Symantec Data Insight User's Guide

5.0

June 2016

Symantec™

Symantec Data Insight User's Guide

Documentation version: 5.0.4

Legal Notice

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. VERITAS TECHNOLOGIES LLC 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.

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

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 the company to answer your questions in a timely fashion.

Our 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 our support offerings, you can visit our website at the following URL:

www.veritas.com/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.veritas.com/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 Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

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

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/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
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

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

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Contents

Technical Support 4

Chapter 1 Introducing Symantec Data Insight 11

About Symantec Data Insight 11
About data custodian 14
About permissions 15
About SharePoint permissions 16
About audit logs 17
About migrated domains 18
Applications for Symantec Data Loss Prevention 19

Chapter 2 Using the Symantec Data Insight Management Console 20

About the Symantec Data Insight Management Console 20
Header 21
Tabs 21
Navigation pane 21
Content pane 21
Operation icons on the Management Console 22
Logging in to the Data Insight Management Console 23
Logging out of the Data Insight Management Console 24
Accessing online Help 24

Chapter 3 Navigating the Workspace tab 25

About the Data Insight Workspace 25
Using the Workspace filters 29
Managing the Workspace 31
Searching the storage device hierarchy 33
Searching for users and user groups 33

Chapter 4 Analyzing data using the Workspace views 35

About information risk 35
Viewing summary of data sources 36
Viewing shares summary 38

About control points 40
About the risk score for users 40
Viewing user summary 42
Viewing details of Watchlist users 43
Viewing details of alert notifications 44

Chapter 5 Viewing access information for files and folders 45

About viewing file or folder summary 45
Viewing the overview of a data repository 46
Managing data custodian for paths 46
Viewing the summary of user activity on a file or folder 49
Viewing user activity on files or folders 50
Assigning an inferred data owner as custodian 51
Assigning an active user as custodian 52
Assigning a custodian from the Permissions tab 52
Viewing file and folder activity 53
Viewing CIFS permissions on folders 54
Viewing NFS permissions on folders 55
Viewing SharePoint permissions for folders 56
Viewing audit logs for files and folders 56
About visualizing collaboration on a share 59
Analyzing activity on collaborative shares 60

Chapter 6 Viewing access information for users and user groups 62

Viewing the overview of a user 62
Viewing the overview of a group 63
Managing custodian assignments for users 64
Viewing folder activity by users 65
Viewing CIFS permissions for users 66
Viewing CIFS permissions for user groups 68
Viewing NFS permissions for users and user groups 69
Viewing SharePoint permissions for users and user groups 69
Viewing audit logs for users 71

Chapter 7 Managing inactive data 73

About managing data using Enterprise Vault and custom scripts 73
About Retention categories 74
About post-processing actions 75
Managing data from the Shares list view 75

Managing inactive data from the Folder Activity tab 76
Managing inactive data by using a report 77

Chapter 8 Using the Self-Service Portal 79

About the Self-Service Portal 79
Logging in to the Self-Service Portal 81
Using the Self-Service Portal to review user entitlements 81
Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents 83
Using the Self-Service Portal to confirm ownership of resources 84
Using the Self-Service Portal to classify sensitive data 84

Chapter 9 Using Data Insight reports 86

About Data Insight reports 86
Creating a report 87
About Data Insight security reports 88
    Access Details report 88
    Permissions reports 89
    Ownership Reports 106
Create/Edit security report options 108
About Data Insight storage reports 116
    Access Summary reports 117
    Capacity reports 117
    Data Lifecycle reports 119
    Consumption Reports 121
Create/Edit storage report options 125
About Data Insight custom reports 132
    About DQL query templates 132
    Creating custom templates for DQL queries 137
Create/Edit DQL report options 137
Considerations for importing paths using a CSV file 142

Chapter 10 Managing reports 143

Viewing report details 143
    About stale information in reports 145
Filtering a report 145
Editing a report 146
Copying a report 146
Running a report 146
Customizing a report output 148
Configuring a report to generate a truncated output 148

Sending a report by email 150
Automatically archiving reports 151
Canceling a report run 152
Deleting a report 152

Appendix A Command Line Reference 153

mxcustodian 154

Index 157

Chapter 1

Introducing Symantec Data Insight

This chapter includes the following topics:

- About Symantec Data Insight
- About data custodian
- About permissions
- About SharePoint permissions
- About audit logs
- About migrated domains
- Applications for Symantec Data Loss Prevention

About Symantec 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. This method enables more efficient remediation and data management.

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

Symantec Data Insight helps the 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.

Data Insight provides 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 ownership and the usage information from Data Insight can be used for the following purposes:

- Data owner identification
  Data Insight enables rule-based inference of data owners based on actual usage. Data 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 the information to tie the most active user of a file to a manager or responsible party for remediation steps.
- Data custodian identification
  Data Insight enables the 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 made any accesses on the files and folders. In addition to the physical paths, you can also assign custodians on DFS paths.
  See “About data custodian” on page 14.
- Data leak investigation
  In the event of a data leak, you may want to know who saw a particular file. On the Symantec Data Insight Management Server, you can view detailed information and an audit history of who accessed the data.
  See “About audit logs” on page 17.
- Locate at-risk data
  Data Insight enables organizations to find which shares or folders have overly permissive access rights. Organizations can use this data to prioritize risk-reduction efforts such as the discovery of sensitive data or a review of

permissions (or access control rights) to limit access to only those individuals who have a business need.

See "About permissions " on page 15.

See "About SharePoint permissions " on page 16.

- Manage inactive data

  Data Insight enables better data governance by letting you archive inactive and orphan data using Symantec Enterprise Vault. Additionally, you can decide to manage the archived data by applying retention rules, deleting the archived data, or by putting legal hold on the archived data.

  See "About managing data using Enterprise Vault and custom scripts " on page 73.

- Provide advanced analytics about activity patterns

  Data Insight enables you to analyze the activity on high-risk folders by providing in-depth analysis of usage and collaborative activity. The analysis helps you classify users based on configured attributes to better understand the activity pattern of users in your environment.

  See "About the Data Insight Workspace" on page 25.

  See "About visualizing collaboration on a share" on page 59.

- Permission remediation

  Data Insight leverages the usage analytics provided by audit logs to provide recommendations for revoking permissions of inactive or disabled users on a path. You can then analyze the business impact of applying the recommendations and configure settings to handle the permission changes.

  It also enables you to search for specific permissions and revoke them where necessary as also modifying group membership directly from the **Workspace**.

- Remediation using the Self-Service Portal

  Data owners and custodians can take remediation actions using the Self-Service portal. Custodians can log in to the Self-Service Portal to do the following:

  - View Data Loss Prevention (DLP) policy violations and remediate DLP incidents using Smart Response rules.
  - Review permission on resources and make recommendations to allow or revoke user access on resources.
  - Provide confirmation about whether the custodians indeed own the data resources that are assigned to them.

  For more information, see the *Symantec Data Insight Administrator's Guide*.

- Raise alerts

  You can configure policies to raise alerts when there is anomalous activity on sensitive data.

About data custodian

A Data Insight user assigned server administrator role can designate one or more persons as the custodian of a data location. The assigned custodian does not require access to files or folders.

Data Insight uses information about custodians to infer persons responsible for remediation and to determine report recipients. Tagging data repositories with custodians also provides you an explicit point-of-contact for data ownership queries.

A custodian is a user who has a record within Active Directory, NIS, NIS+ or LDAP. A group cannot be assigned as a custodian. The custodian tags are assigned at the parent level and are automatically inherited by all subfolders and files. Custodian tags are only assigned at filer, share, or folder level for CIFS and NFS file systems and Web application, site collection, or folder level for SharePoint. You cannot directly assign a custodian to files. In addition to physical paths, custodians can also be assigned on DFS paths.

Data Insight applies custodian assignment at any level in the following ways:

- If a subfolder is renamed within the same parent, no changes apply to custodian tags on that subfolder.
- If a subfolder is moved from one parent to another, then the inherited tags of the previous parent are removed and the tags of the new parent are automatically inherited.
- Tags that are explicitly assigned move with the subfolder. This also applies to everything under the sub-tree of the moved subfolder.

You must manually remove the custodian assignment from Data Insight. For example, if an assigned custodian's record is deleted from Active Directory, Data Insight does not automatically remove that custodian from the data location to which the custodian is assigned.

See "Managing data custodian for paths" on page 46.

You can automatically assign custodians on various paths and generate a comma-separated values (CSV) file with information about data custodian assignments using the `mxcustodian.exe` utility. For more details, See mxcustodian on page 154.

As a Data Insight administrator, you can assign custodians to multiple paths at once. For more infomation about assigning custodians in bulk, see the *Symantec Data Insight Administrator's Guide.*

About permissions

Symantec Data Insight enables you to view all users and groups and associated folder permissions. It gives you a hierarchical view of the groups' or a user 's effective access permissions to a file and folder.

Every folder is assigned a permission. It also can derive permissions from its parent folder. Effective permissions determine the type of access allowed to a user on a file or folder. Effective permissions are primarily derived from the combination of the following sources:

- The explicit permission assigned to a file or folder and its parent(s).
- The permissions a file or folder inherits from its parent(s).
- The relationship between specific users and groups who have been given permission.

For example, the folder, `/Finance/Payroll`, has the following permissions which are inherited by its children:

- *User 1* has read privilege.
- *Group 1* has read and write privilege.
- The folder `F1` under the `Payroll` folder has permissions as follows:
  - *User 2* has read privilege on folder `F1`.
  - *User 2* is part of Group 1.

In this case, Data Insight determines the effective permissions for file `F1` as follows:

- *User 1* has read privilege.
- *Group 1* has read and write privilege.
- *User 2* has read and write privilege. *User 2* inherits these privileges from *Group 1*.

Information about permissions when used with the access history of users helps to decide whether a user is assigned appropriate permissions. For example, sometimes a group is given full control, read, write, modify, and execute permissions to a folder. However, only certain users from the group access the folder. In such cases, visibility into permissions enables you to review and reassign permissions, as appropriate.

Visualization of access control information also enables you to analyze whether sensitive files are accessible only to authorized users. This in turn helps you monitor the usage of sensitive data and limit access to it, if necessary.

Data Insight lets you view NFS share permissions on folders, users, and groups. NFS permissions are Unix style permissions.

Data Insight does not retain membership information of a deleted user or group. Thus, the permission view of a deleted user or group contains only those data resources where the deleted user or group has explicit permissions (either on the folder or on the share).

About SharePoint permissions

Data Insight enables you to view SharePoint permissions that are granted to users and user groups on paths.

SharePoint users and user groups are not assigned the permissions directly. They are assigned permission levels. A permission level (role) is a set of specific permissions that is assigned to specific users or user groups. It helps in controlling which permissions are granted to the users and user groups.

In SharePoint, permissions are a part of a high level role and each role is a combination of permissions. Users and user groups are assigned roles rather than individual permissions. A site owner assigns these roles to different users and user groups. For example, the Read role assigned to a user or user group may be a combination of any of the following permissions in addition to the Limited Access permissions:

- View Items
- Open Items
- View Versions
- Create Alerts
- Use Self-Service Site Creation (when enabled at Web application)
- Browse User Information
- View Application Pages
- User Remote Interfaces
- Use Client Integration
- Features View pages

You can view the roles assigned to users and user groups on the Data Insight Management Console. A site owner is responsible for assigning these roles to different users and user groups. You cannot edit a role to include or exclude any permission from the Data Insight Console.

SharePoint has the following five default roles:

- Full Control
- Design
- Contribute
- Read
- Limited access

About audit logs

Symantec Data Insight collects and stores access events from file servers and SharePoint sites. These access events are used to analyze the user activity on various files, folders, and subfolders for a given time period. The audit logs provide detailed information about:

- Users accessing the file or folder
- The file type
- The access types such as:
  - Read
  - Write
  - Create
  - Delete
  - Rename
  - Security Event - Logged when the access control entries of a file or folder are changed. This event helps to identify who changed the permissions.
  - Permission Change - This event captures the details of permission changes to a folder.
- The access timestamp
- The IP address of the machine that the user has generated the access activity from.

The details of the Permission Change event provide information about the following:

- If a trustee (user or group) is allowed or denied permission on a path.
- If a trustee's permissions are removed on a path.
- If a trustee is given additional permission or denied certain permission on a path. For example, if a user 'X' has Read and Write permissions on a folder. If the

user is also subsequently allowed Modify permission on the folder, Data Insight records an Permission Change event.

Note: Currently, Data Insight fetches only the file system permission changes for CIFS paths only. It does not fetch Permission Change events for NFS or SharePoint paths. Permission changes at the share level are not reported.

You can use these access events for the following purposes:

- Audit permission changes on a folder.
- Understand who are the most active users of a file or folder in the event of a data leak.
- Carry out forensic investigations that help you understand the specific access events on sensitive data. For example, in case of a data leak, the information security team would want to know who accessed a particular file and the most active users of that file.
- Provide information about orphan data, that is data owned by users who have left the organization or moved to a different business unit.
- Provide information about the stale data that is never or rarely accessed.

For the purpose of calculating the access count, Data Insight records a read event when a user opens a file, reads it at least once, and closes it. Similarly, when a user writes to a file between an open and a close event, Data Insight considers it a write event. If there are read and write events, then one event is counted for each read and write.

See “Viewing audit logs for files and folders ” on page 56.

About migrated domains

During the course of operations, a directory service domain can be migrated to another domain. When a directory service domain migrates, the directory service assigns a new SID (Security Identifier) to each user and group from that domain. The original SID of each migrating user or group is added to an attribute called sIDHistory. Thus, sIDHistory attribute keeps track of all the previous SIDs of an object as it migrates from one domain to another.

When Data Insight scans a directory service domain, it fetches the sIDHistory attribute of all the users and groups. If Data Insight finds a user, say A, whose SID is present in the history of another user, say B, it knows that user A has migrated to user B. If user B is itself not contained in the sIDHistory of any other object in the directory service, Data Insight marks B as the latest user that user A has migrated into. Consequently, user A's LatestSID custom attribute points to user B on the Data Insight console. The LatestSID custom attribute links a user or group to its newest migrated version.

While Data Insight scans configured domains, it automatically adds a domain called MigratedSIDs. This domain is used to collect SIDs that are present in sIDHistory of some user or group, but do not belong directly to any object in Data Insight.

For example, if a user *test_user* in domain *test_domain* has the SID S-X-X-X-X in the sIDHistory, and there is no user in any directory service domain scanned by Data Insight with that SID, then Data Insight adds a new user *test_user#1* in the MigratedSIDs domain with SID S-X-X-X-X and it sets the user's LatestSID custom attribute to *test_user@test_domain*. When Data Insight adds multiple SIDs from sIDHistory of a user or group to MigratedSIDs domain, it suffixes the display name of the object with #1, #2, #3.

Data Insight considers the new SID and the SID history of the user to compute the effective permissions and to display user activity information. When Data Insight calculates effective permissions of a user that has some SID in the sIDHistory, it also adds explicit permissions of all the SIDs in the history. For example, if a user A in *domain D1* has migrated into user B in *domain D2*. User A has read permissions on a folder `test` while user B has write permissions on it, Data Insight shows user B as having both read and write permissions on folder `test`.

Applications for Symantec Data Loss Prevention

To understand how Data Insight works with Symantec Data Loss Prevention, see the *Symantec Data Loss Prevention Data Insight Implementation Guide*.

Chapter 2

Using the Symantec Data Insight Management Console

This chapter includes the following topics:

- About the Symantec Data Insight Management Console
- Operation icons on the Management Console
- Logging in to the Data Insight Management Console
- Logging out of the Data Insight Management Console
- Accessing online Help

About the Symantec Data Insight Management Console

The Symantec Data Insight Management Console is the main interface to a Data Insight deployment. You initially log in to the Management Console from a web browser, using your credentials.

Upon successful login, the Data Insight Management Console displays. The Workspace tab opens by default which displays a dashboard that provides a snapshot of all configured devices and users that Data Insight monitors. You can navigate to the underlying views that provide details about the activity and permissions for users and folders.

The other tabs consist of a navigation pane and the main content pane.

Header

At the top of the Console window, the header enables you to:

- Click **About** to display version information about the Data Insight deployment.
- Click **Logout** to disconnect from the Management Server.
- Click **Help** to access *Symantec Data Insight Management Console Help*.

Tabs

Beneath the header, a series of tabs provide access to each major area of the Symantec Data Insight Management Console:

- **Workspace**: View the activity on folders, access history of users, and permission details of users and user groups.
- **Policies**: View configured policies and create new policies. Also view and manage the alerts that are raised in response to configured policies.
- **Reports**: Generate and view reports.
- **Settings**: Customize the settings for the Management Server and other product servers, configure NAS devices, define and manage user accounts, and view events.

Navigation pane

The Data Insight Management Console displays a navigation pane on the left side for all tabs, except the **Workspace** tab. The navigation pane gives you quick access to specific information depending on the tab you have selected. For example, on the **Reports** tab, you can view a list of all the supported report types or on the **Settings** tab you can view the list of the settings required to configure Data Insight.

Content pane

The Symantec Data Insight Console’s main display area, or content pane, displays information about folders, files, users, configuration data, and events. The information displays in a variety of tabular and graphical formats. You can also perform tasks like exporting data to a file and emailing the data to business owners.

Note: In some of the tables, only the default columns are displayed. The less important columns are hidden from the default view. You can un-hide them by hovering your mouse pointer over any column header and clicking the downward arrow. It gives you a list of available columns to select from. Also you can sort the table data by clicking either **Sort Ascending** or **Sort Descending** options in the drop-down menu.

Operation icons on the Management Console

Table 2-1 shows the operation icons that are located on the console screen:

Table 2-1 Operation icons on the Management Console

Icon	Description
☒	Go up one level in the navigation control.
☒	Filter filers, Web applications, shares, site collections, users, and groups. The filter options depend on the current level of hierarchy.
☒	Clears the filter.
☒	The settings icon is used in assigning custodians.
☒	Screen refresh. Symantec recommends using this refresh button instead of your browser's **Refresh** or **Reload** button.
☒	Email the data on the current screen to one or more recipients. If the current screen's data cannot be sent as an email, the icon is unavailable.
☒	Exports all data on a panel on the current screen to a `.csv` file.
☒	Exports all data on the current screen to a `.csv` file.
☒	Submits request to the Enterprise Vault server to archive the selected folders.

Table 2-1 Operation icons on the Management Console *(continued)*

Icon	Description
☒	The action selector icon displays a menu with the following two options: ■ Archive files using Enterprise Vault. ■ Submit request to invoke a custom action on selected paths.
☒	Submit request to invoke a custom action on selected paths.

Logging in to the Data Insight Management Console

To log on to the console from the Management Server or a worker node

1. Do one of the following:
   - Click the shortcut created on the Desktop during installation.
   - Click **Start** > **Programs** > **Symantec** > **Symantec Data Insight** > **Data Insight Console**.
2. On the Login screen, enter the credentials of a user with privileges to log in to the Management Server.
3. Enter the name of the domain to which the user belongs.
4. Click **Submit**.

   The Management Console appears.

To log on to the console from a machine other than the Management Server or the worker nodes

1. Open a Web browser and enter https://<*ms_host*>:<*ms_port*>. For example, https://datainsight.company.com:443.
2. On the Login screen, enter the credentials of a user with privileges to log in to the Management Server.
3. Enter the name of the domain to which the user belongs.
4. Click **Submit**.

   The Management Console appears.

Logging out of the Data Insight Management Console

To log out

1. Click logout at the top right of the screen.
2. Click **OK** to go back to the login screen.

Accessing online Help

Symantec Data Insight offers a browser-based online Help system. You can access the online Help from anywhere in the Data Insight Management Console.

To access online Help, in the Console header or, in a dialog box or wizard, click **Help**. The online Help displays.

Navigating the Workspace tab

This chapter includes the following topics:

- About the Data Insight Workspace
- Using the Workspace filters
- Managing the Workspace
- Searching the storage device hierarchy
- Searching for users and user groups

About the Data Insight Workspace

The **Workspace** tab of the Data Insight Management Console gives you in-depth analytics of the configured data sources and users who have activity on these data sources. When you log on to Data Insight, you are automatically directed to the Data Insight dashboard. The dashboard enables interactive navigation and it lets you drill down to the deepest level of the file system hierarchy to view analytics for configured data sources and users. The information on the dashboard is summarized in tile-like panels. You can view details of the displayed data by navigating to the **List View** of the tile.

Note: Data Insight recommends that you use a resolution of 1600 * 1024 to be able to view the all columns on the Dashboard properly.

The dashboard helps you do the following:

- Visualize complex analytics about activity, risk, and storage.

- Review access pattern of watch-listed users.
- Review the alerts that are generated when configured policies are violated.
- Analyze the dashboard data from different perspectives.

You can use the **Security**, **Activity**, or the **Storage** views to change the perspective of the data that is displayed on the dashboard. For example, the **Security** view displays information about the number of sensitive files in a storage repository, number of active users on these data sources, and the risk score of the most active users. Whereas, the **Activity** view provides the information about the number of access events, the number of active files, the most active users. By default, the dashboard opens the **Security** view.

Note: By default, the **Users**, **Watchlist**, and **Alerts** list views display data only for the **Security** perspective.

The tiles on the dashboard display all configured data sources, shares, and users listed in order of their risk score. Scroll to view all configured entities on a tile or click **More** to review the details of a specific entity.

By default, the information displayed by the Workspace is refreshed once every day. However, you can compute the dashboard data on the **Workspace** any time by running the dashboard report manually from the **Advanced Analytics** settings. Click **Actions** > **Refresh** to reflect the most current data on the dashboard.

For information about the configuring advanced analytics, see the *Data Insight Administrator's Guide*.

The Data Insight **Dashboard** displays the following tiles:

Table 3-1 Workspace Dashboard tiles

Tile	Description
Data Sources	Displays all the configured data sources such as filers, SharePoint web applications, and cloud storage accounts. The data sources are listed in order of their risk score. Depending on the view that you select, the tile displays the following information: ■ Number of sensitive files on the data source. ■ The number of shares with sensitive data on them. ■ The risk score assigned to a share after considering the number of open shares, active user count, and the number of sensitive files on the share. ■ The size of inactive data on a data source. ■ The number of active users on the data source. See "Viewing summary of data sources" on page 36.
Shares	Displays all shares that Data Insight monitors. Depending on the view that you select, the tile displays the following data: ■ The number of sensitive and active files on a share and the number of open shares. ■ The risk score of a share considering the active user count and the sensitive file count of the share, and the maximum permitted user count for the share. A higher count of active users and sensitive files contributes to a higher risk for a share. See "About information risk" on page 35. ■ The activity (number of accesses) on the share. ■ The total files on the share and the total size of the data on the share. See "Viewing shares summary" on page 38. You can manage inactive data from the **Shares** list view. See "Managing data from the Shares list view" on page 75.

