prevention Lookup Plug-in Guide*.
Step 3	Set up a Network Discover scan of the file systems of interest.	See the *Symantec Data Loss Prevention Administration Guide*.
Step 4	Test that the details from the Symantec 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 47.

To retrieve details from Symantec Data Insight about file use into custom attributes, complete the setup in Table 2-1, and then complete the following steps:

Table 2-3 Setting up the Symantec Data Loss Prevention system to retrieve details about file use from the Symantec Data Insight Management Server into custom attributes

Step	Action	Description
Step 1	On the Enforce Server, create custom attributes for each file detail that you want retrieved from the Symantec Data Insight Management Server.	See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.
Step 2	Map the details from the Symantec Data Insight Management Server into the custom attributes that you created.	Edit the properties file for Symantec Data Insight on the Enforce Server, to map the details from the Symantec Data Insight Management Server into the custom attributes that you created. See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.
Step 3	Set up all your lookup plug-ins.	Edit the `Plugins.properties` file to set up all your lookup plug-ins. See "Editing the plug-ins properties file to enable the Symantec Data Insight lookup plug-in" on page 27.
Step 4	Set up a Network Discover scan of the file systems of interest.	See the *Symantec Data Loss Prevention Administration Guide*.
Step 5	Test that the details from the Symantec 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 47.

Configuring Symantec Data Loss Prevention for Symantec Data Insight

Before you can use the information from Symantec Data Insight, you need to configure the connection to the Symantec 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 the relevant information from the Symantec Data Loss Prevention incidents plus the information from the Symantec Data Insight Management Server.

See "Configuring the risk score and timeframes for the report of folders at risk" on page 23.

To configure the connection to the Symantec Data Insight Management Server

1. On the Enforce Server, click **System > Settings > Data Insight**.

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

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

2. Click **Configure**.

3. Enter the **Host Name** of the Symantec Data Insight Management Server.

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

5. Click **Retrieve Certificate**.

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

6. View the certificate that is returned from the Symantec Data Insight Management Server, and confirm that it is the correct certificate.

7. Enter the log on information to the Symantec 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. To verify the connection to the Symantec Data Insight Management Server, click **Test Connection**.

   This tests the connection to the specified Symantec Data Insight Management Server using the specified credentials. This **Test Connection** operation is available only after the server certificate is verified.

Configuring the risk score and timeframes for the report of folders at risk

Table 2-4 shows the parameters to configure the weights of the components of 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 Symantec Data Insight Management Server.

You can also configure the timeframes that are in the details of the report.

Table 2-4 Folder risk report configuration options

Parameter	Default	Description
Access History Timeframe	365	The number of days in the timeframe for user access in the risk score formula.
Unique Users Timeframe	7	The number of days that is the timeframe for the user access in the formula.
Formula	Severity and folder exposure	Select one of the following choices for the components in the risk score formula: ■ **Severity** The severity level of the incident in the Symantec Data Loss Prevention incident report. ■ **Severity and folder exposure** Folder exposure is the number of users who can read from the folder where the incidents were found. ■ **Severity, folder exposure and user access** 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.
Weights (0-100):		The severity weight of the item at risk. The maximum value of any weight is 100.
High Severity	100.0	Weight of a high severity item at risk.
Medium Severity	10.0	Weight of a medium severity item at risk.
Low Severity	2.0	Weight of a low severity item at risk.
Info Severity	1.0	Weight of an informational severity item at risk.

You can also configure the data refresh schedule to retrieve the information from the Data Insight Management Server.

See "Configuring the Data Insight data refresh properties file" on page 37.

About custom attributes and the Symantec Data Insight lookup plug-in

The Symantec Data Insight lookup plug-in pulls data from a Symantec 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.

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.

See the *Symantec Data Loss Prevention Administration Guide* for more information about incident attributes.

You must create custom attributes for each attribute you want populated from the Symantec Data Insight Management Server. You create only the custom attributes that you need.

See "Creating custom attributes" on page 25.

To populate custom attributes with the incident-related data, the Enforce Server uses a Symantec Data Insight lookup plug-in to retrieve the additional data from the Symantec Data Insight Management Server.

