

Symantec Data Insight User's Guide

4.5

Symantec Data Insight 4.5 User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

4.5

Documentation version: 4.5 Rev 0

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

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

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

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

| | |
|---------------------------------|--|
| Asia-Pacific and Japan | customercare_apac@symantec.com |
| Europe, Middle-East, and Africa | semea@symantec.com |
| North America and Latin America | supportsolutions@symantec.com |

Contents

| | |
|-------------------------|---|
| Technical Support | 4 |
| Chapter 1 | Introducing Symantec Data Insight 11 |
| | About Symantec Data Insight 11 |
| | About data custodian 14 |
| | About audit logs 15 |
| | About permissions 16 |
| | About SharePoint permissions 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 20 |
| | 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 23 |
| | Accessing online help 23 |
| Chapter 3 | Navigating the Workspace tab 24 |
| | About the navigation pane 24 |
| | Searching the storage device hierarchy 24 |
| | Searching for users and user groups 25 |
| | Filtering users and user groups 26 |
| Chapter 4 | Viewing access information for files and folders 28 |
| | About viewing file or folder summary 28 |
| | Viewing the overview of a data repository 29 |

| | | |
|-----------|---|----|
| | Managing data custodian for paths | 30 |
| | Viewing the summary of user activity on a file or folder | 32 |
| | Viewing user activity on files or folders | 32 |
| | Assigning an inferred data owner as custodian | 34 |
| | Assigning an active user as custodian | 34 |
| | Assigning a custodian from the Permissions tab | 34 |
| | Viewing file and folder activity | 35 |
| | Viewing CIFS permissions on folders | 36 |
| | Viewing NFS permissions on folders | 37 |
| | Viewing SharePoint permissions for folders | 37 |
| | Viewing audit logs for files and folders | 37 |
| | About visualizing collaboration on a share | 39 |
| | Analyzing activity on collaborative shares | 40 |
| | About the Context Map view | 42 |
| | About control points | 43 |
| | Viewing advanced analytics for a path | 43 |
| Chapter 5 | Viewing access information for users and user groups | 46 |
| | Viewing the overview of a user | 46 |
| | Viewing the overview of a group | 47 |
| | Managing custodian assignments for users | 47 |
| | Viewing folder activity by users | 49 |
| | Viewing CIFS permissions for users | 50 |
| | Viewing CIFS permissions for user groups | 51 |
| | Viewing NFS permissions for users and user groups | 52 |
| | Viewing SharePoint permissions for users and user groups | 52 |
| | Viewing audit logs for users | 53 |
| Chapter 6 | Viewing permission recommendation on paths | 56 |
| | About recommending permission changes | 56 |
| | Reviewing permission recommendations | 57 |
| | Analyzing permission recommendations and applying changes | 57 |
| Chapter 7 | Managing inactive data | 59 |
| | About managing data using Enterprise Vault and custom scripts | 59 |
| | About Retention categories | 60 |
| | About post-processing actions | 61 |
| | Managing inactive data from the Folder Activity tab | 61 |
| | Managing data from the Context Map view | 62 |

| | | |
|------------|---|-----|
| | Managing inactive data by using a report | 63 |
| Chapter 8 | Using the Self-Service Portal | 65 |
| | About the Self-Service Portal | 65 |
| | What you can do with the Self-Service Portal | 66 |
| | Logging in to the Self-Service Portal | 67 |
| | Using the Self-Service Portal to review user entitlements | 68 |
| | Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents | 69 |
| | Using the Self-Service Portal to confirm ownership of resources | 70 |
| Chapter 9 | Using Data Insight reports | 72 |
| | About Data Insight reports | 73 |
| | About Data Insight security reports | 73 |
| | Access Details report | 74 |
| | Permissions reports | 74 |
| | Ownership Reports | 76 |
| | About Data Insight storage reports | 78 |
| | Access Summary reports | 79 |
| | Capacity reports | 79 |
| | Data Lifecycle reports | 80 |
| | Consumption Reports | 83 |
| | About Data Insight custom reports | 86 |
| | About DQL query templates | 86 |
| | Creating custom templates for DQL queries | 91 |
| | Viewing report details | 91 |
| | Filtering a report | 93 |
| | Creating a report | 93 |
| | Create/Edit security report options | 94 |
| | Create/Edit storage report options | 105 |
| | Create/Edit DQL report options | 114 |
| | Editing a report | 116 |
| | Copying a report | 117 |
| | Running a report | 117 |
| | Customizing a report output | 118 |
| | Configuring a report to generate a truncated output | 119 |
| | Sending a report by email | 121 |
| | Archiving of reports automatically | 122 |
| | Canceling a report run | 123 |
| | Deleting a report | 123 |
| Appendix A | Command Line Reference | 124 |

mxcustodian 125

Index 128

Introducing Symantec Data Insight

This chapter includes the following topics:

- [About Symantec Data Insight](#)
- [About data custodian](#)
- [About audit logs](#)
- [About permissions](#)
- [About SharePoint permissions](#)
- [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 15.
- 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 16.

See [“About SharePoint permissions ”](#) on page 17.

- 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 59.

- 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 Context Map view”](#) on page 42.

See [“About visualizing collaboration on a share”](#) on page 39.

- Permission recommendations

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

See [“About recommending permission changes”](#) on page 56.

- 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.

See [“About the Self-Service Portal”](#) on page 65.

- 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 30.

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 125.

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

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 sub-folders 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 - The security event is logged when the access control entries of a file or folder are changed. This event helps to identify who changed the permissions.
- The access timestamp
- The IP address of the machine that the user has generated the access activity from.

You can use these access events for the following purposes:

- 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 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 37.

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 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*.

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. It consists of a header, a set of tabs, 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:

- **Dashboard:** View information about the activity, storage, and security statistics for the devices that are being monitored by Data Insight.
- **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

On the left side of the Symantec Data Insight Management Console window, the navigation pane gives you quick access to specific information depending on the tab you have selected. For example, on the Workspace tab, you can view a list of folders, users, user groups or on the Settings tab you can view the list of the settings required to configure Data Insight.

Content pane








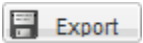



The Symantec Data Insight Console's main display area, or content pane, displays information about folders, files, users, configuration data, and events. The information displays in a variety of tabular and graphical formats. You can also perform tasks like exporting data to a file and emailing the data 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 filters, 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 <code>.csv</code> file. |
|  | Exports all data on the current screen to a <code>.csv</code> file. |
|  | Submits request to the Enterprise Vault server to archive the selected folders. |
|  | The action selector icon displays a menu with the following two options: <ul style="list-style-type: none">■ 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. The management console prompts you to confirm the logout.
- 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 navigation pane](#)
- [Filtering users and user groups](#)

About the navigation pane

The navigation pane is on the left side of the Symantec Data Insight Management Console window. It gives you quick access to specific information depending on the tab you have selected. For example, on the **Workspace** tab, you can view a list of folders, users, user groups or on the **Settings** tab you can view the list of the settings required to configure Data Insight.

See [“Filtering users and user groups”](#) on page 26.

Searching the storage device hierarchy

.

From the **Workspace** tab of the Data Insight Management Console, you can view the detailed information about the access pattern for files, folders, and web applications.

You can view the attributes of a file or a folder located on a filer, SharePoint site, or web application on the **Folders** tab in the navigation pane.

You can navigate shares, sites, and folder hierarchy.

To navigate the folder hierarchy

- ◆ Do one of the following:

- Click the filer, or web application to view the **Overview** tab.
- Drill down the filer or web application hierarchy in the navigation pane. When you are at a particular level in the hierarchy, you can filter the list of children using the search bar at the top of the pane.
- 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.
- Use the global search at the top right of the content pane area to look for a particular site collection, share, group, or user.

See [“Viewing the overview of a data repository”](#) on page 29.

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 **Workspace** tab of the Data Insight Management Console.

In the **Workspace** tab, click the **Users** or **Groups** sub-tab in the navigation pane on the left to view list of users or groups.

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

- To search for users or groups in a specific domain, enter the name of the domain in the **Domain Filter** search bar. To clear domain filter selection, remove the domain name, and press Enter.
Use the **Domain Filter** search bar 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.
- To search for users or groups based on their attributes, click in the **Filter User by Attribute** field, add a filter in the Advanced filter pop-up, and click **Go**.
- Enter the name of the user or group in the search bar to search for a user.