Table 3-1 Workspace Dashboard tiles *(continued)*

Tile	Description
Users	Displays all configured users in Data Insight. The tile displays the following information: ■ The risk score of a user based on parameters such as abnormal access pattern, accesses made on sensitive data, and the number of alerts raised against the user. See "About the risk score for users" on page 40. ■ The number of shares on which the user has permissions. ■ The number of sensitive files that are accessed by the user. ■ Th total accesses by the user across all configured devices in he last 15 days (default). ■ The number of unique files accessed by the user in the last 15 days (default). See "Viewing user summary" on page 42.
Watchlist	Displays the list of users on the administrator's watch list, sorted according to the risk score assigned to them. For information about configuring a the watch list settings, see the *Data Insight Administrator's Guide*. See "Viewing details of Watchlist users" on page 43. **Note:** The **Watchlist** tile and list views are only visible to the user assigned the Server Administrator role.
Alerts	Displays the summary count of alert notifications raised against configured policies and the severity of the alerts. See "Viewing details of alert notifications" on page 44. **Note:** The **Alerts** tile and list views are only visible to the user assigned the Server Administrator role.

Note: Data Insight persists the last view that is open on the **Workspace** tab when you log out. You can start where you left off when you log in to Data Insight again.

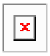
See "Managing the Workspace" on page 31.

See "Using the Workspace filters" on page 29.

Using the Workspace filters

Data Insight provides extensive filters to sort through the data on the list view pages. You can use the filters to limit the scope of the data that is displayed on the list views of the **Workspace** tab. When filters are applied, the list views display the data that satisfies the selected filter criteria.

Figure 3-1 Workspace filters



To use the filters

1. Navigate to the list view of the tile for which you want to view analytics data.
2. On the list view, click on the filter icon.

   The filter panel expands to show the available filters.

   To display only the frequently-used filters, click the **Filter** drop-down, and select the filters that you want to display.
3. Click on any option and enter or select the values for the filter criteria.

   For example, you want to review all the open shares in your storage environment that have a risk score between 80 to 100. Navigate to the **Shares** list view and expand the filter panel. Select the **Open** check box; click **Risk**, and slide the score slider to select the range of the risk score.

   If a filter has many possible values, you can enter specific value in the search bar for that filter. For example, if there are multiple DLP policies that are configured, you can enter that name of the DLP policy that you are interested in the **DLP Policy** filter.

   Note: If you select more than one filter criteria, the conditions are evaluated using a logical AND operator. However, if you select multiple values for a single filter criteria, Data Insight evaluates the values using the logical OR operator.
4. Click **Apply**.
5. Click **Reset** to clear the filters.

Note that different filters are available for the **Data Sources**, **Shares**, **DFS**, **Users**, **Groups**, **Watchlist**, and **Alerts** list views.

Note: An orange **Filter** icon indicates that a filter is applied to the displayed data set.

Filter	Description
Disabled	Displays disabled filers, shares, or users.
Deleted	Displays all users that have been deleted from the directory service. This filter is only available on the **Users** list view.
Custodian	On the **Data**and **Shares** list view, the filter displays all users who are assigned as custodians on paths. On the **Users** list view, select **Custodian** check box to displays all paths on which a user is assigned as custodians.
Control Point	Displays the number of control points across configured shares or site collections. On the **Shares** list view, select the **Control point** check box to display all paths in the file system hierarchy where the permissions differ from that of the parent folder or where the active users differ significantly from active users of its sibling folders.
User Name / **Group Name**	Displays analytics pertaining to the specific user or group.
Open Shares	This filter option is only available on the **Data Sources** and **Shares** list view. On the **Data Sources** list view, you can further refine the condition by selecting the size of the share and the number of files on the open shares. Displays all open shares across all configured filers or on selected filers.
Path	For a share, enter the full or part of the path name, IP address, or URL as the case may be.
Risk	Use the slider to enter a value for the risk score. The threshold for the risk score for users and data sources is 50. A risk score more than 50 may be a cause for concern. This filter condition is available for the **Data Sources**, **Shares**, and **Users** list view.
Device Type	Select the type of device for which you want to view analytics.

Filter	Description
Activity	Use the slider to specify the number of accesses. For example, you can use the **Activity** filter with the **Device Type** condition to search for all NetApp filers that have accesses between 50000 and 700000. On the **Data** list view, you can also select the type of activity for which you want to view analytics - None (No activity), Collaborative, or Single user.
Files	Use the slider to choose the number of sensitive, active, or inactive files in a content repository. For example, you can use the **Files** criteria along with the **Device Type** filter to find the number of sensitive files on a Box share.
Size	
DLP Policy	Select one or more Data Loss Prevention (DLP) policies that are violated by files or folders being monitored by Data Insight. For example, you can search for all files or folders that violate the conditions specified by the HR policy.
Domain	From the list of configured domains, select the domain for which you want analytics data. Click **More** to display all domains configured in Data Insight. Or enter the name of a domain in the search bar to search for a specific domain.
Owner	Enter the name or part of a name of the owner of a file or folder. The criteria for computing the owner of a data resource is configured in the Workspace Data Owner Policy. For more information, see the *Symantec Data Insight Administrator's Guide*.
Custom attributes	Select one or more values for all or any custom attribute. The attributes that are displayed as filters depend on the custom attributes that are configured in Data Insight.

Managing the Workspace

The **Workspace** tab consists of a dashboard that serves as a landing page when you first log in to Data Insight. The Data Insight dashboard provides interactive visualization of the content repositories and users that Data Insight monitors. It also provides a way to navigate to the underlying detailed views.

See “About the Data Insight Workspace” on page 25.

The list views on the **Workspace** tab provide advanced analytics about configured data sources and users that Data Insight monitors.. The list views also provide a high-level summary of the configured storage devices and users from the perspective of space utilization, activity, number of sensitive files, and permissions.

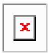
You can further navigate to the underlying profile views that provide analytics on activity and permissions from the list views.

You can navigate to the detailed list views by from the **Dashboard** in the following ways:

- Select the entity for which you want to view the details from the menu at the top-left corner of the **Dashboard**.
- Click the **Data**, **Users**, or **Groups** tabs to directly navigate to the respective list views.
- Click **More** on any tile on the Dashboard. Or click the total number for that entity at the top of each tile.

You can use the search bar at the top of the **Dashboard** and the list-view screens to navigate to the **Overview** tab of a path or a user.

Figure 3-2 Working with the list-views



You can sort, filter, and change the context of the data displayed on the dashboard and list view of the **Workspace** tab.

Changing your current View

Data Insight lets you change the perspective of your data by changing your currently displayed View.

To change the currently displayed view

1. Click the down arrow next to the currently selected View. Select **Security**, **Activity**, or **Storage**, as required.

   The perspective of the data displayed on the list view changes.

2. Select **Create View**.

   On the pop-up, enter a logical name for the view and select the specific columns that you want to display.

To extract the contents of the dashboard

◆ From the Dashboard or list-view, click **Actions** > **Export**.

See “Using the Workspace filters” on page 29.

Searching the storage device hierarchy

.

You can drill down to the detailed information about the attributes and access pattern of files, folders, and web applications from the **Data Sources** or **Shares** list views and from the Dashboard on the **Workspace** tab.

You can navigate shares, sites, and folder hierarchy.

To search for a storage device,

1. On the **Dashboard** and list views of the **Workspace**, click the filter icon to expand the **Filter** and select your filtering criteria.
2. From the **Workspace** dashboard, navigate to the **Data Sources**, **Shares**, **DFS** list view.
3. On the list view page, do one of the following:
   - Drill down the filer or web application hierarchy to review the details on the **Summary** panel on the right.
   - From the **Summary** panel, click **Expand Profile** to drill down to the detailed views. Or click the object name in the list view to navigate to the detailed views.
   - Use the **Go to** bar at the top of the content pane to type the full path that you want to open. Type the path in the format, `\\filer\share\path` in case of a CIFS location, and filer:/share/path in case of an NFS location and `http://<URL of the SharePoint site>` to search for a site. The **Go to** bar also supports auto-complete which gives you suggestions for paths as you type.

     You can view the sibling paths of the filer, share, site collection, or folder on the path that you type in the **Go to** bar. Click the drop-down arrow to view the list of all the siblings of a particular entity. You can also apply the filter on a sibling path to directly access a particular entity.

See “Viewing the overview of a data repository ” on page 46.

Searching for users and user groups

You can view the detailed information about the access pattern of users and user groups and the permissions assigned to them from the list-views of users and groups.

In the **Workspace** tab, click the **Users** or **Groups** sub-tab to navigate to list-views of users or groups. Alternatively, click on the menu the left and select **Users** or **Groups**.

Optionally, you can navigate to the users list-view by clicking the **More** link from the **Users** tile.

You can search for users or user groups in one of the following ways:

Using filters	To search for users or groups, click the filter icon and and select your filtering criteria. See "Using the Workspace filters" on page 29. Use the **Domain** condition to filter default Windows Built-in users and groups, such as the Everyone group, unresolved SIDs, and users and groups from migrated domains. Unresolved SIDs result when users or groups are deleted in the directory service, and Data Insight cannot map them to users or groups in the Data Insight users database. See "About migrated domains" on page 18.
Using the Go To bar on the Dashboard and list views	Enter the name or security identifier (SID) value of a user or group.

See "Viewing the overview of a user" on page 62.

See "Viewing the overview of a group" on page 63.

Chapter 4

Analyzing data using the Workspace views

This chapter includes the following topics:

- About information risk
- Viewing summary of data sources
- Viewing shares summary
- About the risk score for users
- Viewing user summary
- Viewing details of Watchlist users
- Viewing details of alert notifications

About information risk

Data Insight enables you to identify the risk to critical data sources and helps you effectively protect them. It assigns a risk score to the configured shares that enables you to understand the importance of the data source and the need to protect it. Note that cloud storage accounts and site collections are also considered as shares for the purpose of computing the risk score.

The information risk score takes into account multiple attributes such as permissions, activity, and number of sensitive files in a share that contribute towards the risk factor of a share. For every share, Data Insight displays a risk score between 0 and 100. A risk score over 50 signifies a higher risk for the share.

You can use the risk score information to remediate permissions and monitor activity on the shares that Data Insight flags as being risky.

For information about permission orchestration and configuring user watchlist settings, see the*Symantec Data Insight Administrator's Guide*.

The risk score that is assigned to a data source is computed at share level and is calculated based on the following criteria:

The open factor for a share	This value is the number of users who have permissions on a share that is classified as open according to open share policy or the number of users who have permissions on a share as compared to the highest number of users with permissions on any share configured in Data Insight. For more information about configuring the open share policy, see the *Symantec Data Insight Administrator's Guide*.
The number of sensitive files in a share.	Number of sensitive file counts for a share as compared to the maximum sensitive file count on any share configured in Data Insight.
The number of active users for a share.	This value is the number of active users on a share as compared to the maximum number of active users on any share configured in Data Insight.

See “Viewing shares summary” on page 38.

Viewing summary of data sources

The list view of the **Data Sources** displays the complete list of configured data sources such as file servers, SharePoint web applications, and cloud storage accounts. Click the plus sign next to a data source to drill down the hierarchy of a data source such as share and site collection.

Depending on the perspective that you have selected, you may view the following details about a data source:

- The total number of files on the open shares on a data source.
- The disk space occupied by the open shares.
- Number of sensitive files present in a data source.
- Number of users with activity on the data source.
- Risk score assigned to the shares or site collections under the data source.

The bubble chart is divided into ten buckets, with each bubble signifies a risk range. The higher five buckets are orange and signify a higher risk range. The size of the bubble signifies the percentage of shares or site collections on a data source that are in a particular risk range.
See “About information risk” on page 35.

- Total activity reported for the data source.
- Total number of files with activity and the number of active users.
- Total number of files contained, the disk space occupied by the contents, the inactive users, and inactive data size on the data source.

Select a row in the **Data Sources** page to see a summary of the corresponding data source. Depending upon currently selected the level of the file system hierarchy, **Summary** panel displays the following information:

- Total number of open shares on the data source.
  Open shares are the shares that are accessible to global access groups, like Everyone, domain users, and Authenticated Users on the network, or shares that match the criteria defined in the open share policy. Such open shares may contain sensitive data.
  For information about configuring open share policy, see the *Symantec Data Insight Administrator's Guide*.
- Whether it is a control point and the number of control points in the data source hierarchy.
- The size on disk.
  This size can be different from the logical size of the share or site collection. If a path is archived by Enterprise Vault, its on-disk size is much lower than its logical size.
- The owner of the data source and the Workspace Data Owner Policy used to compute the owner.
- The type of the data source. For example NetApp, EMC Isilon, Windows File Server, cloud storage account etc.
- Number of shares, folder, and active users present.
- Graphical view of risk range.
- The Data Loss Prevention policies that have been violated
- The custodian assigned on the data source or on any path in the hierarchy of the data source.
- Details of the attributes of the users who have activity on the data source.

Click **Expand Profile** on the **Summary** panel to open the profile panel for the data source. The profile panel lets you view the following:

- Details of active, inactive, and sensitive files.
- The overview of the data source
  See "Viewing the overview of a data repository " on page 46.
- Details of custodians assigned for the data source.
  See "Managing data custodian for paths" on page 46.

See "Managing the Workspace" on page 31.

See "About the Data Insight Workspace" on page 25.

Viewing shares summary

The list view of the **Shares** tile displays the complete list of shares that are configured in Data Insight. Click the plus sign next to a data source to drill down to the folder level details.

Depending on the selected perspective, you may view the following details about your data source:

- Information whether a share is an open share.
- The type of activity that is reported for the share. For example, none (no activity), single user, multi-user, or collaborative activity.
- Number of sensitive files present on the share.
- Total number of active users.
- The risk score of a share considering the maximum number of users with permissions on the share, the active user count, and the sensitive file count of the share. A higher count of users who access the share and sensitive files on the share contribute to a higher risk for a share.
  See "About information risk" on page 35.
- Total access count reported on the share.
- Total number of active files present in the share.
- Total files present in the share.
- Disk-space occupied by the share.
- Inactive data size.

Select a row in the **Shares** list-view to see a summary of the corresponding share. The **Summary** panel displays the following information of a share:

- Information whether the share is an open share.
  For information about open shares and configuring an open share policy, see the *Symantec Data Insight Administrator's Guide*.
- Whether the share is a control point.
  See “About control points” on page 40.
- The owner of the data source and the Workspace Data Owner Policy that is used to compute the owner.
- Total disk-space occupied by the share.
- Total number of files present on the share.
- Details of the user who owns the share.
- Counts of folders, active users, and control points present in the share.
- Counts of active, inactive, and sensitive files present in the share.
- Risk-score for the share.
- The Data Loss Prevention policies that have been violated
- The custodian assigned on share.
- Attributes of the users who have activity on the data source.

You can archive paths direct from the **Shares** list view.

See “Managing data from the Shares list view” on page 75.

Click **Expand Profile** on the **Summary** panel to open the profile panel for the share or site collection. You can do the following on the profile views:

- View overview information for the share or site collection.
  See “Viewing the overview of a data repository ” on page 46.
- View and assign custodian
  See “Managing data custodian for paths” on page 46.
- View details of user activity on the paths.
  See “Viewing user activity on files or folders” on page 50.
- View details of activity by configured users on the paths.
  See “Viewing file and folder activity” on page 53.
- View the details of permissions on the paths.
  See “Viewing CIFS permissions on folders” on page 54.
- View audit logs.
  See “Viewing audit logs for files and folders ” on page 56.

About control points

A control point is the level in a file system heirarchy where permissions must be changed. A control point on a share is defined as a folder which is primarily accessed by a set of users who are either a subset of or are completely different from the users who access its sibling folders within the share. The users are grouped into sets using well describing attributes.

Control points can be any of the following:

- Folders where permissions deviate from the parent folders, either the folder does not inherit permission from the parent folder or unique permissions are assigned at that level in the hierarchy.
- Folders where the active users differ significantly from active users of its sibling folders.

To identify control points within a share, Data Insight starts its analysis from the defined folder depth within the share. Data Insight then compares the user set that is accessing such a folder for similarity with its ancestors. The control point is defined at the level below which the similarity breaks significantly. The default folder depth for computing control points within a share is 5. This means that by default, Data Insight evaluates the folder hierarchy 5 levels deep to calculate the control points within a share.

For more information on configuring the depth for calculating control points, see the *Symantec Data Insight Administrator's Guide*.

You can use information about control points within a share to provide recommendations to improve existing permissions.

About the risk score for users

Data Insight enables you to monitor malicious activity in your storage environment. Data Insight profiles all users by assigning a risk-score to every configured user. Higher the risk score of a user, higher is the perceived risk posed by the user.

A risky user typically displays anomalies such as:

- Abrupt deviation in activity pattern where deviation on activity on sensitive files is given more weightage. (Anomaly)
- The fraction of the total number of data sources that a user has permissions on.(Access)
- Abnormal increase in number of alerts against the user. (Alerts)

Note that the user risk score is computed by considering the individual scores of different parameters for the last 15 days by default.

Data Insight computes the risk-score for a user based on the weighted sum of individual scores of the following parameters.

Table 4-1 Components for computing user risk score

Components	Descriptions
Deviation in accesses pattern on sensitive and non-sensitive files.	The overall deviation score is the weighted sum of the deviation values for sensitive and non-sensitive files.
Number of alerts against the user.	Percentage of alerts for a user against the total number of alerts, weighted by the severity of the policy that was violated.
Number of shares the user has read/write access on.	Percentage of shares on which the user has read access, against the total shares across all the storage devices.
Number of shares the user has write access on.	Percentage of shares on which the user has write access, against the total shares across all the storage devices.
Number of shares the user is custodian on.	Percentage of shares for which the user is a custodian, against the total shares across all the storage devices.
Deviation in the number of unique files that are accessed by the user. (Considering sensitive and non-sensitive files)	Overall score is the weighted sum of unique files that are accessed during past 15 days.
Deviation in the number of unique files that are accessed by the user. (Considering sensitive files only)	Overall score is the weighted sum of unique files that are accessed during past 15 days.
Deviation in the number of distinct DLP policies violated by the files accessed by the user.	Overall score is weighted sum of DLP policies. The weights are proportional to the severity level of the policies.

Note that Data Insight assigns a default priority to these parameters when calculating their weighted sum.

The risk score assigned to a user helps you do the following:

- Identify potentially malicious users.
- Review the permissions that are granted to the users.
- Review if a risky user is a custodian on any storage resource.

- Review the top active data that is being accessed by the risky user.
- Add a user with a high risk score to a watchlist to enable you to closely monitor the user's activities.

See “About the Data Insight Workspace” on page 25.

See “Viewing user summary” on page 42.

Viewing user summary

The **User** list-view shows you the granular details of configured users.

The following details are displayed:

- The grouping attribute of the user.
  For more information about configuring the primary grouping attribute, refer *Symantec Data InsightAdministrator's Guide* .
- The total activity by the user across configured devices for the last 15 days .
- The number of number of unique files accessed by the user in the last 15 days.
- The risk-score of the user.
  An orange bar graph denotes a risk score of more than 50.
  See “About the risk score for users” on page 40.

An orange user icon indicates that the user is included in the watchlist configured by the Data Insight administrator.

Select a row in the **Users** tile see a summary of the corresponding user. The **Summary** panel displays the additional information about a user such as:

- The status of the user - whether the user is disabled or deleted.
- The attributes configured for the user.
- The risk score assigned to a user.
- The top shares the user has activity on.
- A graphical representation of the user's activity profile over the configured advanced analytics period.
- The breakdown of the type of accesses made by the user, such as the number of reads, writes, deletes, etc.
- The Data Loss Prevention policies that the user has violated in the last 15 days.
  Data Insight integrates with DLP to pull data classification information. However, the classification information can also be imported into Data Insight by using a CSV file.

Click **Expand Profile** on the **Summary** panel to open the profile panel for the user. The profile panel lets you drill down to further details the following:

- The overview of the user's attributes, such as display name of the user, the SID, the attributes configured for the user, and the groups the user belongs to.
  See "Viewing the overview of a user" on page 62.
- The details of the paths on which the user is assigned as custodian.
- The details of accesses made by the user, arranged by time and by folders.
  See "Viewing folder activity by users" on page 65.
- The permission details for a selected user.
  See "Viewing SharePoint permissions for users and user groups" on page 69.
- Audit logs for the user.
- See "Viewing audit logs for users " on page 71.

Viewing details of Watchlist users

The **Watchlist** tile on the Dashboard gives you a snapshot of the users who are included in the watchlist. You can include users with a high risk score or highly privileged users (users who have permissions to access critical data sources) on the watchlist.

The users in a watchlist are ordered in the decreasing order of individual risk scores. For information about configuring the user's watchlist, see the *Symantec Data Insight Administrator's Guide*.

You can drill down to the Watchlist list view from the Dashboard to review the following details for the watch-listed users:

- The primary grouping attribute configured for the user.
- The number of shares on which the user has activity.
- The number accesses made by the user.
- The number of shares on which the user has permissions.
- The number of files accessed by the user.
- The number of sensitive files accessed by the user.
- The risk score of the user.
  See "About the risk score for users" on page 40.

Select a row in the **Watchlist** list-view to see a summary of the selected users. The **Summary** panel displays the following information of a share:

- The status of the user - if disabled or deleted.

- The total accesses made by the user, and the breakdown of the type of accesses.
- The specific shares on which the user has most accesses.
- The break up of the factors considered to compute the risk score for the user.
- The number of alerts raised against the user.

Click **Expand Profile** to navigate to the user-centric tabs for a watch-listed user.

See “Viewing user summary” on page 42.

See “About the Data Insight Workspace” on page 25.

Viewing details of alert notifications

The Alerts list-view displays the following details:

- The name and type of policy against which the alert is raised.
- The severity and the number of the alerts.

For information about configuring policies, see the *Symantec Data Insight Administrator's Guide*.

Chapter 5

Viewing access information for files and folders

This chapter includes the following topics:

- About viewing file or folder summary
- Viewing the overview of a data repository
- Managing data custodian for paths
- Viewing the summary of user activity on a file or folder
- Viewing user activity on files or folders
- Viewing file and folder activity
- Viewing CIFS permissions on folders
- Viewing NFS permissions on folders
- Viewing SharePoint permissions for folders
- Viewing audit logs for files and folders
- About visualizing collaboration on a share

About viewing file or folder summary

From the **Workspace** tab of the Data Insight Management Console, you can view the detailed information about the access

You can navigate shares, site collections, files, and folders by navigating to the list-views of the **Data Sources** and **Shares** tiles. Use the **Go to** bar at the top of the content pane to type the full path that you want to open. Type the path in the format, `\\filer\share\path` in case of a CIFS path, `/filer/share/path` in case of NFS path and `http://<URL of the SharePoint site>` to search for a site.