The names for the attributes are not predefined because the mapping can be configured.

See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.

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

- Data user. The data user is the user who most frequently accessed the file.
- 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.
- Business owner as defined in the Symantec Data Insight product.

The values for the custom attributes can also be re-populated by clicking on the **Lookup** option 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.

Note: If the new lookup returns null or empty values for any custom attribute fields, those empty values overwrite the existing values.

The start date of the access history can be configured for the plug-in.

See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.

Creating custom attributes

Custom attributes can be grouped into attribute groups, similar to how statuses are grouped into status groups, to organize the information in a useful way. Examples of common attribute groups include **Employee Information**, **Manager Information**, and **Remediation Information**. All custom attributes are available for all incidents.

To create custom attributes and add them to a group

1. On the Enforce Server, click **System > Incident Data > Attributes > Custom Attributes**. Note that a number of custom attributes were defined and loaded for you by the Solution Pack that you selected during installation. All existing custom attributes are listed in the **Custom Attributes** window.
2. To create a new custom attribute, click the **Add** option.
3. Type a name for the attribute in the **Name** box. If appropriate, check the **Is Email Address** box.

4 Select an attribute group from the **Attribute Group** drop-down list. If necessary, create a new attribute group. Select **Create New Attribute Group** from the drop-down list, and type the new group name in the text box that appears.

5 Click the **Save** option.

6 Generate a new incident, or view an existing incident, and verify that it contains the new custom attribute.

The name you give to a custom attribute does not matter. But a custom attribute you create must be structured the same as the corresponding external data source. For example, suppose an external source stores department information as separate geographic location and department name. In this case, you must create corresponding location and department name custom attributes. You cannot create a single department ID custom attribute combining both the location and the department name.

Once you define your custom attributes, they become available to every incident. Each incident receives its own set of custom attributes (though some name-value pairs may be empty depending on circumstances). The custom attribute values for an incident can be populated and changed independently of other incidents.

You can edit the custom attribute values if you have been assigned to a role that includes edit access for custom attributes. If you want to update a group of incidents, you can select those incidents on the incident list page. You can then select the **Set Attributes** command from the **Incident Actions** menu. You can select **Lookup Attributes**, to look up the values of custom attributes. Note that the **Set Attributes** command and **Attributes** section on the **Incident Snapshot** page are available only if at least one custom attribute is defined.

See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.

Configuring status attributes and values

As incidents are processed from discovery to resolution, each stage can be marked with a different status. The status lets you track the progress of the incident through your workflow. Based on the preferences of your organization and the commonly used terminology in your industry, you can define the different statuses that you want to use for workflow tracking.

The **Status Values** section lists the available incident status attributes that can be assigned to a given incident. The order in which status attributes appear in this list determines the order they appear in drop-down menus used to set the status of an incident. You can perform the following actions from the **Status Values** section:

Action	Procedure
Create a new incident status attribute.	Click the **Add** button.
Delete an incident status attribute.	Click the attribute's red X and then confirm your decision.
Change an incident status attribute.	Click on the attribute you want to change, enter a new name, and click **Save**. To change the name of an existing status, click on the pencil icon for that status, enter the new name, and click **Save**.
Make an incident status attribute the default.	Click **[set as default]** for an attribute to make it the default status for all new incidents.
Change an incident status attribute's order in drop-down menus.	■ Click **[up]** to move an attribute up in the order. ■ Click **[down]** to move an attribute down in the order.

To create a new incident status attribute

1. Go to the **Attributes** screen (**System > Incident Data > Attributes**) screen.

   Click the **Status** tab.
2. Click the **Add** button in the **Status Values** section.
3. Enter a name for the new status attribute.
4. Click **Save**.

Editing the plug-ins properties file to enable the Symantec Data Insight lookup plug-in

To enable the Symantec Data Insight lookup plug-in, you must edit the `Plugins.properties` file, and enable the Symantec Data Insight lookup plug-in.