- To search for a user or user group on the basis of display or login name, right-click a user or a group, and select **Show Login Name** or **Show Display Name** as the case may be.
- To search for a user or a group by using its security identifier (SID), enter the SID value in the Go to bar located under the **Workspace** tab of the Management Console.

See [“Viewing the overview of a user”](#) on page 46.

See [“Viewing the overview of a group”](#) on page 47.

Filtering users and user groups

You can search for users and user groups based on their attributes, domain, or using the predefined filters. The following predefined filters are available for selection:

- Custodian Users - Displays only those users who have been assigned as data custodian on configured paths in Data Insight.
- Disabled Users - Displays users whose accounts have been disabled in the directory service.
- MigratedSIDs - Displays users whose accounts have been migrated from another domain.

See [“About migrated domains”](#) on page 18.

- Unresolved SIDs - Displays users whose accounts have been deleted in the directory service, and Data Insight is not able to map the SIDs to user information in the Data Insight configuration.

Data Insight automatically adds a domain called UnresolvedSIDs when it scans configured domains. This domain contains all the sIDs or distinguished names of users or groups that Data Insight has no information about. Data Insight may encounter such sIDs (or distinguished names) when a group fetched by Data Insight contains a member from another domain that is not scanned by Data Insight.

Deleted and disabled users are flagged with an icon to indicate their status. The deleted users are indicated with a greyed-out user icon and the disabled users are indicated with a red cross icon. In Data Insight reports, the deleted users and user groups are marked with an asterisk.

To search for a user or a user group:

- 1 Click the **Users** or **Groups** tab, as the case maybe, to display the users or group information fetched from the directory services.
- 2 Enter the name of a user or a user group in the search bar, or click **Select Filter**.
- 3 Select the required filter. The filtered output is displayed in the navigation pane.

You can also build a query based on the attributes of a user or user group and save it for future use.

To filter users and user groups on the basis of attribute query:

- 1 Select **Attribute Query > Add/Delete Query**.
- 2 Click **Select query** to filter users based on an already saved query.
- 3 Click **New Query** radio button to add a new query.
- 4 Enter a query name.
- 5 Select **Custom Attribute** or **BU Attribute**, and from the drop-down lists, select the attribute that you want to use as filter.
- 6 Click the add icon to build multiple queries, or click the delete icon to delete the additional rows.
- 7 Click **Apply** to apply the selected conditions to the users list.
 - Click **Delete** to delete the currently selected query.
 - Click **Exit** to exit the Attribute Query Editor.
- 8 Click **Save & Apply** to save the query and apply the criteria specified in the query to the users listed in the navigation pane.

Note: The **Save & Apply** option saves the query in the filter, and you can use the saved query to filter users and user groups at the time of creating a report. The query created by one user is not visible to another user.

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 the Context Map view](#)

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 pattern for files, folders and web applications.

You can navigate shares, sites, files, and folders using any one of the following ways:

- Navigate to a share or a site collection directly by using the search text box at the top of the tree-view pane.
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.
- Use the global search at the top right of the content pane area to look for a particular site collection, share, group, or user.

Viewing the overview of a data repository

To view the attributes of a folder :

- 1 Click the **Folders** tab to display the configured filers or Web applications.
- 2 Click a filer or Web application. The **Overview** tab displays by default. It shows the summary of the assigned and inherited custodians.
- 3 On the navigation pane in the left-hand panel, expand a filer or Web application to display a list of configured shares or site collection, as the case may be.
- 4 Expand a share/site collection to view the folders, sites, document libraries, or picture libraries share/site collection.
- 5 Click a folder. Or right-click a folder in the navigation pane and select **Overview**.
By default, the **Overview** tab displays the following summary of the selected data repository:
 - The physical and logical 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.

For assigning a custodian, See [“Managing data custodian for paths”](#) on page 30.

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.
- For a user, view all the paths on which the user is assigned or is an inherited custodian.
- 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 On the **Workspace** tab, navigate to the entity for which you want to assign a custodian.

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

- 2 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**.
- 3 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.

- 4 To assign a custodian based on user or group directory attributes, from the drop-down list **Select User/Group Attribute**.
- 5 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.

- 6 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`.