Viewing the overview of a data repository

To view the attributes of a folder :

1. From the **Workspace** navigate to the **Data Sources** list-view.
2. Expand a filer or Web application to display a list of configured shares or site collection.
3. Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.
4. Click a folder. The **Summary** panel populates to display additional details.
5. Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

   By default, the **Overview** tab displays the following summary of the selected data repository:

   - The size of the data.
   - The access summary.
   - The list of assigned or inherited custodians.
   - The list of all the files contained in the folder.

6. Click the Export icon at the bottom of the **Files** panel to save the data to a `.csv` file.

   You can also assign a custodian for a path from the **Overview** page.

7. You can also assign a custodian for a path from the **Overview** page.

   See “Managing data custodian for paths” on page 46.

Managing data custodian for paths

You can assign one or more custodians for a given data location. You can perform the following tasks on the **Overview** tab for a Web application, site collection, filer, share, or folder:

- For a data resource, view all the data custodians assigned to it. You can view the inherited data custodians, explicitly assigned custodians, and the parent repository from which they are inherited.
- Add new custodians.
- Remove explicitly assigned custodians on the path.

Once a custodian is assigned on a path, the custodian tag is automatically inherited by all the child paths under the parent path Custodian assignment cannot be overridden by a child path. For example, when you assign a custodian at a filer level, the shares and folders on the filer inherit the custodian assignment. But, if you assign a custodian on any share on the file server, the assignment does not get assigned to its parent.

You can assign and delete a custodian on any level, except on files on the **Overview** page for the same.

To assign a custodian do the following:

1. From the **Workspace**, navigate to the **Data Sources** list-view.
2. Drill down to share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.
3. Click a folder. The **Summary** panel populates to display additional details.
4. Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

   By default, the **Overview** tab displays the a summary of the selected data repository.
5. To assign a specific user as a custodian for the path, click the Settings icon and, from the drop-down list select **Add Custodian** > **Select User**.
6. Enter the name of the user in the Search field. Select the appropriate user from the search results, and click **OK**.

   You can filter users by domain or by using attribute-based queries.
7. To assign a custodian based on user or group directory attributes, from the drop-down list **Select User/Group Attribute**.
8. To assign a custodian based on user or group attributes, click **User** or **Group** radio button or enter a user/group name in the search bar.

9 Select an attribute. All the users referred to by the attribute value are assigned as custodian.

If the attribute has multiple values, Data Insight does not allow granular assignment of only one of them.

For attribute based custodian assignment, Data Insight picks up attributes that point to other objects in the directory service. For example, managedBy.

10 You can assign an inferred owner on a path as the custodian for the path. On the **User Activity** > **Summary** tab, right-click an inferred data owner and click **Add as Custodian**.

11 Optionally, you can assign a user who actively accesses a data location as the custodian of that data location. On the **User Activity** > **Active Users** tab, right-click an active user from the list displayed on the page, and select **Add as Custodian**.

12 Optionally, you can choose custodian from a set of users who have permissions on the path. On the **Permissions** tab, right-click a user from the list displayed on the page, and select **Add as Custodian**.

13 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

14 Click the Email icon to email custodian assignment information from the **Overview** page of a data location to desired email recipients.

To delete a custodian do the following:

1 From the **Workspace**, navigate to the list-view of the **Data Sources** tile.

2 Drill down to share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

3 Click a folder. The **Summary** panel populates to display additional details. Click the profile arrow. The **Summary** panel expands to display the profile view.

4 On the **Overview** tab of a resource, you can view the list of custodians assigned or inherited for that path. You can delete custodian assignments for a path in the following two ways:

- Select the assigned custodian and click the delete icon.
- To explicitly remove all custodian assignments for a path, click the custodian icon and select **Remove all**.

Note: You cannot delete assignments that have been inherited from parent paths. You must navigate to the parent location and delete the assignment from Overview page of the level at which the assignment was made.

A Data Insight administrator can assign custodians to multiple paths simultaneously by using the **Settings** > **Custodian Manager** option. For more information, see the *Symantec Data Insight Administrator's Guide*.

Viewing the summary of user activity on a file or folder

To view the summary of user activity on a file or folder

1. From the **Workspace** tab, navigate to the **Data Sources** list-view.
2. Expand a filer or Web application to display a list of configured shares or site collection.
3. Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.
4. Click a folder. The **Summary** panel populates to display additional details.
5. Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.
6. By default, the **Overview** tab displays the a summary of the selected data repository.
7. Click **User Activity**.
8. By default, the **Summary** sub-tab displays the following attributes of the folder for the last six months from the current date:
   - The user who created the file or folder.
   - The user who last modified the file or folder
   - The inferred data owner.
   - The last access date.
   - The total access count of the inferred data owner, including the number of read events and write events.
   - A graphical view of the total access count for the top five users of the selected file or folder.
     Click on a section of the pie-chart to view the detailed audit logs for a user.
     See “About audit logs” on page 17.
     See “Viewing audit logs for files and folders ” on page 56.
   - A tabular view of the access pattern of the top five users of the selected file or folder.
9. To view the summary of the user activity for the folder for a specific time period, enter the start and end dates in the **To** and **From** fields, and click **Go**.

Viewing user activity on files or folders

You can view the summary of access information, the access details of all users of a file or folder, and details of inactive users on the list-view of the **User** tile.

To view user activity on a file or folder

1. From the **Workspace** navigate to the **Data Sources** list-view.
2. Expand a filer or Web application to display a list of configured shares or site collection.
3. Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.
4. Click a folder. The **Summary** panel populates to display additional details.
5. Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

   By default, the **Overview** tab displays the a summary of the selected data repository.
6. Click **User Activity**.
7. By default, the **Summary** sub-tab displays the following attributes of a selected path for the last six months from the current date:
   - The user who created the file or folder.
   - The user who last modified the file or folder.
   - The inferred data owner.
     If a global data owner policy is defined, the data owner is inferred based on the criteria selected in the policy. For more information on defining the data owner policy, see the *Symantec Data Insight Administrator's Guide*.
     You can also assign an inferred data owner as custodian for that location.
     See "Assigning an inferred data owner as custodian" on page 51.
   - The last access date.
   - The total access count of the inferred data owner, including the number of read events and write events.
   - A graphical view of the total access count for the top five users of the selected file or folder.
     Click on a section of the pie-chart to view the detailed audit logs for a user.
     See "About audit logs" on page 17.
     See "Viewing audit logs for files and folders " on page 56.
   - A tabular view of the access pattern of the top five users of the selected file or folder.

8 Click the **Active Users** sub-tab to display the list of users who have accessed the file or folder.

The screen also provides details of the total access count for each user and gives a break-up of the read and write accesses by the users on the file or folder for the last six months. A legend describes the color-code used to depict the count of the read, write, and other accesses for each user.

You can also assign an active user as custodian.

See "Assigning an active user as custodian" on page 52.

9 To view the user activity for the folder for a specific time period, enter the start and end dates in the **From** and **To** fields, and click **Go**. The system displays the access count for that period.

10 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

11 Click **Inactive Users** to display a list of users who have access permission to the selected file or folder, but have not accessed it for the last six months.

12 To view a list of inactive users for a specific time period, enter the start and end dates in **From** and **To** fields, and click **Go**. The system displays the list of inactive users for that period.

13 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

Assigning an inferred data owner as custodian

You can assign an inferred owner on a path as the custodian for the path.

To assign a custodian

1 From the **Workspace** navigate to **Data Sources** the list-view.

2 Expand a filer or Web application to display a list of configured shares or site collection.

3 Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

4 Click a folder. The **Summary** panel populates to display additional details.

5 Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

By default, the **Overview** tab displays the a summary of the selected data repository.

6 Click the **User Activity** tab.

7 Click the **Summary** sub-tab to display the inferred data owner.

8 Right-click the inferred data owner, and select **Add as Custodian**. For assigning a custodian, See "Managing data custodian for paths" on page 46.

Assigning an active user as custodian

You can assign an active user as a custodian for a path from the **User Activity** page.

To assign an active user as a custodian

1 On the **Workspace** navigate to the **Data Sources** list-view.

2 Expand a filer or Web application to display a list of configured shares or site collection.

3 Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

4 Click a folder. The **Summary** panel populates to display additional details.

5 Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

By default, the **Overview** tab displays the a summary of the selected data repository.

6 Click **User Activity** tab.

7 Click the **Active Users** sub-tab to display a list of active users.

8 From the list displayed, right-click the user you want to assign as a custodian and select **Add as Custodian**.

9 Click the **Overview** tab for the path to verify whether the user is added to the list of custodians for that path.

See "Managing data custodian for paths" on page 46.

Assigning a custodian from the Permissions tab

You can assign a user who has the highest access permissions on a path as the custodian for the path.

To assign a custodian

1 From the **Workspace** navigate to the list-view **Data Sources**.

2 Expand a filer or Web application to display a list of configured shares or site collection.

3 Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

4 Click a folder. The **Summary** panel populates to display additional details.

5 Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

By default, the **Overview** tab displays the a summary of the selected data repository.

6 Click **Permissions** tab.

7 Right-click a user from the list displayed on the page, and select **Add as Custodian**.

See "Managing data custodian for paths" on page 46.

Viewing file and folder activity

The **Folder Activity / File Activity** tab displays activity on the selected file or folder by time. For a folder, it also shows sub-folder activity statistics and a list of subfolders which have not been accessed at all during a specified period.

To view activity on a file or folder

1 From the **Workspace** navigate to the **Data Sources** list-view.

2 Expand a filer or Web application to display a list of configured shares or site collection.

3 Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

4 Click a folder. The **Summary** panel populates to display additional details.

5 Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

By default, the **Overview** tab displays the a summary of the selected data repository.

6 Click **File Activity** or **Folder Activity** .

7 Data Insight displays the activity details for each of the following criteria:

- **By Time** - Click this sub-tab to view the number of Read, Write and Other accesses on the selected file or folder for a specified time period. You can also view a graphical representation of the access counts during each month in a specified time range.

- **By Subfolders and Files** - Click this sub-tab to view the Read, Write, and Other accesses as well as the total number of accesses, during a specified time on the sub-folders and files contained in the selected folder. The total access count includes the accesses on the current folder. This sub-tab is available only for folders.
- **Inactive Subfolders** - Click this sub-tab to view the details of the sub-folders contained in the selected folder that have not been accessed during a specified time period.

  You can use Symantec Enterprise Vault™ to archive the folders listed on the Inactive Subfolders tab directly from the Data Insight Management Console. This sub-tab is available only for folders.

  See “Managing inactive data from the Folder Activity tab” on page 76.

8 You can also write scripts to define actions to manage the inactive folders listed on the sub-tab. Click the Actions icon at the bottom of the tree-view pane, and select the appropriate script to apply the custom action on the folders listed on the **Inactive Subfolders** sub-tab.

  For more information about using custom scripts to manage inactive data, see the *Symantec Data Insight Administrator's Guide*.

9 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

Viewing CIFS permissions on folders

You can view the details of effective permissions, Access Control List for folders, and the share-level permissions on folders on the **Permissions** tab.

To view the permissions on folders

1 From the **Workspace** navigate to the **Data Sources** list view.

2 Expand a filer or Web application to display a list of configured shares or site collection.

3 Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

4 Click a folder. The **Summary** panel populates to display additional details.

5 Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

  By default, the **Overview** tab displays the a summary of the selected data repository.

6. Click **Permissions**. Or right-click the folder and select **Permissions**.

   Data Insight displays a list of users and groups and details of permissions associated with them for the selected folder. By default, Data Insight displays the effective permissions for various users and groups on that folder.

   If a user group has permissions on the folder, you can also view the details of the number of users who are direct members of the group, or have inherited the membership of the group from a parent group

7. Click the **Include share level permissions** check box to include share-level permissions when computing effective permissions.
8. Click **File System Access Control List** to view a list of all the users or groups, who have an Access Control Entry (ACE) defined on that folder. The ACE can be inherited or explicitly defined.
9. Click **Share-level permissions** to view a user's or a group's share-level permissions.
10. Click **Advanced permissions**, in each sub-tab, to view the details of the operation that a user or a group is allowed or denied on that folder.
11. Click the **Export** icon at the bottom of the page to save the data to a `.csv` file.

See "About permissions " on page 15.

Viewing NFS permissions on folders

You can view the details of NFS permissions on the **Permissions** tab.

To view the permissions on folders

1. From the **Workspace** navigate to the **Data Sources** list view.
2. Expand a filer or Web application to display a list of configured shares or site collection.
3. Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.
4. Click a folder. The **Summary** panel populates to display additional details.

5 Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

By default, the **Overview** tab displays the a summary of the selected data repository.

6 Click **Permissions**.

Data Insight displays a list of users and user groups and details of the NFS permissions associated with them.

Viewing SharePoint permissions for folders

You can view the details of SharePoint permissions on the **Permissions** tab.

To view SharePoint permissions

1 From the **Workspace** navigate to the**Data Sources** list-view.

2 Expand a filer or Web application to display a list of configured shares or site collection.

3 Expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

4 Click a folder. The **Summary** panel populates to display additional details.

5 Click the profile arrow on the **Summary** panel to display the underlying folder-centric views.

By default, the **Overview** tab displays the a summary of the selected data repository.

6 Navigate to the path for which you want to view the permission details.

7 Click **Permissions**.

A summary of the users and the roles assigned to them appears. The roles include the tasks that a user is allowed to perform.

8 Select a role assigned to a user to view all the permissions assigned to that particular role.

Viewing audit logs for files and folders

Note: By default, Data Insight displays the activity logs for a selected file or folder for the last six months from the current date.

To view audit logs for files and folders

1. From the **Workspace** navigate to the **Data Sources** list-view.

   See “About viewing file or folder summary” on page 45.

2. Expand a filer or Web application to display a list of configured shares or site collections. Or expand a share or site collection to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.

3. Click a folder. The **Summary** panel populates to display additional details.

4. Click**Expand Profile** on the **Summary** panel to display the underlying folder-centric views.

   By default, the **Overview** tab displays the a summary of the selected data repository.

5. Click **Audit Logs**. Or right-click the file or folder and select **Audit Logs**.

6. Apply the time filter for which you want to view the user activity on a specific file or folder.

7. Select **Include sub-folders**, if you want to view activity logs for the subfolders that are contained in the selected folder.

8. Click **Go**.

   The Access Pattern Map appears, which provides details about the users who have accessed that file or folder and the count of read and write user events on it. The option **Include events on files before rename** includes all events, including those before the Rename audit event was received for the file.

9. The audit logs provide the following information:

   - The name of the user who generated the event.
     In case of an Permission Change event, Data Insight displays the name of a fictitious user. You can view the details of the event in the **Other Info** column, however the name of the user is displayed as _DI_PERMCHG_DUMMY_USER_.
     See “About audit logs” on page 17.

   - The name of the file that is accessed.

   - The path of the file.

   - The type of access event.
     In case of a folder on a SharePoint site, the SharePoint access type such as checkout, view, check in, write, update, delete, and move to Data Insight meta access types - Read, Write, Create, Delete, and Rename.

Permission Change events are represented by the access type - PERMCHANGE.

- The type of file
- The access count
- The IP address of the computer from which the file was accessed.
  Currently, you cannot view the IP address of the computer from which the file was accessed for Windows File Servers, VxFS filers, and SharePoint sites.
  In case of an Permission Change event, the IP address is displayed as 0.0.0.0.
- The start and end time for the time window in which the event occurred.

10 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

11 Click the drop-down arrow on any column header and select **Columns**. Then, select the parameters you want to show or hide in the Access Pattern table.

To filter the audit logs

1 To further filter the logs, do one of the following:

- Select adjacent cells in the Access Pattern Map, right-click, and select **View Audit Logs**.
- To view all accesses for the day, click on the column header of the Access Pattern Map.
- To view all accesses of a user, click on the row header of that user.

You can control-click to select multiple adjacent cells in the Access Pattern Map.

2 You can choose to filter the audit logs further using one or all of the following criteria:

- The period for which you want to view the audit logs.
- The start and the end date for which you want to view events.
- The type of access.
  Data Insight maps all SharePoint access types such as checkout, view, check in, write, update, delete, and move to Data Insight meta access types - Read, Write, Create, Delete, and Rename.
  You can enter multiple comma-separated values.

3 Enter the filter criteria in the relevant fields and click **Go**.

About visualizing collaboration on a share

To understand the collaboration of users on a share, Data Insight provides a collaboration graph that helps you visualize how a set of users and individual users are collaborating on a share. Data Insight identifies a share as collaborative, if a significant number of users access or change the same or different files directly under a folder within a given time period. For example, if User A creates, reads, modifies, and renames `abc.txt` under `\\g\s\a\b\foo` and User B modifies `xyz.txt` under `\\g\s\a\b\foo`, then User A and User B are said to be collaborating. Share \\g\s is considered as a collaborative share.

The time period for analyzing collaborative activity on a share is configured on the **Settings** > **Advanced Analytics** page. For more information, see *Symantec Data Insight Administrator's Guide*.

The Social Network Map graph provides you with a global picture of collaborative behavior among users based on their activity on the selected share. It also helps you visualize the various organizational units that may be collaborating on a share. It enables you to identify users who are working closely together or users who stand out because their activity patten is less collaborative as compared to users who are actively collaborating among themselves. Collaborating users are grouped together in clusters and connecting lines are used to show collaboration between the users. Users that are connected with a dense network of lines indicate a high level of collaboration between them. While the users that are loosely connected show low or weak collaboration.

The Social Network Map groups users in clusters based on their collaboration and each cluster has a different color-code. The users in a cluster are classified on the basis of certain attributes. For more information about configuring user attributes, see the *Symantec Data Insight Administrator's Guide*.

You can use the Social Network Map tool to visualize collaboration per share, and not across your entire storage environment.

You can use the Social Network Map to do the following:

- Analyze the activity pattern among users and groups and identify the level of collaboration on a share.
- Identify the pattern of collaboration between different cluster groups.
- Collaborative activity on a share.
- Identify weakly-connected users who are not collaborating within a folder, but have activity on the share.
- Visualize the various organizational units that may be collaborating on a share.

- Identify and analyze outlier users based on organizational units and other attributes.
- Export the graph along with information about user attributes and degree of collaboration to an output file.

Analyzing activity on collaborative shares

Use the Social Network Map graph to analyze collaboration of users within a folder on a share.

Viewing the pattern of collaboration on a share

1. From the **Workspace** tab of the Management Console, navigate to the list-view of the **Data Source** tile.
2. On the list-view page, select the share for which you want to view the collaboration graph. The summary panel at the right hand side populates with additional details about the share.
3. Click the profile arrow to view the profile of the share.

   The **Overview** tab displays by default.
4. Click **Social Network Map**. Or right-click the share, and select **Social Network Map**.

   Data Insight displays a visual representation of the users accessing the share. Edges connect users collaborating on folders within the share during the given time period. The users are grouped into clusters based the collaborative activity on the share. The cluster groups are also color-coded such that collaborating users have the same color.

   The graph displays the collaboration of the users within their cluster and also across all cluster groups that are represented in the graph.
5. Information on the right-hand panel helps you analyze the Social Network Map in detail. Also, the selections that you make here are summarized in the top panel.

   Click **Summary**. The Summary panel displays the following details:

   - The number of active users collaborating on the share
   - The number of sensitive files on the share
   - The number of weakly-connected users, if any
   - The list of cluster groups in the graph
   - The primary attribute that is configured for users in each cluster group, and the number of users for each attribute value.

6 Click a cluster group to view the top folders under which the users in the cluster are collaboraitng. You can also view the number of users for each attribute value in the cluster group.

7 Click **Outlier Analysis** to view the distribution graph which shows the distribution of connections within a cluster per user. You can also render the graph to view the number of users with a given range of connections within a cluster or across clusters.

From the drop-down, select **Total**, **Within Cluster**, or **Cross Cluster**, and enter the range of connections. For example, you can highlight users in the graph that have 5 to 7 connections within a cluster group.

8 To further analyze the data, do the following:

- Select a cluster group to highlight it in the Social Network Map.
- Select one or more attribute values to highlight users with the selected attributes in the cluster.
- Or, select a cluster and one or more attributes to highlight users within the selected cluster.

Note: If you select different values across different filter criteria, the filters are applied together. Whereas, the filters are evaluated serially, if you select the multiple values within a filter criteria.

9 Click **Exclusions** to filter the map to view the collaborative activity of only the users with the attribute values that you are interested in. The panel displays a list of configured attributes for users in all the cluster groups that are represented in the map.

10 Uncheck the attributes that you are not interested in. Data Insight renders the graph again by eliminating the users with the selected attributes values.

You can also choose to exclude attribute values when rendering maps for large social networks.

11 Mouse-over or click a user in the graph to view the attributes configured for the user. The pop-up also displays the details of the connections that the user has within the cluster group and with users in other cluster groups

Click **View Audit Logs** to view the activity for the selected user.

12 Click the Export icons to export the data that is represented by the Social Network Map in a `.csv` file.

Viewing access information for users and user groups

This chapter includes the following topics:

- Viewing the overview of a user
- Viewing the overview of a group
- Managing custodian assignments for users
- Viewing folder activity by users
- Viewing CIFS permissions for users
- Viewing CIFS permissions for user groups
- Viewing NFS permissions for users and user groups
- Viewing SharePoint permissions for users and user groups
- Viewing audit logs for users

Viewing the overview of a user

To view the attributes of a user

1. From the drop-down menu on the **Workspace** tab, select **Users**.
2. On the Groups list view page, select a user. The **Summary** panel populates to display additional details.

3 Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

4 By default, the **Overview** tab displays the following summary of the selected user:

- The list of all the groups of which the user is a member.
  You can view the groups of which the user is a primary member and the groups in which the user has inherited the membership. The differentiation between direct and indirect group membership enables you to make relevant permissions changes.
  For information about making permission changes, see the *Symantec Data Insight Administrator's Guide*.
- The directory domain attributes of the user.

5 Click **Export** to export the information on the page to a `.csv` file.

6 You can also assign or delete custodian assignments from the **Overview** tab.

See "Managing custodian assignments for users " on page 64.

Viewing the overview of a group

To view the attributes of a user group

1 From the drop-down menu on the **Workspace** tab, select **Groups**.

2 On the **Groups** list view page, select a group. The **Summary** panel populates to display additional details about the group.