To enable the Symantec Data Insight lookup plug-in

1. Open the `\Protect\config\Plugins.properties` file on the Enforce Server.

   The `Plugins.properties` file is a plain ASCII text file that can be edited with any text editor, such as Notepad (Windows), or vi (Linux).

2. Edit the `com.vontu.api.incident.attributes.AttributeLookup.plugins` property.

   Add `Data Insight Lookup` at the end of this property.

   Or you can comment out this line and remove the comment character from the line in the file that already has `Data Insight Lookup`.

   ```
   # Plugin JAR manifests to enable Data Insight lookups
   #com.vontu.api.incident.attributes.AttributeLookup.
   plugins=Data Insight Lookup
   ```

3. Edit the `com.vontu.plugins.execution.chain` property.

   If you use only the Symantec Data Insight lookup plug-in, that plug-in must be listed in the `com.vontu.plugins.execution.chain` property.

   ```
   com.vontu.plugins.execution.chain=com.vontu.
   lookup.datainsight.DataInsightLookup
   ```

   If you use multiple lookup plug-ins, their sequence in this property determines their order of execution.

   See "Adding other lookup plug-ins to the configuration" on page 33.

4. Remove the comment character from the line that defines the configuration file on the Enforce Server for Symantec Data Insight.

   ```
   # Data Insight Lookup configuration file
   #com.vontu.lookup.datainsight.DataInsightLookup.
   properties=DataInsightLookup.properties
   ```

5. Restart the Vontu Manager service for changes to the `Plugins.properties` file to take effect. The Incident Persister service must also be restarted.

Symantec Data Insight lookup plug-in mapping for custom attributes

Custom attributes are mapped to Symantec Data Insight information with entries in the `DataInsightLookup.properties` file. Each mapping is entered on a separate

line in the file. The order in which these mapping entries appear in the file does not matter.

A mapping is entered in the format:

```
Symantec Data Insight property  = attr.Custom Attribute Name
```

Where:

- *Symantec Data Insight property*
  The Symantec 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 attribute's name 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 in the `DataInsightLookup.properties` file as: `attr.Total\ Writes`.

See "Creating custom attributes" on page 25.

In this file, a mapping can also be defined for an arbitrary custom attribute that the subsequent plug-in in the lookup plug-in chain uses.

For example:

```
File_Total_Writes = attr.Total\ Writes
```

A separate entry is made in the `DataInsightLookup.properties` file for each custom attribute to be populated. For example:

```
## Custom attribute that corresponds to the
##   total number of read accesses

File_Total_Reads = attr.Total\ Reads

## Custom attribute that corresponds to the
##   total number of write accesses

File_Total_Writes = attr.Total\ Writes

## Custom attribute that corresponds to the
##   last user who modified the file
```

```
File_Last_Modified_By = attr.Last\ Modified\ By

## Custom attribute that corresponds to the
##   last time the file was accessed

File_Last_Access_Date = attr.Last\ Accessed
```

See "About Data Insight" on page 9.

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 general properties can be defined in the `DataInsightLookup.properties` file:

Config_Access_History_From_Date	Configurable access history start date for the Symantec Data Insight attributes in the format `yyyy-MM-dd`. If the date is blank, then the history is reported for all dates.
Config_Active_User_Count	Configuration of the number of active users to get from the Symantec Data Insight Management Server. Defaults to 1 if not specified. A best practice is to set this number to 5 or less.
Config_Active_Reader_Count	Configuration of the number of active readers to get from the Symantec Data Insight Management Server. Defaults to 1 if not specified. A best practice is to set this number to 5 or less.
Config_Active_Writer_Count	Configuration of the number of active writers to get from the Symantec Data Insight Management Server. Defaults to 1 if not specified. A best practice is to set this number to 5 or less.

The following file attribute properties can be defined in the `DataInsightLookup.properties` file:

File_Total_Reads	Custom attribute that corresponds to the total number of read accesses.
File_Total_Writes	Custom attribute that corresponds to the total number of write accesses.
File_Last_Modified_By	Custom attribute that corresponds to the last user who modified the file.
File_Last_Access_Date	Custom attribute that corresponds to the last time the file was accessed.
File_Access_History_Start_Date	Custom attribute that corresponds to the first time that access history for the file was collected.