- 7 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**.
- 8 Or, 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**.
- 9 Or, 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**.
- 10 Click the Export icon at the bottom of the page to save the data to a `.csv` file.
- 11 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 On the **Workspace** tab, navigate to the path for which you want to delete a custodian.
- 2 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 Click **User Activity**. Or right-click the folder in the tree view and select **User Activity**.
- 2 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 15.
See [“Viewing audit logs for files and folders ”](#) on page 37.
 - A tabular view of the access pattern of the top five users of the selected file or folder.
- 3 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 **User Activity** tab.

To view user activity on a file or folder

- 1 Navigate to the folder for which you want to view the user activity information.
See [“About viewing file or folder summary”](#) on page 28.
By default, the **Overview** tab displays a summary of the file or folder.
- 2 Click **User Activity**.

- 3 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 34.
 - 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 15.
See [“Viewing audit logs for files and folders”](#) on page 37.
 - A tabular view of the access pattern of the top five users of the selected file or folder.
- 4 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 34.
- 5 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.
- 6 Click the Export icon at the bottom of the page to save the data to a `.csv` file.
- 7 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.

- 8 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.
- 9 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 Click the **Folders** tab and navigate to the path for which you want to assign a custodian.
- 2 Click the **User Activity** tab.
- 3 Click the **Summary** sub-tab to display the inferred data owner.
- 4 Right-click the inferred data owner, and select **Add as Custodian**. For assigning a custodian, See [“Managing data custodian for paths”](#) on page 30.

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 Click the **Folders** tab and navigate to the path for which you want to assign a custodian.
- 2 Click **User Activity** tab.
- 3 Click the **Active Users** sub-tab to display a list of active users.
- 4 From the list displayed, right-click the user you want to assign as a custodian and select **Add as Custodian**.
- 5 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 30.

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 Click the **Folders** tab and navigate to the path for which you want to assign a custodian.
- 2 Click **Permissions** tab.
- 3 Right-click a user from the list displayed on the page, and select **Add as Custodian**.

See [“Managing data custodian for paths”](#) on page 30.

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 Navigate to the file or folder for which you want to view the activity information.

See [“About viewing file or folder summary”](#) on page 28.

By default, the **Overview** tab displays a summary of the folder including details of the files in the folder.

- 2 Click **File Activity** or **Folder Activity**. Or right-click the file or folder in the navigation pane and select **File Activity** or **Folder Activity**.
- 3 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 61.

- 4 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*.

- 5 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 Navigate to the folder for which you want to view the permission details.
See [“About viewing file or folder summary”](#) on page 28.
- 2 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.
- 3 Click the **Include share level permissions** check box to include share-level permissions when computing effective permissions.
- 4 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.
- 5 Click **Share-level permissions** to view a user's or a group's share-level permissions.
- 6 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.
- 7 Click the **Export** icon at the bottom of the page to save the data to a `.csv` file.
See [“About recommending permission changes”](#) on page 56.
See [“Reviewing permission recommendations”](#) on page 57.
See [“About permissions”](#) on page 16.

Viewing NFS permissions on folders

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

To view the permissions on folders

- 1 Navigate to the folder for which you want to view the permission details.
- 2 Click **Permissions**. Or right-click the folder and select **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 Click the **Folders** tab.
- 2 Navigate to the path for which you want to view the permission details.
- 3 Click **Permissions**. Or right-click the path and select **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.

- 4 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 that file or folder for the last six months from the current date.

To view audit logs for files and folders

- 1 Navigate to the file/folder for which you want to view the audit logs.
See [“About viewing file or folder summary”](#) on page 28.
- 2 Click **Audit Logs**. Or right-click the file or folder and select **Audit Logs**.
- 3 Apply the time filter for which you want to view the user activity on a specific file or folder.
- 4 Select **Include sub-folders**, if you want to view activity logs for the sub-folders contained in the selected folder.

5 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.

6 The audit logs provide the following information:

- The name of the user who accessed the folder.
- 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 IP address of the machine from which the file was accessed.

Note: The IP address is not available for Windows File Servers, VxFS filers, and SharePoint servers.

- The type of file
- The access count
- The start and end time of the time window in which the event occurred.

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

- The name of the user in the format, user@domain_name.
- The IP address of the machine from which the file was accessed.
Currently, you can not view the IP address of the machine from which the file was accessed for Windows File Servers, VxFS filers, and SharePoint sites.
- 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 values separated by commas. Enter the filter criteria in the relevant fields and click **Go**.

8 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.

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

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 pattern 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 In the Management Console, select the share for which you want to view the collaboration graph.
- 2 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.