3 Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

4 By default, the **Overview** tab displays the following summary of the selected group:

- The directory attributes of the group.
- A list of the other groups of which the selected group is a member. The view also displays the differentiation between the selected group's direct and indirect membership of other groups.

- A list of the members in the group.

5 Click an icon to do the following:

☒	Exports all data on the screen to a `.csv` file.
☒	Exports the data on a panel on the screen to a `.csv` file.
☒	Delete a group from another group of which it is a direct member. For information about making permission changes, see the *Symantec Data Insight Administrator's Guide*.

Managing custodian assignments for users

The **Custodian** tab of a user provides you with a single interface to the following information:

- View all the custodian locations assigned to the custodian.
- Assign new locations to the custodian.
- View the filtered list of the parent data locations under which the user has custodian assignments.
- Remove data locations assigned to the user.

To assign a custodian location do the following:

1 On the **Workspace** tab, navigate to the **Users** list-view.

2 Click a user. The **Summary** panel populates to display additional details.

3 Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

By default, the **Overview** tab displays a summary of the selected user

4 Click the **Custodian** tab. The page displays the filtered list of the parent data locations under which the user has custodian assignments. For example, if the user is assigned as a custodian on the shares on the filers in a domain, the filtered list of only those filers is displayed.

5 Click the data location. The **Assignments** panel on the right displays whether the user has assignments on any of the children paths under that data location.

6 You can drill down the **Physical** or **DFS** hierarchy to view the children data locations for which the user is a custodian.

7 To assign the user as the custodian for a particular path, click the Custodian icon and select **Add Location**.

8 Select the **Physical** or **DFS** radio button.

9 Select the location, and click **OK**.

10 To view a list of all the data locations in a domain on which the user is a custodian, click the **View All Assignments** button. A list of all the paths for which the user is a custodian is displayed.

To remove all custodian locations

1 On the **Custodian** tab, click the data custodian icon and select **Remove All**.

2 Click **Yes** on the confirmation message.

Note: This option removes all the assigned custodian locations for the user.

To view/export custodian information for a user

1 To view a list of all the data locations in an enterprise on which the user is a custodian, click the Custodian icon, and select **View All Assignments**. A list of all the paths for which the user is a custodian is displayed.

2 Click the Email icon to email custodian assignment information to desired email recipients.

3 Click the Export icon at the bottom of the page to export the data on the screen to a `.csv` file.

Viewing folder activity by users

You can view the access details of the selected user during a specified time or details of folders accessed by the selected user on the **Activity** tab.

To view user activity on a file or folder

1 From the **Workspace**, navigate to the **Users** list-view.

2 Click a user. The **Summary** panel populates to display additional details.

3 Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

By default, the **Overview** tab displays the a summary of the selected user.

4 Click **Activity**. Or right-click the user in the navigation pane and select **Activity**.

5 Use the device filter in the content pane to search for specific devices where selected user has activity. The **Devices with activity** filter is applied by default. The filter pane displays the list of filers or web applications that have some shares or site collections on which the selected user has activity.

Or, click the drop-down to select a specific type of storage device, disabled filers or web applications, or devices.

At the share-level in the hierarchy, you can also filter the paths using other predefined filters, such as disabled shares or site collections where the user has activity.

6 Click the **By Time** sub-tab to view the activity details of the user for a specific time period on the selected share.

7 Enter the start and end dates in the **From** and **To** field.

8 Select the share for which you want to view the user's activity, and click **Go**.

The number of Read, Write, Other, and the total number of accesses by the selected user, on the selected share, during the specified time period appears. The page also displays a graphical representation of the access counts during each month in the specified time range.

9 Click the **By Folders** sub-tab to view the following:

- The folders accessed by the selected user during a specified time period.
- The number of Read, Write, Other, and the total number of accesses by the user on these folders during a specified time period.

10 Enter the start and end dates in the **From** and **To** field, and click **Go**.

The list of all the shares accessed by the user during the specified date range appears. Expand a share to view the list of folders accessed by the selected user.

Viewing CIFS permissions for users

You can view details of the effective permissions as well as the access control entries for a user on the **Permissions** tab.

See “About permissions ” on page 15.

Note: Only the shares which have one or more access control entries related to the selected user, or has any permission entry given to the special group *Everyone* are available for selection on the **Permissions** tab.

To view the permissions assigned to a user

1. On the **Workspace** tab, navigate to the **Users** list-view.
2. Click a user. The **Summary** panel populates to display additional details.
3. Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

   By default, the **Overview** tab displays the a summary of the selected user.
4. Click **Permissions**. Or right-click the user in the navigation pane and select **Permissions**.
5. Use the device filter in the content pane to search for specific devices where selected user has permissions. The **Devices with permission** filter is applied by default. The filter pane displays the list of filers or web applications that have some shares or site collections on which the selected user has permissions.

   Or, click the drop-down to select a specific type of storage device, disabled filers or web applications, or devices.

   At the share-level in the hierarchy, you can also filter the paths using other predefined filters, such as disabled shares or site collections where the user has permissions.

   A summary of the permissions that are assigned to the user on the selected share appears. It includes the following details:

   - The path at which the access control entry has been defined for the user or the group to which the user belongs.
   - The type of permissions.
   - The groups from which the user inherits the permissions.
6. Click **Effective Permissions** to view the list of all the folders, on the selected share, on which the user has effective permissions.

   You can drill down the folder structure to view the permissions that are assigned to the subfolders
7. Click **Advanced permissions** icon in each view to view the details of the operation that a user is allowed or denied on a given path.
8. Click **Share-level permissions** to view a user's share-level permissions on a selected share.
9. Click the Export icon at the bottom of the page to save the data to a `.csv` file.

Viewing CIFS permissions for user groups

You can view details of the effective permissions as well as the access control entries for a user group on the **Permissions** tab.

See “About permissions ” on page 15.

To view the permission assigned to a user group

1. In the **Workspace** tab, navigate to the **Groups** list-view.
2. Click a group. The **Summary** panel populates to display additional details.
3. Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.
4. By default, the **Overview** tab displays the a summary of the selected group:
5. Click **Permissions**. Or right-click the user group in the navigation pane and select **Permissions**.
6. Use the device filter in the content pane to search for specific devices where selected group has permissions. The **Devices with permission** filter is applied by default. The filter pane displays the list of filers or web applications that have some shares or site collections on which the selected group has permissions.

   Click in the **Select Share** field, and from the **Select Resource** pop-up, select the path on which you want to view the group's permissions.
7. Use the device filter in the content pane to search for specific devices where selected group has permissions. Click the drop-down to select a specific type of storage device, disabled filers or web applications, or devices where the group has permissions.

   At the share-level in the heirarchy, you can also filter the paths using other pre-defined filters, such as disabled share or site collections.
8. A summary of the permissions assigned to the user on the selected share appears. It includes the following details:
   - The path at which the access control entry has been defined for the group.
   - The type of permissions.
   - The higher-level group from which the group inherits the permissions.
9. Click **Effective Permissions** to view the list of all the folders, on the selected share, on which the group has effective permissions.
10. Click **Advanced permissions** icon to view the details of the operation that a group is allowed or denied on a given path.

11 Click **Share-level permissions** to view a group's share-level permissions on a selected share.

12 Click the Export icon at the bottom of the page to save the data to a `.csv` file.

Viewing NFS permissions for users and user groups

You can view details of the NFS permissions for users and user groups on the tab.

To view the permissions assigned to a user or user group

1 On the **Workspace** tab, navigate to the **Users** or **Groups** list-view , as the case may be.

2 Select the user or user group for whom you want to view the permissions.

3 Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

4 Click **Permissions**. Or right-click the user in the navigation pane and select **Permissions**.

Data Insight displays the list of resources in a pane and when you select an NFS resource from the list of resources, you'll see the permissions that the user/group has on the subfolders/files within the NFS resource.

5 To view the source of the permissions for a particular user or user group, click the **Inherited From** button.

A pop-up window opens which highlights the source of the applicable permissions.

6 Click the **Select Share** field, and from the **Select Resource** pop-up, select the path on which you want to view the group's permissions, and click **OK**.

Viewing SharePoint permissions for users and user groups

You can view details of the SharePoint permissions for a user on the **Permissions** tab.

To view the SharePoint permissions assigned to a user

1 On the **Workspace** tab, navigate to the **Users** list-view.

2 Click a user. The **Summary** panel populates to display additional details.

3. Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

   By default, the **Overview** tab displays a summary of the selected user

4. Click **Permissions**. Or right-click the user in the navigation pane, and select **Permissions**.

5. Enter the URL of the site in the **Select Share or Site Collection** field and click **GO**. Or click the search icon and from the **Select Resource** widget select a URL and click **OK**. A pop-up displays the list of children of the selected. It also displays the roles for the selected users.

   Use the device filter in the content pane to search for specific devices where selected user has permissions. The **Devices with permission** filter is applied by default. The filter pane displays the list of filers or web applications that have some shares or site collections on which the selected user has permissions.

   Or, click the drop-down to select a specific type of storage device, disabled filers or web applications, or devices where the user has permissions.

   At the share-level in the hierarchy, you can also filter the paths using other predefined filters, such as disabled share or site collections where the user has permissions.

6. A summary of the permissions that are assigned to the user on the selected site collection appears. It includes the following details:

   - The path at which the access control entry has been defined for the user or the group to which the user belongs.
   - The type of role.
   - Unique permissions defined on:

     ☒ The folder and its descendants.

     ☒ The descendants.

     ☒ The folder.

7. Select a role that is assigned to a path to view all permissions included in that role.

Viewing audit logs for users

You can view audit logs of the access details for a particular user in a given time period.

See “About audit logs” on page 17.

To view the audit logs for users:

1. From the **Workspace**, navigate to the **Users** list-view.
2. Click a user. The **Summary** panel populates to display additional details.
3. Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.

   By default, the **Overview** tab displays the a summary of the selected user.
4. Click **Audit Logs**. Or right-click the user, and select **Audit Logs**.
5. Apply the time filter for which you want to view the selected user's activity. By default, Data Insight displays the audit logs for the last six months from the current date.
6. Select the share for which you want to view the activity by the selected user.

   Use the device filter in the content pane to search for specific devices where selected group has permissions. The **Devices with activity** filter is applied by default. The filter pane displays the list of filers or web applications that have some shares or site collections on which the selected user has activity.

   At the share-level in the hierarchy, you can also filter the paths using other predefined filters, such as disabled share or site collections where the user has activity.
7. Enter the start and the end dates in the **To** and **From** field.

   Additionally, you can also filter the audit logs based on the following criteria:

   - The IP address of the computer that the user has generated the access activity from.
   - The type of access for which you want to view audit logs. For SharePoint web applications, you can specify either access type (meta operations, such as Read, Write, Delete, Create, and Rename) or access details (SharePoint operations).
     Data Insight maps all SharePoint access types such as checkout, view, check in, write, update, delete, and move to Data Insight meta access types - Read, Write, Delete, and Rename.
     You can enter multiple values separated by commas. Enter the filter criteria in the relevant fields and click **Go**.

8. Click on a folder to see the user's activity on that folder.
9. The audit logs provide the following information:
   - The name of the file that is accessed.
   - The path of the file.
   - The type of access event.

     In case of a folder on a SharePoint site, the SharePoint access type such as checkout, view, check in, write, or update.
   - The type of file.
   - The access count.
   - The IP address of the computer from which the file was accessed.

     Currently, you cannot view the IP address of the computer from which the file was accessed for Windows File Servers, VxFS filers, and SharePoint sites.
   - The start and the end time of the access events.
10. Click the drop-down arrow on any column header and select Columns. Then select the parameters you want to show.

Chapter 7

Managing inactive data

This chapter includes the following topics:

- About managing data using Enterprise Vault and custom scripts
- About Retention categories
- About post-processing actions
- Managing data from the Shares list view
- Managing inactive data from the Folder Activity tab
- Managing inactive data by using a report

About managing data using Enterprise Vault and custom scripts

You can initiate a data management operation for the following :

- The files that are listed under **Workspace** > **Folders** > **Folder Activity** > **Inactive Subfolders** sub tab.
  See "Managing inactive data from the Folder Activity tab" on page 76.
- The files that appear inside the following types reports:
  - **Access Details** reports
  - **Access Summary** reports
  - **DQL** reports
  - **Data Lifecycle** reports

  See "Managing inactive data by using a report" on page 77.

Note: Data Insight supports archiving the files on CIFS shares.

You can view the status of the data management operations on the **Settings** > **Action Status** page of the Data Insight Management Console.

For more information on how to track an operation, see the *Symantec Data Insight Administrator's Guide.*

You can perform the following actions for the archived items:

- Specify a retention category on the archived data to indicate how long the data must be stored.
  See "About Retention categories" on page 74.
- Specify a post-processing action to indicate how the original file is handled after the archive operation is complete. You can either retain the original file and choose to delete it once the archive operation is complete or create a placeholder shortcut for the file after archiving is complete.
  See "About post-processing actions" on page 75.

About Retention categories

Retention categories determine how long the archived data is stored in Enterprise vault, before it is allowed to be deleted from the storage device. You can categorize the stored data into various groups by assigning them a retention category. This categorization makes it easier to retrieve archived items because it is possible to search by category.

You can assign a retention category to the archived data based on parameters such as business value and sensitivity etc. For example, typically user generated personal data has less business value than the data that is owned by the Sales department. You might want to store personal data for six months and the Sales data for five years. In such a scenario you can define two retention categories for each of these two types of data. For each retention category, you can define a retention policy, to indicate the minimum storage period for the data belonging to that retention category.

From the Data Insight Management Console, you can choose only those retention categories which are defined in the Enterprise Vault. To define a new retention category, you must have access to Enterprise Vault Administration Console. Data Insight automatically fetches the retention categories from the Enterprise Vault server at a scheduled interval and displays them as available options in the Management console. The default interval for fetching retention categories is one hour.

To know more about retention categories and how to define them, see the *Symantec Enterprise Vault Administrator's Guide*.

See “About managing data using Enterprise Vault and custom scripts ” on page 73.

About post-processing actions

Post-processing actions enable you to specify what is to be done with the original file, once the archiving operation is complete. You can choose from the following options:

- **Delete File**: Enterprise Vault archives the file and deletes the original file.
- **Create Shortcut**: Enterprise Vault archives the file and deletes the original file and replaces it with a shortcut for the archived file. After the archiving operation is complete, you should see a different icon for the files that have been archived.
- **None**: Enterprise Vault archives the file, but retains the original file. Neither a shortcut is created for the file, nor is the file deleted.

Enterprise Vault performs a post-processing action only after the archive operation is successfully processed. If an archive operation fails, post-processing actions are not performed.

See “About managing data using Enterprise Vault and custom scripts ” on page 73.

Managing data from the Shares list view

You can perform any data management action on the folders which are on the Context Map view of the Data Insight Management Console.

To manage data from the Shares list view

1. In the Management Console, click the **Workspace** tab.
2. Navigate to the **Shares** list view.

   Shares list view displays for all configured shares or site collections. You can drill down the folder hierarchy to select the path for which you want to archive or otherwise manage the data using custom scripts.
3. Select the check boxes for the paths that you want to manage.
4. From the **Actions** drop-down, select one of the following:
   - **Archive** - Click to archive the folder(s) using Symantec Enterprise Vault.
   - **Custom Action** - Click to execute a custom action.

Note: The name of the **Custom Action** icon appears as defined in the configuration for the custom action. Up to two custom actions can be configured for data management actions like deleting data, or archiving data. For more information on configuring a custom action, refer to the *Symantec Data Insight Administrator's Guide*.

5. If you click the **Archive** icon, the **Archive Files** dialog displays. Select the following options:
   - **Retention Policy**: Select an option to indicate how long the archived data has to be stored, before it is allowed to be deleted.

     Post Processing Action: Select an option to indicate how to handle the source data, after the archive operation is complete.
6. Click **Archive**.
7. If you click the **Custom Action** icon, the **Confirm Custom Action Execution** dialog displays. Click **Yes**.

You can view the status of the archiving operation on the **Settings** > **Action Status** page.

Managing inactive data from the Folder Activity tab

You can perform any data management action on the folders which are listed as **Inactive subfolders**.

To manage inactive subfolders:

1. Click the **Workspace** tab.
2. Navigate to the folder where inactive folders are present. By default, the **Overview** tab displays a summary of the folder including details of the files in the folder.
3. Click **Folder Activity**. Or right-click the file or folder in the navigation pane, and select **Folder Activity**. By default, Data Insight displays the time-wise activity details of the selected folder.
4. Click **Inactive Subfolders**. You can view the details of the subfolders that have not been accessed during a specified time period. The default duration is set for **Last 6 Months**.You can use the **Time Filter** to customize the time duration for which you want to see the inactive subfolders.
5. Select the check box for the subfolder(s) that you want to manage.
6. Click the action selector icon at the bottom of the tree-view pane. A menu appears with the following icons:

- **Archive** - Click to archive the folder(s) using Symantec Enterprise Vault.
- **Custom Action** - Click to execute a custom action.

Note: The name of the **Custom Action** icon appears as defined in the configuration for the custom action. Up to two custom actions can be configured for data management actions like deleting data, or archiving data. For more information on configuring a custom action, refer to the *Symantec Data Insight Administrator's Guide*.

7 If you click the **Archive** icon, the **Archive Files** dialog displays. Select the following options:

- **Retention Category**: Select an option to indicate how long the archived data has to be stored, before it is allowed to be deleted.
- **Post Processing Action**: Select an option to indicate how to handle the source data, after the archive operation is complete.

Click **Archive**.

8 If you click the **Custom Action** icon, the **Confirm Custom Action Execution** dialog displays. Click **Yes**.

Note: You can view the status of the archiving operation on the **Settings** > **Action Status** page.

Managing inactive data by using a report

You can perform any data management action on the files that appear in the following types of reports:

- Access Details reports
- Access Summary reports
- DQL reports
- Data Lifecycle reports

To manage data by using a report:

1 Click the **Reports** tab. The reports home page displays by default.

2 Select a report type from the left-hand side navigation pane. For example, you might select a *Access Details for Paths* report. A new tab opens displaying all the recently generated reports of that type.

3 Identify the report you want to use. Review the report to verify that the files that you want to archive are listed along with their paths.

4 From the **Select Action** drop-down, click **Actions**. A drop-down menu appears with the following options:

- **Archive** - Click to archive the paths listed in the report using Symantec Enterprise Vault.
- **Custom Action** - Click to execute a custom action.

Note: The name of the **Custom Action** icon appears as defined in the configuration for the custom action. Up to two custom actions can be configured for data management actions like deleting data or archiving data. For more information on configuring a custom action, refer to the *Symantec Data Insight Administrator's Guide*

5 If you click the **Archive** icon, the **Archive File** dialog box displays. Provide the following information:

- **Retention Policy**: Select an option to indicate how long the archived data has to be stored, before it is allowed to be deleted.
- **Post Processing Action**: Select an option to indicate how to handle the source data, after the archive operation is complete.

Click **Archive**.

6 If you click the **Custom Action** icon, the **Confirm Custom Action Execution** dialog-box displays.

Note: You can view the status of the archiving operation on the **Settings** > **Action Status** page.

Chapter 8

Using the Self-Service Portal

This chapter includes the following topics:

- About the Self-Service Portal
- Logging in to the Self-Service Portal
- Using the Self-Service Portal to review user entitlements
- Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents
- Using the Self-Service Portal to confirm ownership of resources
- Using the Self-Service Portal to classify sensitive data

About the Self-Service Portal

Data Insight enables you to monitor the data on Network Attached Storage (NAS) and helps you to identify the data owner of files and folders based on the access history. It lets you carry out forensics in the form of various pre-canned and custom reports.

Data Insight also lets you manually tag users in your organization as being responsible for the resources in your storage environment. Such users are called custodians and are responsible for remediating these resources.

Data Insight integrates with Data Loss Prevention (DLP) to help security administrators and the information security teams in your organization to monitor and report on access to sensitive information. A Data Insight lookup plug-in retrieves information from the DLP Enforce Server about confidential information on the shares being monitored by Data Insight. DLP creates an incident for every file that violates configured DLP policies. The DLP Network Discover incident report lists such file system shares. The usage information that Data Insight collects automatically feeds into the incident detail of files that violate DLP policies. Data Insight identifies the data owners to notify about these incidents. This method enables users to identify sensitive data along with the responsible users to enable more efficient remediation and data management.

Data Insight also enables you to review permissions on files and folders and remediate excessive permissions. Analyzing the permissions on resources ensures that only users with the business need have access to the data.

Thus, Data Insight supports large-scale business owner-driven remediation processes and workflows. You can create workflows from the Data Insight Management Console, and submit these workflows for further action by selected custodians or configured data owners.

The Self-Service Portal provides you an interface to complete the remediation workflows. When you submit a workflow from the Data Insight console, on the start date of the workflow an email is sent to the custodians of the selected resources. The email includes a link to the Self-Service Portal. The custodians can then do the following tasks on the portal:

- Launch the portal using the link in the email, and log in to the portal with their Active Directory credentials.
- View the resources that need to be remediated.
- Apply configured actions on the resources that are assigned to them.
- Submit the requests for execution to the DLP Enforce Server, Symantec Enterprise Vault server, or the Data Insight Management Server, depending on the type of workflow request.

The files on which an action is submitted no longer appear on the portal. The summary of the total files awaiting remediation is also updated to show the number of remaining files. You can view the number of submitted files and the files on which an action is pending at the top-right corner of the page.

If you fail to take action on the paths that are submitted for your attention within the stipulated time, the workflow is canceled.

The Self-Service Portal is available beginning Symantec Data Insight version 4.5. You can use the portal for remediating incidents beginning Symantec Data Loss Prevention version 12.5.

Logging in to the Self-Service Portal

Custodians log in to the Self-Service Portal using the link in the email alert that they receive when a remediation workflow is submitted by a Data Insight or Data Loss Prevention administrator.

The link to the portal is valid only as long as paths in the workflow request are pending action by the custodians or until the end date specified in the workflow. Note that custodians cannot use the same link to log in to the portal after a workflow is complete, is cancelled for any reason, or if the custodian has taken action on all assigned paths.

In some cases, the Data Insight administrator may log in to the portal on your behalf. You will receive a notification alerting you that a Data Insight administrator has logged in to a workflow that is assigned to you. You can disable further notifications for a particular workflow. However, you will continue to receive reminder notifications for other workflows that are assigned you.

To log in to the Self-Service Portal

1. Click the link contained in the email alert.

   The portal login page appears. The **Username** field is pre-populated with the your network username.