The following data user access properties can be defined in the `DataInsightLookup.properties` file:

Data_User	Custom 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.
Data_User_Last_Access	Custom attribute that corresponds to the last time that the data user accessed a file. The format is `YYYY-MM-DD hh:mm UTC+/-hh`.
Data_User_Reads	Custom attributes that correspond to the read access count of the data user.
Data_User_Writes	Custom attributes that correspond to the write access count of the data user.
Business_Owner	Custom attribute that corresponds to the business owner of the data user as defined in the Symantec Data Insight Management Server.

The following user access properties can be defined in the `DataInsightLookup.properties` file.

Note: For more than two users, replace "n" with the user number. For example, enter `Most_Active_User_3`.

Most_Active_User_1 Most_Active_User_2 Most_Active_User_n	Custom attributes that correspond to the most active users. Configure the `Config_Active_User_Count` property to get more than one user.
Most_Active_User_Reads_1 Most_Active_User_Reads_2 Most_Active_User_Reads_n	Number of reads from the most active users. Configure the `Config_Active_User_Count` to get more than one user.
Most_Active_User_Writes_1 Most_Active_User_Writes_2 Most_Active_User_Writes_n	Number of writes from the most active users. Configure the `Config_Active_User_Count` to get more than one user.
Most_Active_Reader_1 Most_Active_Reader_2 Most_Active_Reader_n	Custom attributes that correspond to the most active readers. Configure the `Config_Active_Reader_Count` property to get more than one user.
Most_Active_Reader_Reads_1 Most_Active_Reader_Reads_2 Most_Active_Reader_Reads_n	Number of reads from the most active readers. Configure the `Config_Active_Reader_Count` property to get more than one user.
Most_Active_Reader_Writes_1 Most_Active_Reader_Writes_2 Most_Active_Reader_Writes_n	Number of writes from the most active readers. Configure the `Config_Active_Reader_Count` property to get more than one user.
Most_Active_Writer_1 Most_Active_Writer_2 Most_Active_Writer_n	Custom attributes that correspond to the most active writers. Configure the `Config_Active_Writer_Count` property to get more than one user.
Most_Active_Writer_Reads_1 Most_Active_Writer_Reads_2 Most_Active_Writer_Reads_n	Number of reads from the most active writers. Configure the `Config_Active_Writer_Count` property to get more than one user.
Most_Active_Writer_Writes_1 Most_Active_Writer_Writes_2 Most_Active_Writer_Writes_n	Number of writes from the most active writers. Configure the `Config_Active_Writer_Count` property to get more than one user.

Configuring the Symantec Data Insight lookup plug-in to populate the Data Owner fields

You can configure the Data Insight plug-in to populate the **Data Owner Name** field and the **Data Owner Email Address** field.

To configure the Data Insight plug-in to populate the Data Owner Name and Data Owner Email Address fields

1. Set up the connection to the Data Insight Management Server, and configure the Data Insight lookup plug-in.

   See "Locating and managing data at risk" on page 18.

2. Edit the `Plugins.properties` file. Specify that the incident parameters for the **Data Owner Name** field and the **Data Owner Email Address** field can be modified. Edit the `Plugins.properties` file, and verify that these fields are available for output:

   ```
   com.vontu.api.incident.attributes.AttributeLookup.output.parameters=
   data-owner-name, data-owner-email
   ```

3. Add `incident` to the following parameter:

   ```
   com.vontu.api.incident.attributes.AttributeLookup.parameters=incident
   ```

4. In the mapping in the `DataInsightLookup.properties` file, you can set the **Data Owner Name** field directly, instead of setting a custom attribute.

   For example:

   ```
   Data_User = attr.data-owner-name
   ```

5. You can also chain the LDAP Lookup Plug-In or the CSV Lookup Plug-In to set the **Data Owner Email Address** field.

   See the *Symantec Data Loss Prevention Lookup Plug-in Guide*.

Adding other lookup plug-ins to the configuration

The Symantec Data Insight lookup plug-in can be used in combination with the Lookup API and the other Symantec Data Loss Prevention 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.