- 3 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.
- 4 Click a cluster group to view the top folders under which the users in the cluster are collaborating. You can also view the number of users for each attribute value in the cluster group.
 - 5 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.

- 6 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.

- 7 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.
- 8 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.

- 9 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.

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

About the Context Map view

The Context Map view on the **Workspace** tab provides in-depth information about the activity at any level within a file system hierarchy. This view enables you to identify the following:

- The most active branches on the file system. The Context Map view provides a heatmap of the activity percentage to help you identify the type of accesses being made on any level within the share,
- The control points within the share. See [“About control points”](#) on page 43.
- The open shares within a file system hierarchy. For information about open shares and configuring an open share policy, see the *Symantec Data Insight Administrator's Guide*.
- High-risk folders (folders containing sensitive files) based on Data Loss Prevention (DLP) policies and incidents.
- The attributes of the users who have activity on any given level in the hierarchy. You can use the attributes to group the users with similar attributes. The attribute information enables you to understand the business context users and their activity pattern.
- The density of an attribute value, in percentage. For a selected path, Data Insight sorts the accesses on the path based on attribute values of active users. The percentage value is calculated on the total activity by users bearing an attribute value on selected path, as against the total number of active users at that level in the hierarchy.

The activity statistics for a share is calculated by taking into account the total activity on the share and the activity at a particular level of the share. The activity statistics for a folder considers the activity on the folder and its children.

You can configure the attributes to be considered for computing the control points from the **Advanced Analytics** configuration page on the Management Console. Symantec recommends that you configure key grouping custom attributes such as, *Department*, to enable richer analysis. For more information on configuring user attributes, see the *Symantec Data Insight Administrator's Guide*.

The Context Map view uses historical data to provide analytics. Symantec recommends that the unstructured data should be monitored for at least six months to have enough data to provide analytics about highly collaborative shares, openness of shares, and the shares that have sensitive files, and control points. This view differs from the Data Insight dashboard in that it enables interactive navigation and it lets you drill down to the deepest level of the file system hierarchy. You can view analytics for folders and files on a share, whereas the Data Insight dashboard lets you drill down only to the level of a share or site collection.

See [“Viewing advanced analytics for a path”](#) on page 43.

About control points

A control point is the level in a file system hierarchy 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 reset 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.

Viewing advanced analytics for a path

By default, the **Context Map** view displays summary information about activity and sensitive files in the file system hierarchy, as also the summary of storage on the configured devices. You can choose to filter the data by selecting a context. The

data displayed in the **Context Map** view changes based on the context that you choose. For example, the **Security** view displays information about the number of sensitive files, open shares, and a list of Data Loss Prevention (DLP) policies that are violated on that path. Whereas, the **Activity** context provides the following information for the selected path:

- The number of access events.
- The heatmap of the activity percentage.
- The number of active files.
- The number of inactive files.
- The number of users who have accesses on the path.
- The distribution of users based on the attribute values.

You can also create a **Custom** view by selecting the columns for which you want to see data.

To view analytics for a selected path

- 1 On the **Workspace > Folders** tab, do one of the following:
 - Click **Context Map**. Data Insight displays the **Context Map** view for all configured storage devices. You can drill down the folder hierarchy to select the path for which you want to view the detailed analytics.
 - Or, in the tree view panel, navigate to the path for which you want to view analytics, and click Context Map.

The **Context Map** view displays all configured storage devices or the selected path.

To navigate to other views for a path, click **Context Map** again.

The **Context Map** view displays the following information for the selected path:

- The storage capacity on the selected storage device.
- The free space available on the storage device.
- The used space on the storage device.
- The heatmap showing the percentage of total read, write, and other accesses on the path relative to the total activity on the share.
- The total accesses on the path.
- The number of active users on the path.
- The type of accesses on the path - read, write, or other accesses.
- The number of files and folders under the selected path.