2. Enter your network password, and click **Login**.

3. When you log in to the portal, you may be presented with a welcome message if it is so configured for the workflow.

   On the message, click **OK** to continue with remediation actions on paths submitted for your attention.

Using the Self-Service Portal to review user entitlements

You can use the Self-Service Portal to review user access permissions to the paths that are assigned to you. On the **Entitlement Review** page of the portal, you can perform the following tasks:

- View a snapshot of the users whose permissions are assigned for your review.
- Filter the users to be reviewed based on their activity profiles and the assigned paths. For example, you might be interested to first review the entitlements for the users who are inactive.
- Grant or revoke user permissions on the specified paths.

- You can also decline the review request or delegate the review work to another user.

To review user entitlements

1. Use the path filter drop-down to select the path for which you want to review the user permissions. From the drop-down list click the path for which you want to review user entitlements. All the review requests for the selected path are displayed on the panel.
2. Use the **Users by activity** filter to sort the users based on their activity profiles.
3. Do any of the following:
   - To review the permissions of individual users, click **Yes** to grant access to the path, and click **No** to revoke the user's access on the path
   - To review the permissions for multiple users, select the users based on the action you want to take. For example, select the users whose permissions you want to revoke on the selected path.
     Click either **Allow access** or **Revoke access** to grant or to decline the permissions on the selected group of users.

To decline or delegate entitlement review requests

1. Click the down-pointing arrow for the path filter. From the drop-down list select the paths using the check-boxes.
2. Do any of the following:
   - Click **Decline** to reject the request to review permissions on the selected path.
   - Click **Delegate** to delegate the entitlement review task to another user.

After you submit the review request from the portal, the details are sent to the Data Insight Management Server. The Data Insight administrator can view the paths for which custodians have suggested changes to the permissions, and can perform the relevant changes. Alternatively, Data Insight can automatically trigger a permission remediation action to distribute the actions to the proper authorities such as, directory server administrators.

To automatically initiate a permission remediation action, you must first configure the permission remediation settings. For more information, refer to *Symantec Data Insight Administrator's Guide*.

See “Logging in to the Self-Service Portal” on page 81.

Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents

You can use the Self-Service Portal to remediate incidents on the paths that are assigned to you. On the **DLP Incident Remediation** page of the portal, you can do following tasks:

- View a snapshot of the number of files that are assigned for your attention. The files are sorted according to the severity of incidents that are associated with them.
- Filter the list of files based on the severity of the incidents that the files have violated, the recency of the last access date, or the DLP policy that the files violate. The filters available to you depend on the options that are selected when configuring the workflow template.
  The different filters are applied together, and the list is filtered to show the data that matches the applied criteria.
- Perform a configured action on multiple files at one time. The available actions are DLP Smart Response rules configured in DLP. You can select more than one file from the list and then choose the desired action.

To remediate the files

1. Select the files that you want to remediate.

   You can choose to filter the list of files using the filter criteria at the top of the page. For example, you can prioritize the remediation of files that are associated with high severity incidents that violate a particular policy. Files that match the selected filter criteria are listed. Select the desired files from the list.

2. From the **Select Action** drop-down, select the action that you want to take on the selected files. For example, you may quarantine the files or mark the files for deletion. The listed actions are the Smart Response rules that are configured within DLP.

   For more information about Smart Response rules, see the *Symantec Data Loss Prevention Administration Guide*.

3. Click **Submit** to send the remediation request to the Data Insight Management Server for further action.

   On submission of the request, the actions that you select are sent to the Data Insight Management Server, which in turn requests the Response Rule Execution Service running on the DLP Enforce Server to execute the response rules. You can view the status of the workflow on the Data Insight Management Console.

Using the Self-Service Portal to confirm ownership of resources

You can use the Self-Service Portal to confirm or decline if you are the custodian of a particular path. On the **Ownership Confirmation** page of the portal, you can do following tasks:

- View all the paths for which you are requested to confirm your ownership.
- Select the paths you own and indicate your ownership.

To confirm ownership:

1. Select the paths for which you have to confirm your ownership.
2. Click **Confirm** to accept ownership of the data resource for the purpose of remediation.

After you submit the confirmation request from the portal, the actions are sent to the Data Insight Management Server. The Data Insight administrator can view the paths for which custodians have declined ownership, and assign other custodians to the paths. For more information, refer to *Symantec Data Insight Administrator's Guide*.

See "Logging in to the Self-Service Portal" on page 81.

Using the Self-Service Portal to classify sensitive data

You can use the Self-Service Portal to classify files based on business value of their content. You can mark files with sensitive information as record. Files that are marked as record are submitted to Symantec Enterprise Vault, if it is configured in Data Insight, for further action.

On the **Records Classification** page of the portal, you can do following tasks:

- View a snapshot of the number of files that are assigned for your attention.
- Mark the assigned files as record or no record. .
- Filter the list of files based on the the recency of the last access date or last modified date, or the policy that the files violate. The filters available to you depend on the options that are selected when configuring the workflow template.

  The different filters are applied together, and the list is filtered to show the data that matches the applied criteria.

To classify the files

1. Select the files that you want to remediate.
2. From the **Select Action** drop-down, select the action that you want to take on the selected files. For example, you may choose to archive the file. The listed actions indicate whether you want to mark the file as record or not. The name of the actions may vary depending on the name configured in the workflow.
3. Click **Submit** to send the remediation request to Symantec Enterprise Vault or the Data Insight Management Server for further action.

   The files that are marked as record are automatically archived using Symantec Enterprise Vault, if automatic action is enabled on these files. You can view the status of the workflow on the Data Insight Management Console.
4. Click **Delegate** to delegate the workflow to any other custodian.

Chapter 9

Using Data Insight reports

This chapter includes the following topics:

- About Data Insight reports
- Creating a report
- About Data Insight security reports
- Create/Edit security report options
- About Data Insight storage reports
- Create/Edit storage report options
- About Data Insight custom reports
- Create/Edit DQL report options
- Considerations for importing paths using a CSV file

About Data Insight reports

Data Insight includes several report categories with which you can see what storage is available and how it is allocated and utilized. The reports enable you to do the following:

- Monitor activity on the filers and SharePoint Web applications
- Make decisions about the best way to use the storage on configured resources

You can view reports at any time when working within the Data Insight Console and connected to a Data Insight Management Server.

Path driven reports only give access information on the selected paths.

Custodian driven reports give information about the assigned or inherited custodians on a path.

For each report type, you can configure any number of reports with different input parameters. You can then run them to generate outputs in CSV, PDF, and HTML formats.

Note: If a full scan of a filer server, share, or a SharePoint server has not been completed at least once, the data in the reports may not be accurate.

Reports are available for the following categories:

Access Summary Reports	See "Access Summary reports" on page 117.
Access Details Reports	See "Access Details report" on page 88.
Permissions Reports	See "Permissions reports" on page 89.
Capacity Reports	See " Capacity reports" on page 117.
Ownership Reports	See "Ownership Reports" on page 106.
Custom Reports	See "About Data Insight custom reports" on page 132.
Data Lifecycle Reports	See "Data Lifecycle reports " on page 119.
Consumption Reports	See "Consumption Reports" on page 121.

See "About stale information in reports" on page 145.

Creating a report

You can configure any number of reports of a report type. You create an instance of a report type by defining the parameters you want to include in the report, and saving it for continued use.

See "Create/Edit security report options" on page 108.

See "Create/Edit storage report options" on page 125.

See "Create Permissions Search report" on page 91.

See "Creating a Permissions Query Template" on page 93.

To create a report

1 Click on the **Reports** tab.

2 Click a category to view the types of reports in that category.

3 Click a report type to view the list of report instances.

The report details page appears.

4 To create a new instance of a selected report type, click **Create Report**.

5 Complete the relevant fields on the Add new report page, and click **Save**.

6 Click **Save and Run** to run the report immediately after saving it.

Note: For data custodian driven reports, Data Insight creates a report output for each custodian that you select at the time of creating the report.

You can now use the command line interface to create reports. For details, see the *Symantec Data Insight Administrator's Guide*.

About Data Insight security reports

Use Data Insight security reports to view and export the access details for the configured filers, shares, and Web applications, as well as by the configured users.

You can view custodian reports for various data locations.

You can create security reports for the following categories:

- Access Details reports
  See "Access Details report" on page 88.
- Permissions reports
  See "Permissions reports" on page 89.
- Ownership Reports
  See "Ownership Reports" on page 106.

Access Details report

Use the access details reports to view the details of access events on selected files or folders or by selected users. Two types of Access Details reports are available for selection:

- Access Details report for users or groups
  Use this report to get detailed accesses by one or more users or by members of one or more groups during the selected time window. Optionally, you can also include one or more users, as an input parameter for this report to display only the accesses by the selected users.
- Access Details report for paths

Use this report to get details of accesses on one or more files or folders during the selected time window. Optionally, you can also include one or more users, as an input parameter for this report, to get accessess of the selected users on the selected data resources.

Note the following about activity information captured by the Access Details reports:

- Data Insight does not expand built-in groups like Everyone or Authenticated Users. Authenticated Users group is not a true Active Directory group. Users are added to this group dynamically as they authenticate and log in to a domain. Since this is a dynamic group, Data Insight does not get membership information for this group during an Active Directory scan. Thus, activity information about such users and groups is not captured in these reports even if these groups to users or groups are selected when configuring the reports.
- Data Insight captures the IP address of the source machine (the location from which activity is generated) only in the case of NetApp CIFS and EMC CIFS paths. For rest of the devices such as Windows File Server, SharePoint, NFS paths, the Access Details report returns the IP address as 0.0.0.0.
- At this time, Data Insight does not relate an Permission change event with a specific user. Thus, when configuring an Access Details for Paths report, Permission Change events are not reported if you select a specific user or group.

  To get information about all Permission Change events, you must select **User Selection** > **All Users/Groups** option when configuring the report. If you do not make any selection on the **User Selection** tab, Data Insight creates the report for all users by default.

Permissions reports

Use the Permission reports to get detailed information of the permissions assigned to various users, files, and folders. You can also use these reports to orchestrate permissions to reduce risk and control access.

Drill down the summary table to view the detailed report.

Inactive Users

Inactive users are users who have privileges to access the specified paths, but have not accessed these paths during the selected time period.

The Inactive Users report displays a list of inactive users on the selected paths during the specified duration. The report also shows the directory service attributes of the inactive users.

Path Permissions

The Path Permissions report displays the permissions assigned on the selected paths. The Path Permissions report calls out the permissions that are inherited from the parent folder and whether the access to a path is granted because a user is a member of a group that has access. If the Inherited from path and Inherited from group columns in the report are blank, it implies that a user has access because the permissions have been explicitly assigned to the user; the permissions are not inherited from any source, neither from the path ancestors nor from any group that the user is a member of.

You can optionally restrict the report to permissions assigned on selected paths to the selected users.

This report takes input parameters in the following two ways:

- Path driven reports - give access information on the selected paths by the selected users.
- Custodian driven reports - give information about paths on which user is assigned as custodian.

Permissions Search report

The Permissions Search report uses the Permissions Query Template as input to search for permissions to specific trustees (users, groups, or unresolved SIDs) that match or violate the rules defined in the template.

You can create templates to search for the following:

Access Control Entries (ACEs) in an ACL	The ACE that identifies a trustee, specifies the access rights - allowed or denied for that trustee on an object (on a path). The ACE Search report returns individual ACEs that match or violate the rules in the template.
Access Control List (ACL)	The ACL is a list of access control entries for a file or folder. The ACL Search report returns the entire ACL that match or violate the rules in the template, although the rules evaluate the ACEs within the ACL.

See “About Permissions Query templates” on page 92.

See “Creating a report ” on page 87.

See "Create Permissions Search report" on page 91.

See "Creating a Permissions Query Template" on page 93.

See "Creating custom rules" on page 98.

Create Permissions Search report

Use this dialog to create an instance of a report.

Table 9-1 Create Permissions Search report options

Option	Description
Report Information	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Description** - A short description of the data that is contained in the report. ■ **Output Format** - Select the format in which you want to generate the report. You can select one or all of the given output formats. ■ **Schedule** - Select the schedule at which you want the report to run. ■ **Maximum Reports to preserve** - Select the number of report outputs you want the system to preserve. The default value to preserve the report outputs is now unlimited.
Configuration	From the **Select Template** drop-down, click **Manage Templates** to create a template. See "Creating a Permissions Query Template" on page 93. See "Creating custom rules" on page 98. **Include custom attributes of user** - Select the check box to include custom attributes in the report output. From the drop-down list, select a configured custom attribute. By default, the check box is cleared. For more information on configuring the custom directory attributes, see the *Symantec Data Insight Administrator's Guide*.

Table 9-1 Create Permissions Search report options *(continued)*

Option	Description
Data Selection	Do the following: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or, select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. Or, select the **Containers** radio button to view the available containers that can be added in the report. 2 Click the site, file server, share, or folder to select it. The selected data set is listed in the **Selected Data** pane. You can also use a .csv file to import paths for creating reports. Only valid paths in the .csv file are displayed in the **Selected Data** pane. 3 **Add resource**- Enter the resource path and click **Add** to include the path name in the report output.
Notification	Enter email addresses of users you want to send the report to. If the size of the attachment is above the configured limit, an email is sent without the attachment. You can configure the size of the attachment under **Settings** > **SMTP Settings.**

About Permissions Query templates

Data Insight lets you create rules that you can use to analyze permissions assignment in your organization. The rules can be applied to your data set to search for the permissions that determine a trustee's (user, group, or unresolved SID) access to an object as also search for violations that help you control access to resources.. A permission search rule is a set of conditions with one or more parameters.

The permission search rules are a combination of parameters such as ACE type, the trustee type, the trustee (user or group), the type of rights, and the object that the rule is evaluating. A rule may specify all or any of these parameters. You can either add pre-defined rules to a template or create custom rules that define one or more conditions that form a permission search criteria. You can use different keywords to specify how Data Insight should evaluate the rules in the template.

The Permissions Query Template is a container for multiple frequently-used rules that you can use as input to create a permission search report.

You can apply the template to your data set to do the following:

- Review access to trustees on shares and folders.

- Ensure that your organization adheres to security policies and permission best practices.
- Identify all the compliance violations for permission hygiene.
- Remediate access to global groups such as Everyone.

You can create different templates to classify the rules in different categories such as one template for all compliance rules, or one template for rules to evaluate violations of best practices.

You can use the saved templates to create a Permissions Search Report from the **Reports** tab of the Management Console. A Permissions Search report lists the paths that match or violate the search criteria that are defined in the rules.

The following are examples of the different queries that you can build using the predefined or custom rules:

- Show all paths on which User X has access.
- Show all files that have explicit ACEs defined on them.
- Show all paths with Full permission.
- Show all paths/shares where a trustee of type "User" has access.
- Show all paths where inheritance is broken.

Note: A Permissions Query Template is tightly integrated with a Permissions Search report. All templates that you create are available for selection when you create a Permissions Search report. You can also edit, copy, or delete a saved template either from the report configuration page or from the list view page.

See “Create Permissions Search report” on page 91.

See “Creating a Permissions Query Template” on page 93.

See “Creating custom rules” on page 98.

Creating a Permissions Query Template

The Permissions Query Template is an integral part of the Permissions Search report. A Permissions Query Template enables you to save the frequently-used rules that define a permission search criteria. You can save a combination of multiple predefined and custom rules in a template.

You can create or use a saved Permissions Query Template to create a Permissions Search report.

To create a Permissions Query Template

1. On the Management Console, click **Reports** > **Permissions Reports** > **Permissions Search**.
2. On the Create Permissions Search Report page, click the **Configuration** tab.
3. From the **Select Template** drop-down, select **Manage Templates**.
4. On the **Manage Templates** page, do the following:
   - **Name** - Enter a logical name for the template.
   - Before you can select a predefined rule or create a custom rule, you must select whether you want to search for a specific Access Control Entries (ACEs) or Access Control Lists (ACLs) that match or violate the rules that are defined in the template.
     From the drop-down, select **ACE**/**ACL** that **Match/Do not match Any/All/ Exactly** rules in the template.
     These options dictate how the rules are evaluated when the report is run.
     See "Using the match-type criteria" on page 95.
   - **Rule** - Click the **Add Rule** drop-down to select one or more predefined rules.
     Or click **Add Rule** > **Custom Rule** to create a rule with custom conditions.
     See "Creating custom rules" on page 98.
     The following predefined rules that are available for selection.

Rule	Description
Trustee is user	Search for all users with any type of permission.
Trustee is unresolved	Search for the paths on which Unresolved SIDs (the SIDs which cannot be mapped to any of the domains) have been granted permissions. In case of Unresolved SIDs, you cannot determine whether the SID belongs to a user or group.
Trustee is Everyone	Search for all ACEs where the group of type Everyone has permission.
Trustee is Disabled	Search the paths where disabled users have been granted any permission of type Allow or Deny.

Rule	Description
Trustee is Deleted	Search the paths where deleted users have been granted any permission of type Allow or Deny.
Trustee is non-domain account	Search for all users or groups which do not belong to any configured domain in the directory service. For example, this search query fetches all users or groups that do not belong to either Domain Local, Global, or Universal group.
Trustee is empty group	Search for all groups that have permissions on paths but do not have any members.
Trustee is open group	Search for the user groups that are specified in an open share policy. For more information about open share policy, see the *Symantec Data Insight Administration Guide*.
Permission is Full	Search for the users or groups which have the Full Control (Allow) on a file or folder.
Permission is Deny	Search for the users or groups that have the Deny setting for any kind of permission.

5 Click **Share Template** to enable specific users to reuse the template.

See "About sharing a Permissions Query Template" on page 104.

6 Click **Save**.

Using the match-type criteria

If there are multiple rules in a template, the report output displays the results of the configured rules based on the match type criteria that you select.

The expected results that the ACE search report will return depends on the match type that you select. For example, if the template consists of two rules:

- Trustee is user (Rule 1)
- Trustee is disabled (Rule 2)

Table 9-2 ACE Search match-type criteria

Match type Criteria	Expected Result
Match any of the rules	The report output returns such paths that match either Rule 1 or Rule 2. Thus, the report displays records (paths) with ACEs where a trustee of type user has Allow or Deny type of permission *or* where the trustee state is Disabled. In the report, **Unmatched Rules** column shows the rule that does not match.
Match all of the rules	The report output displays all such paths with ACEs that match both the rules. Thus, the report displays such paths where a trustee of type user has **Allow** or **Deny** type of permission *and* where the trustee state is **Disabled**. In the report, **Unmatched Rules** column must not show any configured rules.
Do not match any of the rules	The report output returns such paths with ACEs, where none of the ACES match any of the configured rules. In the report, **Unmatched Rules** column shows both the configured rules.
Do not match all of the rules	The report output returns such paths that do not match every configured rule, but may match some of the rules. Thus, some paths may match Rule 1 and some paths may match Rule 2. In this case, the report returns all such paths where the Trustee is a user or the paths where a disabled user has Allow or Deny type of permission. The **Unmatched Rules** column should always show at least one rule.

In case of an ACL search report, the report returns the complete ACL although the rules evaluate the individual ACEs within the ACL.

For example, the template consists of the following rules:

- CIFS Permission is (Full) SharePoint Permission is (Full Control) (Rule 1)
- Trustee is Everyone (Rule 2)
- Trustee is Unresolved (Rule 3)
- ACE count = 3 (Rule 4)

Table 9-3 ACL Search Match-type criteria

Match type Criteria	Expected Result
ACLs that match any of the rules	The report output returns such ACLs where at least one ACE within each ACL matches at least one configured rule. The **Unmatched Rules** column displays the rules that do not match
ACLs that match all of the rules	The report output returns such ACLs where ACEs across each ACL match all configured rules. Thus, a single ACE within an ACL may fulfill all the rules or all ACES across an ACL may fulfill all the rules. Thus, the report may return ACL 1, ACL 2, and ACL 3 where the ACEs across each ACL match rules 1 to 4.
ACLs that match exactly all the rules	The report output returns such ACLs where each ACE within the ACL matches either rule 1,2,3, or 4 or all configured rules. All ACEs within an ACL should match at least one rule, and all configured rules should be present within the ACL. Thus, if an ACL has an ACE that does not match any of the configured rules, that ACL will not be displayed in the report.
ACLs that do not match any of the rules	The report returns such ACLs where for every ACE none of the rules should be matching. All configured rules should ideally show under the **Unmatched rules** column in the report.

Table 9-3 ACL Search Match-type criteria *(continued)*

Match type Criteria	Expected Result
ACLs that do not match all of the rules	The report output returns such ACLs where the ACEs within the ACL do not match the complete set of configured rules, however the ACEs within the ACL may match some of the rules. Thus, the configured rule set should not match at least one ACE. The **Unmatched Rules** column should always show at least one rule.
ACLs that do not match exactly all the rules	The report output returns such paths where at least one ACE within the ACL should not match the configured rule set. Or at least one rule should not be present within the ACL.

Creating custom rules

Data Insight lets you create custom permission search rules which are a combination of multiple criteria that includes the type of permission, the scope of the report output, and attribute filters, as required. These custom rules can be saved to a Permissions Query Template along with the predefined rules.

You must create different rules to search for specific ACEs or ACLs that match or violate the rules that you define.

To create a custom rule

1. On the **Configuration** tab, select **Select Template** > **Manage Templates**.
2. On the **Manage Templates** pop-up, select **Create Template**.

   See "Creating a Permissions Query Template" on page 93.
3. Enter a logical name for the template.
4. From the drop-down, select whether you want to create a custom rule to search for ACLs or ACEs.
5. Select the match type criteria for evaluating the rules.

   See "Using the match-type criteria" on page 95.
6. Select **Add Rule** > **Custom Rule**.
7. On the **Custom Rule** panel, you can select options from the high-level categories, **Permissions** and **Trustee**.

8 You can use conditions based on the configured custom attributes to refine the selections that are made in the **Trustee** section. The available conditions depend on the configured custom attributes. For information about configuring custom attributes, see the *Symantec Data Insight Administrator's Guide*.

9 Select **Inheritance is broken** if you want to search for paths with unique permissions. If you select this option, the report output displays only those paths or sites that do not inherit permissions from the parent.

10 Select **Share permissions are more restrictive than file system ACLs** to display such paths where trustees are allowed permissions at the filer level but denied access at the share-level.

11 Select an operator and specify a value for the **Path Depth**. This option can be used to search for paths where unique permissions are defined at a certain depth in the file system hierarchy.

12 Select **Duplicate ACEs** to search for such ACLs that contain an ACE on the path that is inherited and an identical ACE that is explicitly defined.