For example, the Symantec Data Insight lookup plug-in provides the most active user as a custom attribute in the incident snapshot. Another lookup plug-in can then retrieve related information for that user, such as the department or the manager's email.

The Lookup API invokes one or more lookup plug-ins to interface with one or more external data sources. The lookup plug-in extracts the additional information that is related to the incident using the lookup parameters. Then the Lookup API populates the custom attribute fields of the incident with that additional information.

See the *Symantec Data Loss Prevention Lookup Plug-in Guide* for additional information about multiple plug-ins and complex lookup plug-in chains.

Symantec Data Loss Prevention provides the following types of lookup plug-ins, in addition to the Symantec Data Insight lookup plug-in:

- CSV Lookup Plug-In
  Enables the extraction of pertinent data from a comma-separated values (CSV) file.
- LDAP Lookup Plug-In
  Enables the extraction of pertinent data from a live LDAP system. For example, Microsoft Active Directory, Novell LDAP, Sun LDAP, or IBM LDAP.
- Script Lookup Plug-In
  Enables you to write a custom script in scripting languages such as Perl, Python, or VBScript, to extract the pertinent data. Scripts can extract data from sources such as proxy log files, or DNS systems.

To add additional lookup plug-ins to the configuration

1. Plan the interactions, and the order of execution, of all the configured lookup plug-ins.
2. Configure the additional lookup plug-ins.

   See the *Symantec Data Loss Prevention Lookup Plug-in Guide*.

3 Make sure that all the active lookup plug-ins are enabled in the `Plugins.properties` file. Enter all the active plug-ins on the line for the property `com.vontu.api.incident.attributes.AttributeLookup.plugins`.

The order that multiple plug-ins are listed in the `AttributeLookup.plugins` property does not matter.

```
com.vontu.api.incident.attributes.AttributeLookup.plugins=
Data Insight Lookup,Vontu Script Lookup
```

Note: All the enabled lookup plug-ins must be entered in the same line in this file. Note that some sample (commented) lines may be listed in the file for this property for each of the lookup plug-ins.

4 Define the execution chain and order of execution in the `Plugins.properties` file. Use the `com.vontu.plugins.execution.chain` property. The Symantec Data Insight lookup plug-in should be first in the execution chain so that the data user information is available to the other lookup plug-in.

```
com.vontu.plugins.execution.chain=
com.vontu.lookup.datainsight.DataInsightLookup,
com.vontu.lookup.script.ScriptLookup
```

Testing the Symantec Data Insight lookup plug-in

Before using the Symantec Data Insight lookup plug-in, you should test it.

To test the connection to the Symantec Data Insight Management Server

1 Configure the connection from the Enforce Server to the Symantec Data Insight Management Server.

See "Configuring Symantec Data Loss Prevention for Symantec Data Insight" on page 21.

2 On the **System > Settings > Data Insight** page, click **Test Connection** to verify the connection to the Symantec Data Insight Management Server.

This tests the connection to the specified Symantec 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.

See "Adding other lookup plug-ins to the configuration" on page 33.

See "Locating and managing data at risk" on page 18.

4 Click **Reload Lookup Plug-ins** to reload all the lookup plug-ins from the **Custom Attributes** tab of the **System > Incident Data > Attributes** screen. If the `Plugins.properties` file was changed, you also need to restart the Vontu Manager and Incident Persister services.

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 in the `DataInsightLookup.properties` file have been created.

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

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

2 Click **Reload Lookup Plug-ins** to reload the Lookup plug-in from the **Custom Attributes** tab of the **System > Incident Data > Attributes** screen. If the `Plugins.properties` file was changed, you also need to restart the Vontu Manager and Incident Persister services.

3 View an existing incident snapshot. Click the **Lookup** option on the 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 Symantec Data Insight lookup.
- If the correct values are not populated, or there is no value in a custom attribute you have defined, check the `DataInsightLookup.properties` file for mismatched items.

See "About Data Insight" on page 9.