13 Click **Save Rule** to add the rule to the Permission Query Template.

Note: The criteria that are selected in each section on the **Custom Rule** panel are combined to form a rule.

Permissions

Selections in the **Permission** section let you specify the CIFS and SharePoint permissions that you want to search. By default, you can select the most common CIFS permissions or the default SharePoint permission levels or select **Advanced** in the drop-down to select the meta access types for CIFS and SharePoint. If you select more than one Advanced permission, you can further use the Match All or Match Any criteria to decide whether Data Insight must search for all or any of the selected **Advanced** permissions.

Note: **Allow** and **Deny** options are only applicable to search for CIFS permissions. For SharePoint paths, Data Insight considers **Allow** by default.

Table 9-4 describes how these options can be combined to create a search rule.

Table 9-4

If you want to...	Use this search criteria
Search for trustees who are allowed full control	Select the **Allow** check box, and Click **CIFS Permissions** or **SharePoint Permissions**, as the case may be. Select **Full** in case of CIFS permissions and **FullControl** in case of SharePoint permissions..
Search for trustees denied the **Modify** type of permission on CIFS paths.	Select the **Deny** check box and select **CIFS Permissions** >**Modify**.
Search for trustees with allow **Write** type of permission on CIFS paths .	Select the **Allow** check box, from the drop-down, select **CIFS Permissions** > **Advanced** > **Match All**. This displays a list of all Windows Advance permissions. Select the **Write Data** check box.
Search for trustees with **ManageLists** type of permission for SharePoint paths.	From the drop-down, select **Advanced**, and click **SharePoint Permissions**. This displays a list of all SharePoint permissions associated with the default permission levels. Select the **ManageLists** check box.

Note: Use the options in the **Permissions** section with the options in the **Trustee** section to further refine your search criteria.

Trustee

Selections in the **Trustee** section determine whether you want to display users, groups, unresolved SIDs, or any of these in the Permission Search report output.

Table 9-5

If you want to...	Use this search criteria
Search permissions that are assigned to groups of type domain local, where the group name starts with *xyz*.	**Trustee Type** - From the drop-down, select Group. By default, the group tab is selected, and the options for defining the scope for Groups are displayed. **Scope** - select **Domain Local** Add a condition using the **Select filter** drop-down; select an attribute, operand, and a value for the attribute. For example, Name = *xyz*.
Search for trustee of type Universal, where the status of the group is deleted.	■ **Trustee Type**e - From the drop-down, select **Group**. By default, the group tab is selected, and the options for defining the scope for Groups are displayed. ■ **Scope** - select **Universal** ■ **Status** - **Deleted**
Search for all deleted Built-in Local users.	■ **Trustee Type** - From the drop-down, select **User**. ■ **Scope** - **Local** ■ **Type** - **Built-in** ■ **Status** - **Deleted**
Search for the Global groups whose direct user member is Joe.	■ **Trustee Type** - From the drop-down, select Group. By default, the Group tab is selected. ■ Scope - Global ■ Click the **Member** tab. ■ **Member Type** -**User** ■ **Membership Type** - **Direct** ■ Add a condition using the Select filter drop-down; select an attribute, operand, and a value for the attribute. For example, *Log on Name contains Joe*.

Note that the all selections on the **Custom Rule** page are optional. Data Insight uses the **Any** option, where available, as the default option when no selection is made.

Example custom rules

Table 9-6 describes the various options that you must select to create custom rules for different scenarios.

Table 9-6 Example scenarios and corresponding custom rules

Scenario	Example custom rules
Search for individual users excluding users belonging to the department called Admin.	In the **Trustee** section, select **User** and add the condition, Department != Admin.
Search for use of permissions to global groups.	For this scenario, you must create a custom rule to search for global groups that have permissions on paths. In the **Trustee** section, select **Group** > **Global**.
Permission best practice suggests that only local domain groups should be trustees and a global security group should inherit permissions from a local domain group. Rule - Detect global groups with explicit permissions.	Rule - In the **Trustee** section, select **Group** > **Global**. For this rule, the report output will list all Global groups that have explicit permissions assigned to them.
Search for a groups containing more than one direct member groups.	In the **Trustee** section, select **Group**. In the attribute filter, add the following condition: Direct group count > 1
Search for local domain groups with more than one global group. Ideally, every domain local group should not have more than one global group.	In the **Trustee** section, select **Group** and select the scope as **Domain Local**. On the **Member** tab, select the following: ■ **Member Type** - Group ■ **Membership Type** - Any ■ **Scope** - Local Domain
Search for groups with direct user members of type local whose name contains Joe.	In the **Trustee** section, select **Group** and on the **Member** tab, select the following: ■ **Member Type** - User ■ **Membership Type** - Direct ■ **Scope** - Local In the attribute filter, Logon name contains Joe.

Table 9-6 Example scenarios and corresponding custom rules *(continued)*

Scenario	Example custom rules
Search for global groups that contain member groups. As a best practice, global groups should only contain users accounts as members.	In the **Trustee** section, select **Group**. In the attribute filter, select Direct group count > 0.

See "Creating a Permissions Query Template" on page 93.

Permissions Query Template actions

The following actions are allowed for a Permissions Query Template:

- Edit a template.
- Delete a template.
  See "Editing or deleting a Permissions Query Template" on page 103.
- Copy a template.
  See "Copying a Permissions Query Template" on page 104.
- Share a template.
  See "About sharing a Permissions Query Template" on page 104.

Editing or deleting a Permissions Query Template

You can edit a saved Permission Query Template by modifying the rules that define the permission search criteria or by adding new rules or deleting existing rules.

To edit an existing template

1. Do one of the following:
   - On the Permissions Search reports list page, select the report that uses the template that you want to edit.
     Click **Select Action** > **Edit**.
   - Or Click **Create Report**.
2. On the report configuration panel, click the **Configuration** tab.
3. From the **Select Operation** drop-down, select an existing template, and from the same drop-down, select **Manage Templates**.
4. To modify the template, add pre-defined rules or custom rules to the template, or click **Clear Rules** to delete all rules that are added to the template. To modify an existing rule in the template, click the **Edit** icon next to the rule.

You can also delete an existing template.

Note: You cannot delete a template if it is being used by a Permissions Search report.

To delete a template

1. Navigate to the **Manage Templates** window, and select the template that you want to edit, and select **Manage Templates**.
2. Click the **Delete** icon.

   You are prompted to confirm the template deletion.
3. Click **OK**.

Copying a Permissions Query Template

You can copy an existing template and modify the rules to create a new Permissions Query template. This can save you a lot of time if the template contains a number of rules.

To copy a template

1. On the Create Permission Search Report page, click the **Configuration** tab.
2. From the **Select Template** drop-down, select **Manage Templates**.
3. Click the **Select Operation** drop-down and locate the template that you want to copy by navigating to the list of templates.
4. Click the **Copy** icon next to the selected template.
5. Enter a logical name for the new template, and click **Copy**.

The copied template is now available for selection. You can further edit the copied template to suit your requirements.

About sharing a Permissions Query Template

You can share a Permissions Query Template that contains rules that help you search for specific permission assignments within your organization.

When sharing a template, you must keep the following in mind:

- The template can be accessed only by users who are assigned Server Administrator or Report Administrator role.
- A shared template can be edited only by the creator, or a user who is assigned Server Administrator or Report Administrator role.

Using Permissions Search report output to remediate permissions

The Permissions Search report provides visibility into the permissions on unstructured data as also gives critical insight into violation of permissions best-practices. It provides intelligence that enables you to control access by remediating permissions and group memberships.

You can use the output of the Permissions Search report to analyze and remove excessive permissions.

Note: Ensure that you have configured remediation setttings and enabled permission remediation. For more information, see*Symantec Data Insight Administrator's Guide*.

To remove permissions

1 Create a Permission Query Template with rules that define certain standards or violations.

  See "Creating a Permissions Query Template" on page 93.

2 Create a Permission Search report by selecting a template.

  Depending on the rules that are configured in the template, the report output displays all records that violate the best practices defined in the rules or match rules that define a deviation.

3 Select the report output. Click the corresponding **Select Action** tab, and select **Remediation** >**Remove Permissions**.

4 On the Remove Permissions pop-up review the permission, and click **Submit changes**.

When you submit the request to remove permissions, a Permission Remediation workflow is initiated. The configured remediation action is executed on the recommendations made in the Permissions Search report.

Entitlement Review

The Entitlement Review report reviews user entitlements on a specified path. It also indicates whether the user is active or not.

The Entitlement Review report provides the following information:

- The name of the user.
- The permissions assigned to the user on a specified path.
- The SharePoint permission levels assigned to a user on a specific path.

- The account name of the user.
- The status of the user. For example, if the user is active in the group or not.

User/Group Permissions

The User/Group Permissions report displays the permissions assigned to selected users or groups on the selected paths.

Group Change Analysis

Use this report to analyze the business impact of revoking permissions of users and groups on paths. You can choose to run this report for the permission recommendations that are provided by Data Insight on the **Workspace** tab. Or you can manually create this report from the **Reports** tab.

The Group Change Analysis report helps you evaluate the repercussions of the following actions:

- Revoking the permissions of a group or a set of groups on a selected path.
- Modifying groups by removing users from the group.

The report gives the information about the active users who will lose access to the selected path because they are part of the group whose permission is revoked.

The number of inactive users who have gained access to the selected path.

Drill down the summary table to view the detailed report. Click on a control point to view the detailed analysis.

Ownership Reports

Use these reports to get information about users who are responsible for remediation on assigned data locations.

By default, two types of Ownership reports are available for selection:

Data Custodian Summary

Use this report to get detailed information of the assigned custodians. The Data Custodian Summary report provides the following information:

- The name of the custodian.
- The account name of the custodian, for example, user@domainname.com.
- The filer or Web application on which there is a custodian assignment.
- Access path - the physical path on which the user is assigned as custodian.

- DFS path - The DFS path on which the user is assigned as custodian.
- The status of the selected user in the directory service. For example, active, disabled, or deleted.
- Information about attribute values.

Inferred Owner

Use this report to get a summary of inferred owners on the specified paths. The owners are determined based on the activity on the files during the specified time period.

The Inferred Owner report provides the following information:

- The name of the share or site collection.
- DFS path - The DFS path on which the inferred owner is assigned as custodian.
- The name of the inferred owner.
- The account name of the inferred owner.
- The name of the business unit.
- The name of the business owner.
- The data owner policy through which the data owner is inferred.

In addition to these ownership reports, you can also get ownership information for paths in the following reports:

- Access summary for paths report
- Data Aging report
- Inactive folders report
- Path permissions report
- Consumption by folders report

Data Inventory Report

Use this report to get details about all files stored on all the filers that Data Insight monitors. This report gives detailed information about the following:

- The total number of users who have accessed the files. Owners of the files
- The custom attributes of the users who have accessed the files.
- The line-of business (LOB) to which the users belong.
- The total LOBs that have access to the files.

- The total number of files.
- Whether a file is sensitive or not. Data Insight fetches the sensitivity information for files from Data Loss Prevention.
- The age of the files.
- The activity on the files.

You can choose to create the following options for the Data Inventory report:

- A summary report that lists the number of files in shares across filers.
- A summary along with information about the number of sensitive files on the filers.
- A detailed report that includes all the above-mentioned information

The Data Inventory report does not have a viewable format through the GUI. However, you must select an output format when creating the report. You can view the Data Inventory report output database using an SQLite administration tool, such as the `sqlite3.exe` utility that is bundled with Data Insight installer. Symantec does not recommend using browser-based plug-ins or extensions to open the large database files that are generated by the Data Inventory report.

Create/Edit security report options

Use this dialog to create an instance of a report. The options available on the page and their order depend on the type of report that you select.

Table 9-7 Create/Edit security report options

Option	Description
Report Information	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Description** - A short description of the data contained in the report. ■ **Report Type** - The type of security report. This field is populated by default. ■ **Select resources using** - Select **Paths** or **Custodian Information** radio button. Depending on the selection, you can see the data selection or custodian selection option. **Note:** This field is available only in the following five reports : ■ Access summary report for paths ■ Data aging report ■ Inactive folders report ■ Path permissions report ■ Consumption by folders report ■ **Output Format** - Select the format in which you want to generate the report. You can select one or all of the given output formats. ■ **Maximum Reports to preserve** - Select the number of report outputs you want the system to preserve. The default value to preserve the report outputs is now unlimited. In case of scheduled reports, setting up value of this parameter to **Unlimited** may fill up disk space. Configure the value appropriately by taking disk space into consideration. ■ **Schedule** - Select the schedule at which you want the report to run. ■ **Copy output to** - Enter a path to copy report output files. To successfully copy a report output to an external computer, you must ensure that the **Secondary Logon** windows service is running in the Management Server. ■ **Select Credentials to access "Copy output to" path** - Select a credential from the drop-down menu, so that Data Insight can direct the report output to the specified location. Aditionally you can use the option for adding a new set of credentials if the required credentials are not already added. The credentials must have folder-level read, write, create and delete permissions on the external computer where the report output is copied. ■ **Overwrite option** - Selecting this option overwrites the earlier report output files. If you clear this check box, Data Insight creates a new folder with a report run ID for every report run, and saves the report in the new folder.

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
Configuration	

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
	Select the conditions to configure the report. - **Time Period** - Enter the time range for which you want data to be included in the report. Select **Duration** to indicate the last n hours/days/weeks/months/year. Select **Date Range** to specify a specific time range. - **Bucket Size (Months)** - Enter the bucket interval that you want to include in the report. - **Access Type** - Select the access types you want to include in your report. - **Include custom attributes of user** - By default, the check box is cleared. Select the check box to select the custom attributes from the drop-down list. For more information on configuring the custom directory attributes, see the *Symantec Data Insight Administrator's Guide*. - **Select order of policies for computing data owner**- The up and down buttons help you change the order of data owner policy according to your preference in the report output. - **Inactive Time Period** - From the drop-down, select the duration of inactivity for files. Only the files that have remained inactive for the selected duration are included in the report. This field is only available for the Inactive users report. - **Folder Depth** - Select the depth of subfolders to be included in the report from the drop-down list. This option is useful when you want to limit the total output in the report. From the drop-down, - Select **Current folder**, to include the folders from the current directory. - Select **Full** to include all the folders. - Select **Specify Depth** and enter the level at which you want to include the folders. You can add folder depth for the following reports: - Path Permissions - User/Group Permissions - Inferred Owner - Entitlement Review - **Effective Permissions** or **Access Control List** - Select the appropriate radio button to include required permissions in the report. - **Include share level permissions** - Select the checkbox to include share level permissions in the report. - **Display only unique permissions** - Select the checkbox to include only the unique permissions in the report. - **Show advance permissions** - Select this checkbox to include all the

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
	advance permissions in the report. ■ **Expand User Groups** - Select this checkbox to include the member count in the report. ■ **Member count** - Enter the number of expanded member users that you want to include in the report output. **Note:** This option is available only for Entitlement Review report. ■ **Select columns to hide in output** - Select the columns that you do not want to display in the report. ■ **Truncate output if record exceeds**- Enter the number of records(rows) after which the report output is truncated. See "Configuring a report to generate a truncated output" on page 148. ■ **Department mapping** - You can map the department through the options available in the drop-down list . The generated report maps the department on the basis of the option you choose. ■ **Filter**- This option is available only for the Data Inventory Reports. Use the filter to specify the following : ■ **Time filter**- From the drop down, select an option to consider all the files that are last accessed or modified before a given time. ■ **File Group**- Select this option to specify the file groups, to be considered for generating the report output. ■ **File Type**-Select this option to specify file types to be considered for generating the report output. Specify the extensions of the file types to be considered in a comma separated list. ■ **DLP Policy**-Select a DLP policy to be considered for generating the report output.

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
	■ **Results**-This option is available only for the Data Inventory Reports. Use this option to specify the following: ■ **Summary only**- Select this option to create a report which displays the summary of the files grouped on the basis of either BU Name, BU Owner, or any other Custom Attibutes that you have selected from the **Department Mapping** drop-down. ■ **Summary and Sensitive file details**-Select this option to create a report which displays: ■ The details of the all the sensitive files present. ■ The summary of all the files grouped by business unit name, business unit owner, or any other custom attibutes that you have selected from the **Department Mapping** drop-down. ■ **Summary and all file details**-This option is available only when a DLP policy is selected in the **Filter** option. Select this option to create a report which displays: ■ The details of the all the files. ■ The summary of all the files grouped by business unit owner, or any other custom attibutes that you have selected from the **Department Mapping** drop-down. ■ **Number of Records**- Specify the number of records you want to include in the detailed report. The report computes the number of records as the top N files based on the file size for every data owner. From the top N files, (for example, in case of Data Inventory report) the report will display the top N files based on the department mapping configured. The default is 25 records.

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
Data Selection	Do the following: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or, select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. Or, select the **Containers** radio button to view the available containers that can be added in the report. Click the site, file server, share, or folder to select it. The selected data set is listed in the **Selected Data** pane. 2 **Add resource**- Enter the resource path and click **Add** to include the path name in the report output. 3 You can also use a CSV file to import paths for creating reports. Click **Upload CSV**. On the pop-up, you can download the CSV template to review the input values and the format of the CSV file for that particular report. Only valid paths in the .csv file are displayed in the **Selected Data** pane. Browse to the location of the CSV file and click **Upload**. This option is available for the following reports: ■ Access Details for Paths ■ Access Summary for Paths ■ Path Permissions ■ Entitlement Review
Custodian Selection	For data custodian driven reports Data Insight creates a report output for each selected custodian at the time of generating a report. For each custodian, all paths that belong to the custodian are considered. Custodian selection is an indirect way of selecting paths. For example, If a custodian has two locations assigned - \\netapp1\fin-share and \\netapp1\hr-share, then selecting this custodian as a custodian is equivalent to selecting these two paths through data selection.

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
User Selection	From the list, click the user, group, or all users/groups radio button. The selected entities are listed in the Selected Users/Groups pane. You can type a name in the search bar to search for a user or group. You can also type a domain name in the Domain Filter field to narrow your search to users in a specific domain. **Note:** You can search for a particular Built-in user or group by using the Domain Filter. You can also filter a user or group from the Select Filter field. Select the All Filtered Users check box in the Selected Users/Group pane to include all filtered users in the report. You can also import user information using a CSV file for creating reports. Only valid users in the CSV file are displayed in the **Selected Users/Groups** pane. You must enter the users and groups in the following format: user@domain or group@domain.
Exclusion List	Select the groups or users that you want to exclude from the scope of the report. Click the group or user to select it. The selected data set is listed in the **Selected Groups/Users** pane. **Note:** You can search for a particular Built-in user or group by using the Domain Filter.
Notification	Enter email addresses of users you want to send the report to. If the size of the attachment is above the configured limit, an email is sent without the attachment. You can configure the size of the attachment under **Settings** > **SMTP Settings.**

Table 9-7 Create/Edit security report options *(continued)*

Option	Description
Remediation	Use this tab to instruct Data Insight to execute predefined actions on a report output. Select **Take action on data generated by report** to enable automatic processing of data generated by a report. Select any of the following: ■ **Archiving (Enterprise Vault)** - Select this option to archive data using Symantec Enterprise Vault. If you select this option you must specify a retention category and a post-processing action. ■ **Custom Action 1** / **Custom Action 2** - Select this option to specify a custom action defined by a custom script. See “About managing data using Enterprise Vault and custom scripts ” on page 73.

About Data Insight storage reports

Use Data Insight storage reports to view details of how the storage available on configured data repositories is being used in your organization and to make decisions about the best way to use these storage resources. Storage reports enable you to do the following:

- Analyze your current storage.
- Identify inactive data that is occupying primary storage resources.
- Identify owners of inactive data that is stored on the file servers.
- Move data that is no longer actively used to a cheaper storage.
- Assign charge back of storage costs to the business unit to which data owners belong.
- Forecast archiving storage needs based on the information about the size of inactive data and files that are to be archived.

You can use these reports to identify usage patterns and trends. Based on this information, you can decide how best to assign storage on servers to meet current or emerging capacity needs.

The reports may not contain any data if you have not scheduled any scans.

For most reports, Data Insight displays a summary report and a detailed report.

Summary reports display high-level information in the form of tables or pie charts. From the summary table, you can drill down to a detailed report by clicking on a value, object type, or data point. For example, to view a list of files that have not been accessed for a period of 3 months to 6 months, click 3-6 months in the summary table of the Data Aging report.

You can create storage reports for the following categories:

- Access Summary Reports
  See “Access Summary reports” on page 117.
- Capacity Reports
  See “ Capacity reports” on page 117.
- Data Lifecycle Reports
  See “Data Lifecycle reports ” on page 119.
- Consumption Reports
  See “Consumption Reports” on page 121.

Access Summary reports

Use the access summary reports to view aggregate data about the accesses on selected paths or by selected users. By default, two types of Access Summary reports are available for selection:

- Access Summary reports for users or groups
  Use this report to get total number of accesses by one or more users or by members of one or more groups during the selected time window. Optionally, you can also specify a share or a folder on which you want to know the user's accesses.
- Access Summary report for paths
  Use this report to get total number of accesses on one or more shares, site collections, or folders during the selected time window. You must specify at least one share, site collection, or folder to run this report. Optionally, you can also include one or more users, as an input parameter for this report to limit accesses on selected paths to those users.
  This report takes input parameters in the following two ways:
  - Path driven reports - give access information on the selected paths by the selected users.
  - Custodian driven reports - give information about paths on which the selected user(s) is assigned as custodian.

Capacity reports

Use the Capacity reports to view and export details about how storage on file servers is distributed at the enterprise or at the group levels. You can use this information to find where storage is available for the users and groups that need it. You can also use this information to identify where storage can be used more efficiently.

Filer Utilization

The Filer Utilization report displays a summary of the space used and the free space available on configured Network Attached Storage systems.

You can view the following details about a file server in the report:

- The host name or IP address of the file server.
- The space used on the file server in GBs.
- The free space available on the file server in GBs.
- The total space available on file server.

Note: The Filer Utilization report is not currently available for SharePoint, VxFS, and EMC Celerra file servers.

Filer Growth Trend

The Filer Growth Trend report displays an overview of the fastest growing data repositories in the enterprise. The trend is measured by the percentage increase in the capacity of the data repositories. For each resource, the report displays line graphs that show the trend in the growth of the storage capacity on the resource and growth of space utilization on the resource over a period of time. This report helps you analyze storage utilization trends on the data repositories and identify opportunities for efficient capacity use. The trend data promotes storage requirements planning.

The summary table provides information about the following:

- The host name or IP address of the file server.
- Capacity of the file server at the beginning and end of the selected period.
- Free space on the file server at the beginning and end of the selected period.
- Storage utilization on the file server at the beginning and end of the selected period.
- The percentage growth in the capacity of the file server for the specified duration.
- The percentage of space utilization on the file server for the specified duration.
- The percentage of change in the free space on the file server for the specified duration.

Note: The Filer Growth Trend report is not currently available for SharePoint, VxFS, and EMC Celerra file servers.

Data Lifecycle reports

Use the Data Lifecycle reports to view and export details of space used by inactive files and directories stored on configured file servers or SharePoint Web applications for the selected time period. You can create these reports for all configured data repositories or for selected file servers or SharePoint Web applications.

Each report contains a summary table. You can drill down from the summary table to view the following details of the inactive files:

- The elapsed time since the file or directory was last accessed or created.
- The file server and the share name on which the file is stored, or the Web application and the site collection on which the file is stored
- The file path.
- The space, in MBs, used by the file.
- The date on which it was last accessed.
- The name of the user and user account that last accessed the file or directory.
- The name of the business unit to which the user belongs.
- The name of the owner of the business unit.

Inactive Data by File Group

The Inactive Data by File Group report displays a summary of inactive files on configured file servers or SharePoint Web applications. The inactive files are sorted according to file groups. The information helps you identify the file groups that occupy the most space on your storage resources. You can create these reports for all configured data repositories or for selected file servers, shares, Web applications, or site collections.

By default, the files are sorted into 18 file groups. The summary table in this report displays the size and count of files under a file group.

You can modify the default file groups that appear in the report. For more information on configuring file groups, see the *Symantec Data Insight Administrator's Guide*.

Inactive Data by Owner

The Inactive Data by Owner report displays a summary of inactive files, sorted according to the user accounts that own these files. The information helps you monitor file aging and identify the patterns with which users are accessing and updating files.

The summary table displays the configured user accounts, listed in the descending order based on the size of inactive files owned by users. For each user, the table lists the following:

- The size of inactive files.
- The percentage of space used by the files.
- The count of the files.
- The owner of the business unit.
- The business unit the user belongs to.

You can drill down the summary table to view the detailed report. Click on the name of a user to view details of all the inactive files owned by that user.

Data Aging

The Data Aging report displays cumulative information about file aging on the configured file servers or SharePoint Web applications, sorted according to the last access date range. The information lets you quickly and visually assess stale files on your file servers.

A file’s age is measured by the elapsed time since the file was last accessed on a file system.

The pie charts in this report display aggregate file statistics for inactive files on the selected file servers or SharePoint Web applications. The pie charts display statistics for the following parameters:

- The count of files based on the last access date.
- The size of files based on the last access date.

The summary table in this report lists several age intervals. By default, the bucket interval is 0 to 12 months.

You can drill down the summary table to view the detailed report. Depending on the scope of the report, you can click on the name of a file server, share, or SharePoint site to view data aging details for that file server, share, or site.

This report takes input parameters in the following two ways:

- Path driven reports - give access information on the selected paths by the selected users.
- Custodian driven reports - give information about paths on which user is assigned as custodian.

Inactive Folders

The Inactive Folders report displays a summary of the size of inactive folders on configured file servers and SharePoint Web applications and the count of files that these folders contain.The details table shows the last access time on an inactive folder. This report helps you monitor the folders which are not being accessed frequently, and identify potentially wasted storage on the file server.

This report takes input parameters in the following two ways:

- Path driven reports - give access information on the selected paths by the selected users.
- Custodian driven reports - give information about paths on which user is assigned as custodian.

Consumption Reports

Use the Consumption reports to view and export details of how storage on file servers is allocated and is being used. You can create these reports for all configured data repositories or for selected file servers, shares, SharePoint Web applications, or SharePoint site collections.

The Consumption reports help you identify the user accounts or departments that are placing the most burden on your storage resources. You can also use the information in the report to assign departmental charge back.

Each report contains a summary table. For each user or department, you can drill down the summary table to display statistics for the following parameters:

- The total space occupied by files created by the user.
- The total files created by the user.
- The name of the business unit to which the user belongs.
- The owner of the business unit.

Note the following about the information captured by the Consumption reports:

- Data Insight computes the number of records as the top N files based on the file size for every data owner or for every device path in the report input.

  For example, during report configuration the input path is one share, \\<Filer 1>\<Share 1> and the Number of records = 5.

  In this case the report computes the owner of each file on the share, and lists the top 5 files based on size for every data owner.

  Let us say Share 1 has total 30 files, such that 10 files are owned by UserA, 10 by UserB and 10 by UserC. In this case, the report displays 15 files. (The top 5 files based on size owned by UserA, UserB, and UserC.

For example, during report configuration the input path , \\<Filer 1>\<Share 1>, \\<Filer 1>\<Share 2>, and the Number of records = 10.

Let us say Share 1 has total 20 files, such that 10 files are owned by UserA and 10 by UserB.

Share 2 has total 20 files, 10 files owned by UserA and 10 files by UserC. In this case, the report displays the following output:. (The top 5 files based on size owned by UserA, UserB, and UserC for every share.

  - UserA: Top 10 files (files from Share 1+ files from Share 2 based on size)
  - UserB: Top 10 files (from Share 1)
  - UserC: Top 10 files (from Share 2)

- The report does not return deleted files and files with size 0KB in the output.
- For SharePoint file path, size on disk is not applicable; report will always return size on disk as zero.

Duplicate Files

Duplicate Files report helps you to identify the duplicate files within a given share. It enables you to take informed decisions about reclaiming storage. Note that duplicate file detection is per share only. Data Insight does not detect duplicate files across shares.

Two files are considered to be duplicate if they have the same logical file size and the same file extension. The 0-byte duplicate files such as shortcuts to the original files are ignored for the purpose of this report.

This report provides a graphical summary of the following:

- The extensions that are occupying the most physical disk space. The pie chart shows the total storage occupied by top ten file-extensions that contribute to largest duplicate sets.
- The potential storage that can be reclaimed by archiving or deleting the top ten extensions that contribute to the largest duplicate files. The pie chart shows the extension that will allow you to reclaim maximum storage, if remediated.

In the output, the duplicate paths are categorized by their file extensions. Additionally, the file extensions are sorted in the descending order of reclaimable storage. For a given file extension, the paths are further arranged in sets of related duplicates. For example, if `Foo1` and `Foo2` and `Foo3` are duplicates of each other, they belong to the same set of duplicates. These files are displayed in rows placed next to each other. Duplicate sets are sorted in the descending order of reclaimable storage space.

Consumption by Folders

The Consumption by folders report displays detailed information about the storage used by folders on configured file servers and SharePoint Web applications.

The report displays the following information about the folders selected in the report:

- The count of the active files that are contained in the folders.
- The amount of storage occupied by the active files in the folders.
- The size of the folder.
- The total count of files in the folder.
- The top **n** number of files in the folder sorted by size and file type.
- The column total of a file server or Web application.

The report includes information either for selected paths, or the first level children of the selected paths. If you select a partial DFS path for this report, Data Insight first expands the partial DFS paths to DFS links before it generates the report output.

This report takes input parameters in the following two ways:

- Path driven reports - give access information on the selected paths by the selected users.
- Custodian driven reports - give information about paths on which user is assigned as custodian.

Note the following about the computation of top N files that consume storage on a given device:

- Data Insight computes the number of records as the top N files based on the file size for every device path in the report input.
  For example, during report configuration the input path is one share, \\<Filer 1>\<Share 1>, the Number of records = 5, Folder Depth = Current Folder.
  In this case the report computes the the top 5 files under '/'.
- For example, during report configuration the input path , \\<Filer 1>\<Share 1>, the Number of records = 10 and the Folder Depth = Next-level subdirectories.
  In this case report will list down all directories present under given path along with ‘/’, total number of files, and total number of active files contained. Each directory path returns the Top 10 files present.
  The file count is always recursive.

Consumption by Department

The Consumption by Department report lists the departments in the enterprise in alphabetic order. For each department, the summary table shows the users who own the files or folders in that department, the total amount of space occupied by the files created by users in that department, the number of files. When creating an instance of the report, you can choose to map users to departments using the user's Active Directory domain or any other Active Directory attribute of the user.

You can drill down the summary table to view the detailed report. Click on the name of a custom attribute to view the detailed report. For example, if the report is sorted on the OU user attribute, clicking on the name of an organization unit in the summary table displays the following details for that organization unit. The detailed report displays the following:

- The users belonging to that OU.
- The Data Owner policy applied for computing the ownership.
- The name of the repository on which the files created by a user are stored.
- The path of files on the file server, or the URL or the SharePoint site.
- The size of each file.
- The access count for each file.

Consumption by File Group

The Consumption by File Group report displays a summary of the storage utilization on selected file servers and or on selected Web applications, sorted according to file groups. For each file group, the summary table shows the space used by files and the number of files.

You can drill down the summary table to view the detailed report. Click on a file group type to view the details of the space consumed by files in that file group. The detailed report displays the following:

- The file group type.
- The repository on which the file resides.
- The path to the file on the file server, or the URL or the SharePoint site.
- The size of the file.
- The date and time when the file was last accessed.

You can modify the default file groups that appear in the report. For more information on configuring file groups, see the *Symantec Data Insight Administrator's Guide*.

Consumption by Owner

The Consumption by Owner report displays a summary of the storage being used by files owned by configured user accounts. The owners of files are determined based on the activity on the files during the selected time period.

The report displays information about users and the storage being used by files they own. The report displays a table listing all configured user accounts, listed in the descending order of space used by the files owned by them. For each user, the summary table shows the number of active and inactive files owned, the files created, and the total amount of storage the files occupy.

You can drill down the summary table to view the detailed report. Click on the name of a user to view details of all the files owned by that user, the size of these files, and the access status of these files.

Consumption by File Group and Owner

The Consumption by File Group and Owner report displays information about the count and the size of files owned by configured users sorted according to file groups. The owners of files are determined based on the activity on the files.

For each file group, the summary table gives the break-down of the number of active and inactive files owned, the files created, and the total amount of storage the files occupy.

You can modify the default file groups that appear in the report. For more information on configuring file groups, see the *Symantec Data Insight Administrator's Guide*.

Create/Edit storage report options

Use this dialog to create an instance of a report. The options available on the page and their order depend on the type of report that you select.

Table 9-8 Create/Edit storage report options

Option	Description
Report Information	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Description** -A short description of the data contained in the report. ■ **Report Type** - The type of security report. This field is populated by default. ■ **Select resources using** - Select **Paths** or **Custodian Information** radio button. Depending on the selection, you can see the data selection or custodian selection option. **Note:** This field is available only in the following five reports : ■ Access summary report for paths ■ Data aging report ■ Inactive folders report ■ Path permissions report ■ Consumption by folders report ■ **Output Format** - Select the format in which you want to generate the report. You can select one or all of the given output formats. ■ **Maximum Reports to preserve** - Select the number of report outputs you want the system to preserve. The default value to preserve the report outputs is now unlimited. In case of scheduled reports, setting up value of this parameter to **Unlimited** may fill up disk space. Configure the value appropriately by taking disk space into consideration. ■ **Schedule** - Select the schedule at which you want the report to run. ■ **Copy output to** - Enter a path to copy report output files. To successfully copy a report output to an external computer, you must ensure that the **Secondary Logon** windows service is running in the Management Server. ■ **Select Credentials to access "Copy output to" path** - Select a credential from the drop-down menu, so that Data Insight can direct the report output to the specified location. Additionally you can use the option for adding a new set of credentials if the required credentials are not already added. The credentials must have folder-level read, write, create, and delete permissions on the external computer where the report output is copied. ■ **Overwrite option** - Selecting this option overwrites the earlier report output files. If you clear this check box, Data Insight creates a new folder with a report run ID for every report run, and saves the report in the new folder.

Table 9-8 Create/Edit storage report options *(continued)*

Option	Description
Configuration	

Table 9-8 Create/Edit storage report options *(continued)*

Option	Description
	Select the conditions to configure the report: ■ **Inactivity Period** - From the drop-down, select the duration of inactivity for files. Only the files that have remained inactive for the selected duration are included in the report. This field is only available for the Inactive users report. ■ **Bucket Size (Months)** - Enter the bucket interval that you want to include in the report. ■ **Include custom attributes of user** - By default, the check box is cleared. Select the check box to select the custom attributes from the drop-down list. For more information on configuring the custom directory attributes, see the *Symantec Data Insight Administrator's Guide*. ■ **Include data owner in report output** - Select the order of the criteria for computing the owner of the data. This field is available only for select report types. ■ **Activity Time Period** - Enter the time range for which you want data to be included in the report. Select **Duration** to indicate the last n hours/days/weeks/months/year. Select **Date Range** to specify a specific time range. ■ **Folder depth** - This option is available only for the Consumption by Folders report. Select the subfolder levels to be included in the report. This option is useful when you want to limit the total output in the report. ■ Select **Current Folder**, to include the information about only the selected paths. ■ Select **Next level sub directories** radio button to include information about the first-level children of the selected paths. ■ **Folder depth for selection of paths to report against** - Select the depth of subfolders to be included in the report from the drop-down list. This option is useful when you want to limit the total output in the report. From the drop-down, ■ Select **Current folder** to include information about only the selected paths. ■ Select **Specify Depth** and enter the level at which you want to include the folders. This filed is available only for the following reports: ■ Access Summary for Paths ■ Access Summary for Users/Groups ■ Enter the **No of records** you want to include in the report output.

Table 9-8 Create/Edit storage report options *(continued)*

Option	Description
	The report computes the number of records as the top N files based on the file size for every data owner, for every device path in the report input. From the top N files, (for example, in case of Inactive Folders report) the report will display the top N files that have remained inactive for the configured duration. The default is 25 records. In case of Consumption by folders report, this option appears only if you enable the check-box **Show details in reports**. ■ **Department mapping** - You can map the department through the options available in the drop-down list . The generated report maps the department on the basis of the option you choose. ■ **File type** - Enter comma-separated file type in this field. You can enter the file type in this field for the file group that is not pre-configured for the type of file you want to include in the report output. This option is available for the following reports: ■ Consumption by File Group ■ Consumption by File Group and Owner ■ Inactive Data by File Group ■ **File groups** - Select a file group from the drop-down list. This option is available for the following reports: ■ Consumption by File Group ■ Consumption by File Group and Owner ■ Inactive Data by File Group **Note:** You can select either a file type or a file group in the report output. ■ **Select columns to hide in output** - Select the columns that you do not want to display in the report. ■ **Truncate output if record exceeds**- Enter the number of records (rows) after which the report output is truncated. By default, the value you specify in this field applies to all the report types for whichData Insight supports truncation. See "Configuring a report to generate a truncated output" on page 148.

Table 9-8 Create/Edit storage report options *(continued)*

Option	Description
Data Selection	Do one of the following: 1 Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint Web applications. Or, select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. Or, select the **Containers** radio button to view the available containers that can be added in the report. Click the site, file server, share, folder within a share, or a DFS path to select it. The selected data set is listed in the **Selected resources** pane. 2 **Add resource** - Enter the resource path and click **Add** to include the path name in the report output. 3 You can also use a CSV file to import paths for creating reports. Click **Upload CSV**. On the pop-up, you can download the CSV template to review the input values and the format of the CSV file for that particular report. Only valid paths in the .CSV file are displayed in the **Selected Data** pane. Browse to the location of the CSV file and click **Upload**. This option is available for the following reports: ■ Access Details for Paths ■ Access Summary for Paths ■ Path Permissions ■ Entitlement Review

Table 9-8 Create/Edit storage report options *(continued)*

Option	Description
User Selection	From the list, click the user, group, or all users/groups radio button. The selected entities are listed in the Selected Users/Groups pane. You can type a name in the search bar to search for a user or group. You can also type a domain name in the Domain Filter field to narrow your search to users in a specific domain. **Note:** You can search for a particular Built-in user or group by using the Domain Filter. You can also filter a user or group from the Select Filter field. Select the All Filtered Users check box in the Selected Users/Group pane to include all filtered users in the report. You can also import user information using a .csv file for creating reports. Only valid paths in the .csv file are displayed in the **Selected Users/Groups** pane.
Exclusion List	Select the groups you want to exclude from the scope of the report. Click the group to select it. The selected data set is listed in the **Selected Groups** pane. **Note:** You can search for a particular Built-in user or group by using the Domain Filter.
Notification	Enter email addresses of users you want to send the report to. If the size of the attachment is above the configured limit, an email is sent without the attachment. You can configure the size of the attachment under **Settings** > **SMTP Settings.**
Remediation	Use this tab to instruct Data Insight to execute predefined actions on a report output. Select **Take action on data generated by report** to enable automatic processing of data generated by a report. Select any of the following: ■ **Archiving (Enterprise Vault)** - Select this option to archive data using Symantec Enterprise Vault. If you select this option you must specify a retention category and a post-processing action. ■ **Custom Action 1** / **Custom Action 2** - Select this option to specify a custom action defined by a custom script. See "About managing data using Enterprise Vault and custom scripts " on page 73.

About Data Insight custom reports

Sometimes the existing report types might not be adequate for creating reports according to your needs. For example, you might want to create a report having the name, size, active data size, openness, and number of active users for each share. In such situations, Data Insight enables you to create customized reports to suit your requirements. You can use the proprietary Data Insight Query Language (DQL) to generate such custom reports.

For more information about creating DQL queries, see the *Symantec Data Insight SDK Programmer's Guide*.

About DQL query templates

Data Insight provides you with built-in queries to help you write complex queries. At the time of creating a DQL report, you can select any of the built-in queries, and modify the content to suit your particular reporting needs. Additionally, you can create your own queries and save them to be used later as templates.

See “Creating custom templates for DQL queries” on page 137.

See “Creating a report ” on page 87.

Data Insight provides the following default query templates:

Table 9-9

Category	Name	Description
Data Management	Folder creation details	The query fetches the details about the creator and the date of creation for every first-level folder in the environment.
Data Management	All files with a specific extension	The query fetches details of files with specific extensions in your storage environment. You can use this query to find, for example, all media files. The query helps you find data that does not comply with your organization's policy, and reclaim storage on your device. Modify the template to add other extensions to get results that suit your needs.
Data Management	Files in a confidential folder	The query lists all the files under a specified folder in a share. In this example, the folder has the word "confidential" as part of its name. Modify share name and folder name search criterion to get results that suit your needs.

Table 9-9 *(continued)*

Category	Name	Description
Data Management	Files with undefined file group	The query lists all the files under a specified share that are not defined in Data Insight file groups. You can analyze these files and update the file groups for better reporting of consumption patterns.
Data Management	Folder summary by file type	The query fetches the folder level summary of counts and size used by different file-types in a share. Only the files which are direct member of a folder will be used for computation. Only those file-types that are part of Data Insight file groups will be listed. For all other file types, it will be combined under empty "" file type. Modify the share name to get results that suit your needs.
Data Management	Stale file list	The query lists the files that have not been accessed for the past one year. You can use this report to make better archiving decisions. Modify the duration and the share name to get the results that suit your needs.
Data Management	Storage usage by user attribute	The query lists the consumption of storage on NAS devices based on the user attribute, department. The consumption is determined by calculating the owner of the file and mapping the owner to the corresponding department. Modify the filer name and user attribute to get the results that suit your needs. Additionally, you can modify the owner calculation by specifying access dates and order of the policy for computing the data owner.

Table 9-9 *(continued)*

Category	Name	Description
Risk Analysis	Sensitive files on a filer	The query lists all files which are marked sensitive by the Symantec Data Loss Prevention (DLP). These files can be further analyzed and acted upon as per organization's security measures. If DLP is configured and incidents are reported against a configured report ID, this report lists the sensitive files automatically. Alternatively, you can import sensitive file information to Data Insight using a CSV file. Modify the device name with valid filer name in your environment to get the results that suit your needs.
Risk Analysis	Sensitive files that are active	The query lists all the active sensitive files that violate a certain DLP Policy. In addition to file details, it also provides you the information on the number of active users on the files. Modify the activity period and policy to get the output that is valid for your environment.
Risk Analysis	Sensitive files with violated policies	The query lists all the sensitive files in a share and the associated DLP policy that are violated. Modify the share name to get the output that is valid for your environment.
Risk Analysis	Department-wise summary of risky behavior	The query fetches the summary of the users belonging to other departments who have assessed sensitive files owned by a specific department. For example, you may want to know the users belonging to any non-HR department accessing files owned by the HR department. This query computes the potentially risky behavior on a specific share during a specific time range. The files are classified as being sensitive by DLP policies. Note that sometimes the report may flag legitimate accesses as risky behavior. Use your discretion to eliminate such false alarms. Modify the share name, time range, DLP policy string, user department attribute, and department name in the query to get valid results in your environment.

Table 9-9 *(continued)*

Category	Name	Description
Risk Analysis	Recent suspicious activity	This query fetches the details of the inactive sensitive files that were accessed recently. For example, it can get the list of sensitive files that were inactive for last year but were accessed in last 5 days. It also provides you the information about the person who accessed the file most recently. The sensitive file information is fetched from DLP. Alternatively, you can import sensitive file information to Data Insight using a CSV file. Modify the recent access time range and inactivity time range in your environment to get results that suit your needs.
Forensics	Share access details	This query provides the audit details on a share for a specified time range. Modify the time range and share name to get results specific to your environment.
Forensics	User access details	The query provides the details of accesses by a specified person on a share during a specified time range. Modify the person name, time range, and share name to get the results to suit your needs.
Forensics	Top users of sensitive files	The query lists top ten users who have accessed sensitive files in your storage environment within a specified time-range. Modify the time range to get valid result in your environment.
Forensics	Folders with maximum access counts	The query fetches the list of top ten folders that are accessed in a share during a specific time range. Modify the share name and time-range to get valid result in your environment.
Forensics	Users with maximum access counts	The query fetches the list of top ten users who have accessed a share during a specific time range. Modify the share name and time-range to get valid result in your environment.

Table 9-9 *(continued)*

Category	Name	Description
User / Group Management	Group membership details	The query provides the details about a specified security group, its member groups, and users in the group. Modify the group name and domain name to get the results that are valid for your environment.
User / Group Management	Deleted or disabled groups	The query lists all the disabled or deleted security groups in the environment.
User / Group Management	Deleted or disabled users	The query lists all the disabled or deleted users in the environment.
User / Group Management	Groups with disabled users	The query lists all the groups with disabled users in the environment.
User / Group Management	Empty groups	The query provides a comma-separated list of security groups, their details and SIDs of its member users. To list the empty groups for clean-up, execute following query on the output: `SELECT * FROM groups WHERE memberusers_sid = "`
User / Group Management	Circular groups	The query lists any security groups in the environment which are members of each other forming group loopings.
Data Protection	Open shares	The query lists all paths in your environment that have excessive permissions along with the reasons for their openess.
Data Protection	Shares with permissions to Everyone group	The query lists shares in the environment that have permissions to the "Everyone" group.
Permission Management	Paths with direct permissions to disabled users	The query provides the details about the paths that have explicit access to disabled users.