Configuring the Data Insight data refresh properties file

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

The `DataInsightDataRefresh.properties` file is in the folder `C:\Vontu\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 and troubleshooting for finding and reporting on data at risk

The following best practices provide guidelines for implementation:

- Set up the Symantec Data Insight system and allow it to gather user information for a period of time.
  See the *Symantec Data Insight Administrator's Guide*.
  See "Where to get more information about Symantec Data Insight" on page 14.
- Make sure that the Enforce Server is connected to the Symantec Data Insight Management Server.
  See "Configuring Symantec Data Loss Prevention for Symantec Data Insight" on page 21.

- Configure your schedule to refresh the data from Symantec Data Insight to the Enforce Server.
  See "Configuring the Data Insight data refresh properties file" on page 37.
- Set up 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 Lookup Plug-in Guide*.

Chapter 3

Using the Symantec Data Insight data user information in reports

This chapter includes the following topics:

About reports of folders at risk

The **Folder Risk Report** helps information security analysts identify the top folders for investigation.

To display the folders at risk, click **Incidents > Discover**. In the **Discover Reports** on the left side, click **Folder Risk Report**. If the **Folder Risk Report** does not appear on the left side, then verify that the role for your user name allows access.

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.

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 Symantec 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.

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

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

Information and Options	Description
Filters	See "Filtering the information in the report of folders at risk" on page 44.
Folders with risk score	On the left is a list of folders with by the highest risk at the top. See "Viewing folders ranked by risk, path, or folder exposure" on page 41.
Top Data Owners	For the selected folder on the left, the top data owners are listed. See "Viewing details of a folder at risk" on page 43. 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 the Symantec Data Insight lookup plug-in to populate the Data Owner fields" on page 33.

Table 3-1 Information in the report of folders at risk *(continued)*

Information and Options	Description
Sensitive Files Access Trend	For the selected folder on the left, the trend for the past 12 months is listed. See "Viewing details of a folder at risk" on page 43. 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 23.
User/Group Activity View	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 43.

See "Viewing folders ranked by risk, path, or folder exposure" on page 41.

See "Filtering the information in the report of folders at risk" on page 44.

See "Viewing details of a folder at risk" on page 43.

See "Saving a report of folders at risk" on page 46.

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 "Locating and managing data at risk" on page 18.

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 Symantec 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 44.

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 43.

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 43.

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 Symantec 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 23.

- **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 Symantec Data Insight report links open a new browser window or tab to the Symantec Data Insight management console.
  You must log into theSymantec Data Insight management console before you can view these reports.
  See "Where to get more information about Symantec Data Insight" on page 14.

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 3-2 Details of a folder at risk

Report detail	Description
Top 5 Data Owners	Top five sensitive file data owners, ranked by the number of sensitive files owned (if data owners have been specified in the incidents).
Sensitive Files Access Trend	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 23. This table represents the number of unique users accessing sensitive files in the folder. The list is broken down by month.
User/Group Activity View	File activity of groups in the folder's ACL.

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 3-3 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 46.

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

Table 3-3 Filters for the folder risk report

Filter	Description
Incident Statuses	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. 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**."
Policies	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. To filter by policies: ■ 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 policies from the **All Policies** list. ■ Click the plus sign to move it to the **Included Policies** list. ■ Repeat for any other policies to include. ■ If you want to remove a policy out of the **Included Policies**, click the minus sign. ■ You can search for a policy by typing a string in the box underneath the **Include** label. Initially, this box says "**Search policies**."

Table 3-3 Filters for the folder risk report *(continued)*

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

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 44.

   See "Viewing folders ranked by risk, path, or folder exposure" on page 41.

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.
4. 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.
5. Click **Save**.
6. To edit a saved report, click **Save > Save** after you have edited the filters or changed the sort order.
7. To delete a saved report, click **Delete**.

Finding data users and accesses in incident reports

The Symantec Data Insight lookup plug-in populates the custom attributes that were defined and mapped during the configuration.

See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.

See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.

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 3-4 shows use cases with suggestions for reports.

Table 3-4 Use cases for reports

Use case	Description	Reports
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. Symantec 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 Symantec Data Insight" on page 52. 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 "Adding other lookup plug-ins to the configuration" on page 33. 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 Symantec Data Insight incident details" on page 50.