Creating custom templates for DQL queries

To create custom templates for DQL queries:

1. Create a text file with the following information on separate lines:

   name: <The name of the query template>

   desc: {<The description of the query template>}

   version: <The Data Insight version for which the query template is valid>

   category: <The category to which the query belongs. For example: Data Management, Forensics etc.>

   query:{<The DQL query text>}

   Note: The desc, the version and the category information are optional. The curly braces in the desc line can be omitted in case of single line descriptions.

2. Give the file a suitable name and save it with a `.template` extension at the following location on the Management Server:

   `<DATADIR>/templates/dql`

Create/Edit DQL report options

Use this dialog to create an instance of a report.

Table 9-10 Create/Edit DQL report options

Option	Description
Report Information	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Description** - A short description of the data contained in the report. ■ **Report Type** - This field is pre-populated as DQL Report by default. ■ **Output format** - Click the check-box to indicate that you want the report output in a CSV file. ■ **Maximum Reports to preserve**-Select the number of report output you want the system to preserve. The default value to preserve the report output is *unlimited*. ■ **Schedule** - Select the schedule at which you want the report to run. ■ **Copy output to**- Enter a path to copy report output files. To successfully copy a report output to an external computer, you must ensure that the **Secondary Logon** windows service is running in the Management Server. ■ **Select Credentials to access "Copy output to" path** - Select a credential from the drop-down menu, so that Data Insight can direct the report output to the specified location. Additionally you can use the option for adding a new set of credentials if the required credentials are not already added. The credentials must have folder-level read, write, create, and delete permissions on the external computer where the report output is copied. ■ **Overwrite option** - Selecting this option overwrites the earlier report output files. If you clear this check box, Data Insight creates a new folder with a report run ID for every report run, and saves the report in the new folder.

Table 9-10 Create/Edit DQL report options *(continued)*

Option	Description
Query	

Table 9-10 Create/Edit DQL report options *(continued)*

Option	Description

	Write your DQL query in the space provided.
	You can provide multiple DQL queries separated by a space or a newline. This creates a DQL output with multiple tables for corresponding to each DQL queries.
	While writing the query you must adhere to the syntax and guidelines of the Data Insight Query Language(DQL).
	For more information about creating DQL queries, see the *Symantec Data Insight Programmer's Reference Guide*.
	Click **Use Template** to use the queries provided by Data Insight as templates. Using the drop-down lists select a category and a template. Once you have selected a template, you can edit it as per your needs.
	See "About DQL query templates" on page 132.
	You can use a CSV file to feed a bulk input to a query. Click **Choose file** to browse to the CSV file containing the bulk input and click **Upload** the file.
	For details on how to use the content of CSV file as arguments in a query, refer *Symantec Data Insight Programmer's Reference Guide.*
	Optionally, click **Advanced Options** > **Run SQL commands on generated DQL output database**. This displays a text area where you can type the SQL commands that enable you to access and manipulate the DQL output database. The feature enables you to do the following:
	■ Create new tables.
	■ Delete tables from the report output.
	■ Insert data from existing tables in the output database into new tables.
	■ Use CASE statements in SQL.
	■ Create indexes on tables before performing joins.
	Click **View empty DQL output database schema** to view the schema of the tables which will be generated by DQL.
	Click **Check DQL syntax** to view syntax errors for your DQL query.
	Following is an example of a query that you can write to get a report that provides the distribution of files and storage per extension in a share. Replace <*Share Name*> with the name of the share in your environment.
	DQL Query
	`from path`
	`get extension, count(extension), sum(size)`

Table 9-10 Create/Edit DQL report options *(continued)*

Option	Description

	`where path.msu.name = “<Share Name>"`
	`and type = "file"`
	`and isdeleted = 0`
	`group by extension`
	Advanced Options
	`create table Cap_EXT(path_rowid INTEGER, extension TEXT, no_files INTEGER, size_MB INTEGER);`
	`insert into Cap_EXT`
	`select path_rowid, COALESCE(NULLIF(extension,''), 'Unclassified File Group') , "count(extension)",`
	`round("sum(size)"/1024.0/1024.0, 2) from path`
	`order by "sum(size)" desc;`

Notification	Enter email addresses of users you want to send the report to. If the size of the attachment is above the configured limit, an email is sent without the attachment. You can configure the size of the attachment under **Settings** > **SMTP Settings.**
Remediation	Use this tab to instruct Data Insight to execute predefined actions on a report output. Select **Take action on data generated by report** to enable automatic processing of data generated by a report. Select any of the following: ■ **Archiving (Enterprise Vault)** - Select this option to archive data using Symantec Enterprise Vault. If you select this option you must specify a retention category and a post-processing action. ■ **Custom Action 1** / **Custom Action 2** - Select this option to specify a custom action defined by a custom script. See “About managing data using Enterprise Vault and custom scripts ” on page 73.

Considerations for importing paths using a CSV file

The following considerations apply when you import paths for a report using a CSV file:

- When using a CSV file to upload paths, specify the path name along with the input type in the file. The input type enables Symantec Data Insight to classify the paths.

  For example, `http://sharepoint1/sites/Marketing, SiteCollection`.

  Symantec Data Insight supports the following input types:

  - Filer
  - DFSFiler
  - WebApp
  - DFSPathPartial
  - Share
  - DFSPathLink
  - SiteCollection
  - Folder
  - Site
  - File

  For more information, see https://www.veritas.com/support/en_US/article.000107668.

- Ensure that the paths in the CSV do not have double quotes (for example,`\\filer1\share1\foo\bar”kkk.txt`) as they will not be uploaded for the report configuration.

Chapter 10

Managing reports

This chapter includes the following topics:

- Viewing report details
- Filtering a report
- Editing a report
- Copying a report
- Running a report
- Customizing a report output
- Configuring a report to generate a truncated output
- Sending a report by email
- Automatically archiving reports
- Canceling a report run
- Deleting a report

Viewing report details

On the Reports listing page, you can view the following details:

- The name of the report.
- The last successful output formats of the report.
- The status of the report at the time of the last run.
- The date and time of the last run.
- The user account that created the report.

- The date and time the report was created.
- The report run ID column.

Note: The Reports tab is visible only to those users who have the View privilege on.

To view the Data Insight report details

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Click a category to view the types of reports in that category.
3. Click a report type to view the configured reports of that type.
4. From the **Select Action** drop-down, click **View** to view details of a particular report.

   On the report details page, you can view the input parameters that are given to run the report. You can also download a report output from this page.
5. From the **Select Action** drop-down, click **View Report progress** to view the granular details of the progress of the last report run.

   You can view the progress of the report under the following tabs:

   - **Overview**- Displays the following:
     - The step level details of the report execution.
     - The latest messages from the Indexers nodes for each of the report execution steps.

     From the Overview tab, you can gain real-time feedback on steps for a report and the speed of execution. This information can help you to estimate the time remaining to generate a report.
   - **Details** - Displays the following:
     - The messages from the Indexers nodes involved in report execution arranged in a table.
     - Details such as the Indexer node names, the report execution steps, and the duration of the execution steps.

     From the Details tab, you can monitor the nodes involved in the execution of a report and the time consumed for executing the steps. This information can help you to identify the bottlenecks of report execution.
6. Optionally, select **Auto Refresh** to automatically refresh the progress details every 10 seconds.

See “About stale information in reports” on page 145.

About stale information in reports

When a report is run, Data Insight indicates in the report output those paths for which the audit or metadata information is likely to be stale. Data Insight tracks the time of the last metadata scan/audit that was processed by the Indexer. If the last metadata scan for a path processed by the Indexer is older than 7 days, or the last audit processed is older than 5 days, the report output warns the user about the potentially stale information in the output.

If metadata has not been recently updated, it could mean that the information about paths (lsuch as size, permissions) in the report output might not be up-to-date or missing all- together. Similarly, if audit events have not been processed for some time, it could mean that the audit details in the report output or the ownership calculations that depend on audit activity of users may not be accurate.

You can disable stale information warnings if required by setting the following global property:

```
matrix.reports.stale.index.warning.enabled Value: true/false
```

Similarly, you can configure the allowable limit of stale data in the report output by setting the following global property:

```
matrix.reports.stale.index.warning.days.scan Value: Grace period in days
```

To set the global property

◆ Issue the following command on the Management Server:

```
configdb.exe -O -J <name> -j <value>
```

For example:

```
configdb.exe -O -J matrix.reports.stale.index.warning.enabled -j
false
```

Filtering a report

When you click on the **Reports** tab, the home page displays by default.

The Reports home page lists all the available reports for the logged in user. You can perform all reports-related tasks from the home page except creating new reports.

Use the filter on the Reports home page or list page to search for reports on the basis of report name or report run status. To filter a report on the basis of report status, you must specify the entire report status string for example, success, failure, partial success, or cancelled.

Editing a report

After you create an instance of a report, you can edit the input parameters for generating a report. For example, you might want to edit the users or paths that are selected for the report. Or you might want to change the schedule to run the report.

To edit a report

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Select the report you want to edit, and in the **Select Action** drop-down, click **Edit**.
3. On the Edit report screen, make the necessary changes.
4. Click **Save**.

Copying a report

You can make a copy of a report from a report that is already created.

To copy a report:

1. Click the **Reports** tab of the Data Insight Management Console. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Select the report you want to copy, and in the **Select Action** drop-down, click **Copy**.
3. In the dialog box enter a name for the copy of the report.
4. Click **Copy**.

Running a report

On the Reports home page, select the report that you want to run. Every report is generated at the schedule that you specify at the time of creating the report. However, you can also generate a report without waiting for the scheduled run.

To run a report

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Do one of the following:
   - Click the check box next to the report to select multiple reports, and click **Run**.
   - Or, select the report that you want to generate. In the **Select Action** drop-down, click **Run**.
3. You can view the progress of the report run on the Reports listing page.

By default, you can run two reports at a time. You can configure this value to execute more than two reports at one time. For details, see the *Symantec Data Insight Administrator's Guide*.

To view the details of the steps that are involved in running the report, view the report execution log.

To view the report execution log

1. On the Reports listing page, select the report for which you want to view the log of the latest run of the report.
2. In the **Select Action** drop-down, click **View Report Progress**.
3. On the panel that displays the log, you can view the following information:
   - The various steps executed to generate the report.
   - The success or failure of each step.
   - The node on which the step is executed.
   - The time taken to execute each step.
4. To download the detailed log files for each report run, click the **Download Log** icon located at the bottom of the panel.

   The **Download Log** icon is enabled only after the report execution is complete or cancelled.
5. Click **Save File**.

   The compressed folder contains the log files for each node on which the report run is executed.

Customizing a report output

Data Insight enables you to rename the default column names for the reports you want to generate. For any report type, you can rename its default column names by creating and editing the properties file for that report type.

To customize a report output header

1 Create a `<Report_name>_header.properties` file corresponding to the report type, where *<Report_name>* denotes the report type name. For those reports whose name contains the term *user/group*, replace the slash(/) with a dash(-). For example, while naming a properties file for the report type *User / Group Permissions*, name it as *User - Group Permissions_header.properties*.

   For example, name the properties file for the *Access Details for Paths* report as *Access Details for Paths_header.properties*.

   The content of the *header.properties* file is as follows:

   ```
   #
   # Custom Header information
   # version 1.0
   #
   DFS\ Path=DFS
   Path\ Name=PATH
   BU\ Name=BUName
   BU\ Owner=BUOwner
   ```

   In the example, the value at the left-hand side of the equal sign is the default name of the column for in a report. Insert the (\) character before a single space, to represent a space in the default column name. The value at the right-hand side is the modified title for the column.

2 Save the properties file on the Data Insight Management Server at `C:\DataInsight\data\console\reports\customHeaders`.

Configuring a report to generate a truncated output

A Data Insight report can contain any number rows based on the report type and its input parameters. A report having an large number of rows can have significant overheads for system resources. You can avoid this overhead, by truncating the report to include only a specified number of rows (records).

You can truncate only the following reports:

- Capacity reports.

- DQL reports.
- Data Inventory reports.

You can specify a value to truncate the report outputs for all the supported report types.

To set a global value to truncate all report types

1. On the Data Insight Management Server, navigate to `C:\Program Files\Symantec\DataInsight\bin\.`
2. Open the `reportcli.vmoptions` file in a text editor.
3. Set the value for the argument*, Dreport.details.limit*, with the desired number of records.
4. Save and close the file.

You can also specify a truncation value for a report type which overrides the global truncation value for that report types.

To truncate a particular report type

1. In the Data Insight Management Console, click **Reports**.
2. From the left-hand side pane, click the report you want to generate. The **Reports** listing page displays a list of already generated reports, if any.
3. Click **Create Report**.
4. Click **Configuration**.
5. In **Truncate output if record exceeds** field, specify the maximum number of rows after which you want the report to be truncated..
6. Click **Save**.

Once you configure a report to have a truncated output, the report instance on the **Reports** listing page displays a warning icon under the **Last Run Status** column. Hover your mouse pointer over the warning icon to view the total number of rows that the report would normally contain if no truncation value was specified.

You can modify the truncation value directly from the report listing page and regenerate the current instance of the report. Additionally, you can save setting to be applied for all the future instances of the report.

To modify the truncation value for regenerating a report instance

1. In the Data Insight Management Console, click **Reports**.
2. Click the report type to view the listing page for that report type. It displays the generated instances of the report. The report instance with truncated records displays a warning icon under its **Last Run Status** column.

3 Click the report instance for which you want to modify the truncation value.

4 Click **Select Action**.

5 Click **Regenerate Output**.

6 Enter the new value for the maximum row count for the report.

7 Select **Save settings for future reports** to apply the settings for all the future instances of the report.

8 Click **Generate Output** to generate the report with the revised row count.

Sending a report by email

In addition to displaying the reports in the Console or exporting the contents of the report in your chosen output format(s), you can also send them by email. This feature is useful, for example, for providing operators or administrators with information they need for troubleshooting.

Note: Before you can send report data by email, an SMTP server must be configured for this purpose. For details on specifying an SMTP server for emailing reports, see the *Symantec Data Insight Administrator’s Guide*.

To send a report by email

1 Do one of the following:

- When creating a report, specify the email addresses of the recipients who you want to send the reports. The output is emailed to these recipients each time a report is generated.
- Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
  If you want to send the latest report output through email, on the Reports home page, select the report, and in the **Select Action** drop-down, click **Email Latest**.

2 In the **Email report** popup, enter the email addresses of the recipients.

3 Click **Send**.

4 To email an older report output, in the **Select Action** drop-down, click **View**.

5 On the **Report Details** page, click the **Email** button adjacent to the report output you want to email.

6 Enter the email addresses of the recipients, and click **Send**.

Click the download report link in the received email to download the report output. You can disable this feature by setting the appropriate global properties.

Automatically archiving reports

For all the report types which support archiving actions, you can configure Data Insight to automatically archive a report once the report generates successfully. You can configure the following actions on the **Post-Processing Action** tab:

- Select a retention category on the archived data to indicate how long the data must be stored.

  Note: You must first select the data source from the **Data Selection** tab before you select any retention category.

- Select a post-processing action, such as deleting the original file and replacing it with a shortcut. The shortcut points to the new file location inside the archive.

Archiving is supported for the following types of reports:

- **Access Details** reports.
- **Access Summary** reports.
- **Custom** reports.
- **Data Lifecycle** reports.

To automate the archiving of reports:

1 In the Create Report wizard, navigate to the **Post-Processing Action** tab.

2 Select the **Take action on data generated by report** check box.

3 Select any of the following three options:

   - **Archiving (Enterprise Vault)** - Select this option to archive data using Symantec Enterprise Vault. If you select this option you must specify a retention category and a post-processing action.
   - **Custom Action 1** - Select this option to specify a custom action defined by a custom script.
   - **Custom Action 2** - Select this option to specify a second custom action defined by a custom script.

Note: To know more about how to define a custom action by using a custom script, refer to *Symantec Data Insight Administrator's Guide*

See “About Retention categories” on page 74.

See “About post-processing actions” on page 75.

Canceling a report run

You can cancel the generation of a report that is already in-progress.

To cancel a report run

1. Do one of the following:
   - On the Reports home page, select the report, and in the **Select Action** drop-down, click **Cancel**.
   - On the **Progress View** panel, click **Cancel** .

   See “Running a report” on page 146.
2. The last run status on the Reports listing page displays the status of that report as **Canceled**.

Deleting a report

You can delete an instance of a report and all generated report outputs.

To delete a report

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Click a report type to view the instances of the report.

   A list of all instances for that report type appears in the content pane.
3. Click the check box next to the report to select multiple reports, and click **Delete**.

   Select the report you want to delete, and in the **Select Action** drop-down, click **Delete**.
4. Click **OK** on the confirmation message.

Appendix A

Command Line Reference

This appendix includes the following topics:

- mxcustodian

mxcustodian

`mxcustodian` – A script that is used to automatically assign custodians on various paths and to generate a comma separated values (csv) file with information about data custodian assignments. The `.csv` files, `mxcustodian_assign.csv` and `mxcustodian_error.csv` are saved in the current directory.

SYNOPSIS

```
mxcustodian.exe --paths <pathsfile> --ownermethod <comma-separated-list>
|default
```

```
mxcustodian.exe --paths <pathsfile> --groupscript <script>
--attr <attrname>
```

```
mxcustodian.exe --csv <csv-filepath> --verify
 [--custodian <user@domain>|<SID>]
```

```
mxcustodian.exe --csv <csv-filepath> --assign [-f] [--overwrite]
```

```
mxcustodian.exe --csv <csv-filepath> custodian
<user@domain>|<SID> --assign [-f] [--overwrite]
```

OPTIONS

`- -csv`*<name of input file>*

A file with comma-separated values — path, custodian. The values are provided in the format, one path per line. The given custodians are assigned to their corresponding path.

`- -assign`

Assigns custodians given in the input csv file.

`- -custodian` *<name of custodian>*

A user@domain or SID value to be assigned as custodian to all input paths. Input paths must be specified using – –csv option where the file provided contains one path per line.

`- -paths` *<input file>*

Input file with paths, one path per line. Depending on the method used, the computed custodians for the paths will be printed to the output file, `assignments.txt`.

`– –overwrite`

Overwrites existing custodian assignments with the assignments provided in the input csv file (using – –csv option). By default, Data Insight appends the custodian assignments in the input file to the existing assignments.

`–g – –groupscript`

Invokes the script for each path <*name of path*> in the input file given by the --csv option. The script is passed one path per invocation and prints to its standard output a group, <*name of group*>, corresponding to that path. If the script exits with 0, denoting success, the output group is used. If the script exits with a non-zero value, the path is discarded. The next input path is picked up if `--force` option is used; else this script aborts further execution

Note: When using the “--groupscript” option, you must keep the actual script in the folder `data/scripts/mxcustodian/`. When specifying the parameter for the --groupscript option on the command line, you must specify the fully-qualified path to the script.

Once a group for a path is obtained, the script does the following in the given order:

- Queries the directory service to get the value for the attribute for the group. The attribute can be specified using the `--attr` option.
- Generates a file containing the path and attribute entries, one entry per line.

`–f – –force`

Ignores paths that do not have a corresponding custodian specified in the input csv file, and assigns custodians for other valid paths. This option also prints all error paths in the log file.

`–a – –attr <`*`name of attribute`*`>`

Attribute whose value specifies the custodian for a given path. Use this option with the – –groupscript option.

`– –ownermethod default|<`*`one or more comma-separated list of methods`*`>`

The supported methods of computing an owner in their default order (if a default order is specified) are rw_count, read_count, write_count, creator, last_accessor, last_modifier OR 'parent_owner,<*M*>' where M is the default or any number of comma-separated methods.

– –ownermethods are calculated based on the last 3 months data/time range.

`– –verify`

Verifies and validates input paths and custodians provided using – –csv option. This command does not make any custodian assignments.

`– –outfile<`*`name of the file`*`>`

Name of the file where the results of successful custodian computation, verification, or assignments is stored. If the file name is not specified, the results go to the standard output of the command.

`– –errfile `*`name of the file`*

Name of the file where the errors in custodian computation, verification, or assignments is stored. If the file name is not specified, the results go to the standard error output of the command.

`–f – –ignore_errors`

Ignores paths that do not have a custodian in the input csv file and assigns the custodians for other valid paths. Prints all such error paths in the log file.

`–D – –debug`

Prints additional debug statements in the log file.

`–h – –help`

Prints the usage information for this command.

Index

A

access pattern map 56

accessibility
  Management Console 20
  tabs 21
  tools 21

Archiving
  using Enterprise Vault 73

archiving
  by using reports 77
  inactive subfolders 76
  post-processing actions 75
  retention categories 74

audit logs
  overview 17

C

Considerations
  uploading CSV file 142

considerations
  importing path 142

D

data custodian
  overview 14

F

folders
  assigning active user as custodian 52
  assigning custodian 51

M

Management Console
  logging in 23
  logging out 24
  operation icons 22

O

overview
  access information for users and groups 33
  managing data custodian 46
  migrated domains 18
  viewing access information for folders 33, 45

P

permissions
  assigning custodian 52
  overview 15

R

report
  truncate 148

reports
  cancelling generation 152
  copying 146
  creating 87
    DQL report dialog options 137
    permission search
    See also permissions query template
    security report dialog options 108
    storage report dialog options 125
  customizing column names 148
  deleting 152
  editing 146
  filtering 145
  generating 146
  overview 86
  send by email 150
  storage 117
  type
    custom 132
    security 88
    storage 116
  viewing 143

S

saving
- CSV file 86
- HTML file 86
- PDF file 86

security
- Access Details 88
- Access Summary 117
- ownership reports 106
- Permissions 89

sharepoint permissions
- overview 16

Symantec Data Insight
- overview 11

V

viewing
- attributes of a group 63
- attributes of a user 62
- attributes of file or folder 46
- folder activity log 56
- report execution log 146
- reports 143
- user access details 71
- user activity on folders 65

viewing folder activity
- by time 53
- for inactive subfolders 53
- for subfolders and files 53

viewing permissions
- effective permissions 54
- File System Access Control List 54
- for groups 68
- for users 66
- share-level permissions 54

viewing user activity
- active users 50
- inactive users 50
- overview 50