Table 3-4 Use cases for reports *(continued)*

Use case	Description	Reports
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. Symantec Data Insight provides information to drop down to the next resolvable account that names an individual. Symantec Data Insight provides several data user fields. See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.	Use the summary reports and filters to determine the incidents of interest. See "Creating summary reports for Symantec Data Insight" on page 52. 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 Symantec Data Insight Management Server. See "Viewing Symantec Data Insight incident details" on page 50. See "Selecting custom attributes for data user details" on page 51.
Data leak investigation	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 Symantec Data Insight Management Server. On the Symantec 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.	Use the summary reports and filters to determine the incidents of interest. See "Creating summary reports for Symantec Data Insight" on page 52. Use the incident snapshot report to view details of an incident. See "Viewing Symantec Data Insight incident details" on page 50. 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 Symantec Data Insight console" on page 51. In the incident snapshot, click the **Correlations** tab to view a list of the incidents that share attributes with the current incident.

Viewing Symantec 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 Symantec 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 Symantec 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 Symantec Data Insight console.

   See "Accessing the history of a file in the Symantec Data Insight console" on page 51.

Accessing the history of a file in the Symantec Data Insight console

To view additional details about file access, you can jump directly to the Symantec 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 Symantec Data Insight console, see the *Symantec 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 custom attributes and the Symantec Data Insight lookup plug-in" on page 24.

See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.

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 Symantec 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 Symantec Data Insight lookup plug-in, and configure them.

   See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.

   See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.

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.

4. You can select **Advanced Filters & Summarization**. Then run a summary by the Symantec Data Insight data user. This summary lists the users who most frequently accessed the files in the folder of interest.

5. After an analysis of incidents, you can determine if additional custom attributes are needed from the information that Symantec Data Insight provides. Then new custom attributes can be defined, configured, and looked up.

   See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.

6. 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 in the `DataInsightLookup.properties` file and a new lookup is run, the new mapping overrides any old values in the reports.

Creating summary reports for Symantec 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 Symantec 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.

   See "Saving custom incident reports" on page 53.

Saving custom incident reports

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

You can edit the report later on the **Edit Preferences** screen.

Optionally, you can schedule the report to be run automatically on a regular basis.

See "Scheduling custom incident reports" on page 54.

To save a custom report

1. Set up a customized filter or summary report.

   Click **Save > Save As**.

2. Enter a unique report name and describe the report. The report name can include up to 50 characters.

3. 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. 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. If you log on with a different role, the report is visible on the **Incident Reports** screen, but not accessible to you.

4. Click **Save**.

Scheduling custom incident reports

Optionally, you can schedule a saved report to be run automatically on a regular basis.

You can also schedule the report to be emailed to specified addresses or to the data owners on a regular schedule.

See the *Symantec Data Loss Prevention Data Insight Implementation Guide*.

See "Creating and distributing aggregated incident reports to data owners" on page 56.

To schedule a custom report

1. Click **Send > Schedule Distribution**.

   If SMTP is not set up on your Enforce Server, you are not able to select the **Send** menu item to send the report.

2 Specify the **Delivery Details**:

To:	Select whether the report is sent to specified email addresses or to the data owners.
Manual - Sent to specified e-mail addresses	Enter the specific email addresses manually in the text box.
Auto - Send to incident data owners	To send the report to the data owners, the **Send report data with emails** setting must be enabled for this option to appear. If you select to have the report sent to the incident data owners, then the email address in the incident attribute **Data Owner Email Address** is the address where the report is sent. This **Data Owner Email Address** must be set manually, or with a lookup plug-in. See "Creating and distributing aggregated incident reports to data owners" on page 56. See the *Symantec Data Loss Prevention Data Insight Implementation Guide*. A maximum of 10000 incidents can be distributed per data owner.
CC:	Enter the email addresses manually in the text box.
Subject:	Use the default subject or modify it.
Body:	Enter the body of the email. Response action variables can also be entered in the body.

3 In the **Schedule Delivery** section, specify the delivery schedule.

4 In the **Change Incident Status / Attributes** section, you can implement workflow.

The **Auto - Send to incident data owners** option must be set for this section to appear.

5. After sending the report, you can change an incident's status to any of the valid values. Select a status value from the drop-down list.
6. You can also enter new values for any custom attributes.

   These attributes must be already set up.
7. Select one of the custom attributes from the drop-down list.
8. Click **Add**.
9. In the text box, enter the new value for this custom attribute.

   After sending the report, the selected custom attributes set the new values for those incidents that were sent in the report.
10. Click **Next**.
11. Enter the name and description of the saved report.
12. Click **Save**.

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 3-5 Setting up, creating, and distributing aggregated incident reports to data owners

Step	Action	Description
Step 1	Install and set up the Symantec Data Insight Management Server. Make sure that the Symantec Data Insight Management Server has access to the files or file systems of interest.	See the following Symantec Data Insight documentation: ■ *Symantec Data Insight Installation Guide* ■ *Symantec Data Insight Administrator's Guide*
Step 2	Install the Symantec Data Loss Prevention product, including at least one Network Discover Server.	See the *Symantec Data Loss Prevention Installation Guide*.
Step 3	Set up the connection between the Enforce Server and the Symantec Data Insight Management Server.	See "Configuring Symantec Data Loss Prevention for Symantec Data Insight" on page 21. **Note:** Symantec Data Insight is a separately licensed option. If Symantec Data Insight is not licensed on the Enforce Server, the menu option to configure the connection to the Symantec Data Insight Management Server does not appear.
Step 4	Test the connection from the Enforce Server to the Symantec Data Insight Management Server.	See "Testing the Symantec Data Insight lookup plug-in" on page 35.
Step 5	On the Enforce Server, create a custom status value or custom attribute for the Data Owner Name verification, and any workflow status attributes.	See "About custom attributes and the Symantec Data Insight lookup plug-in" on page 24.

Table 3-5 Setting up, creating, and distributing aggregated incident reports to data owners *(continued)*

Step	Action	Description
Step 6	Map the details from the Symantec Data Insight Management Server into the custom attributes that you created.	Edit the properties file for Symantec Data Insight on the Enforce Server, to map the details from the Symantec Data Insight Management Server into the custom attributes that you created. See "Symantec Data Insight lookup plug-in mapping for custom attributes" on page 28.
Step 7	Map any of the Symantec Data Insight attributes directly into the **Data Owner Name** field.	To map the Symantec Data Insight data user (the person who uses the file most frequently) to the **Data Owner Name**, set the `Data_User` parameter. See "Configuring the Symantec Data Insight lookup plug-in to populate the Data Owner fields" on page 33.
Step 8	Set up all your lookup plug-ins. For example, you may want to chain the LDAP Lookup Plug-In to take the **Data Owner Name** and set the **Data Owner Email Address** 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 **Data Owner Email Address** can have multiple email addresses that are separated with commas. **Note:** If duplicate attribute names exist between these names and custom attributes, then both fields are updated.	Edit the `Plugins.properties` file to set up all your lookup plug-ins. See "Editing the plug-ins properties file to enable the Symantec Data Insight lookup plug-in" on page 27. See the *Symantec Data Loss Prevention Lookup Plug-in Guide*.
Step 9	Verify that the Enforce Server general settings are set up to send email notifications.	Set up the SMTP notification settings. Set the option **Send report data with emails**.

Table 3-5 Setting up, creating, and distributing aggregated incident reports to data owners *(continued)*

Step	Action	Description
Step 10	Verify that the incident responder has the privileges to run the reports.	The **Remediate Incidents** privilege is required to configure and run the reports. The **Lookup Attributes** privilege is required to set attributes from the lookup plug-ins. The User Privilege **CSV Attachment in Email Reports** is required to attach the CSV report to the email.
Step 11	Set up a Network Discover and run a sample scan of the file systems of interest.	
Step 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. See "Scheduling custom incident reports" on page 54. 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.
Step 13	Save the custom reports and set up a distribution schedule.	See "Saving custom incident reports" on page 53. See "Scheduling custom incident reports" on page 54.