- The number of active files on the selected path and their total size.
 - The number of inactive files on the selected path and their total size.
 - The number of shares or site collections on the configured device.
 - The number of open shares on the filer.
 - The size of the open shares.
 - The number of files in the open shares.
 - Whether the selected path is a control point.
 - The number of control points.
 - The number of sensitive files on the path.
 - The number of Data Loss Prevention policies that are associated with the sensitive files on the path.
 - The name of the DLP policy.
 - The number of custodians on the path.
 - Names of the custodians.
 - The values for configured attributes.
 - The count of users with activity on the path sorted according to their attributes.
- 2 The panel on the right of the screen provides an overview of the selected path.
- 3 Use the filter at the top of the page to refine the scope of the displayed data. Create filters using the criteria in the drop-down list. For example, from the drop-down, select **Active files**, enter a numeric value, and click **Add Filter**.

As you add new filters, the list is filtered to show the data that matches your filter. Note that filters with the same criteria but different values are evaluated serially, and different filters criteria are applied together.

The filter criteria require numeric, percentage, boolean, or text string values. For example, the **Is Control Point** parameter requires a boolean value, such as, Is Control Point = Yes. Whereas, the Activity Type, Custodian List, Owner, and DLP Policy List parameters require a string value. For example, Custodian List = < *Name of custodian* >

You must specify the size and percentage value with its unit measure. For example, Active size > 1GB. When specifying a range of numbers, use comma as the separator. For example, Activity % Between 20%,30%.

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 Click the **Users** tab to display the configured users.
- 2 Click a user.

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 recommendations.

- The directory domain attributes of the user.
- 3 Click **Export** to export the information on the page to a `.csv` file.
- 4 You can also assign or delete custodian assignments from the **Overview** tab. See [“Managing custodian assignments for users”](#) on page 47.

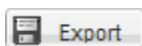
Viewing the overview of a group

To view the attributes of a user group

- 1 Click the **Groups** tab to display the configured groups.
- 2 Click a group.

By default, the **Overview** tab displays a summary of the selected group. The summary includes the following details:

- 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.
- 3 Click any of the following icons to export data to a `.csv` file:



Exports all data on the screen to a `.csv` file.



Exports the data on a panel on the screen to a `.csv` file.

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 > Users** tab, navigate to the user that you want to assign a custodian on a data location.

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

- 2 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.
- 3 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.
- 4 You can drill down the **Physical** or **DFS** hierarchy to view the children data locations for which the user is a custodian.
- 5 To assign the user as the custodian for a particular path, click the Custodian icon and select **Add Location**.
- 6 Select the **Physical** or **DFS** radio button.
- 7 Select the location, and click **OK**.
- 8 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 Navigate to the user for whom you want to view the activity information.
- 2 Click **Activity**. Or right-click the user in the navigation pane and select **Activity**.
- 3 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.

- 4 Click the **By Time** sub-tab to view the activity details of the user for a specific time period on the selected share.
- 5 Enter the start and end dates in the **From** and **To** field.
- 6 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.

- 7 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.
- 8 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 16.

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 Navigate to the user for whom you want to view the permissions.
- 2 Click **Permissions**. Or right-click the user in the navigation pane and select **Permissions**.
- 3 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.

- 4 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

- 5 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.
- 6 Click **Share-level permissions** to view a user's share-level permissions on a selected share.
- 7 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 16.

To view the permission assigned to a user group

- 1 Navigate to the group for which you want to view the permissions.
- 2 Click **Permissions**. Or right-click the user group in the navigation pane and select **Permissions**.
- 3 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 filters 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.

- 4 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 filters 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.

- 5 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.

- 6 Click **Effective Permissions** to view the list of all the folders, on the selected share, on which the group has effective permissions.
- 7 Click **Advanced permissions** icon to view the details of the operation that a group is allowed or denied on a given path.
- 8 Click **Share-level permissions** to view a group'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 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 Navigate to the user or user group for whom you want to view the permissions.
- 2 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.

- 3 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.

- 4 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 Click the **Users** tab.
- 2 Navigate to the user for whom you want to view the permissions.
- 3 Click **Permissions**. Or right-click the user in the navigation pane, and select **Permissions**.

- 4 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 filters 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 filters 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.

- 5 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.

- 6 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 15.

To view the audit logs for users:

- 1 Select the user you want to view audit logs for.
- 2 Click **Audit Logs**. Or right-click the user, and select **Audit Logs**.

- 3 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.

- 4 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 filters 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.

- 5 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**.

- 6 Click on a folder to see the user's activity on that folder.

- 7 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.
- 8 Click the drop-down arrow on any column header and select Columns. Then select the parameters you want to show.

Viewing permission recommendation on paths

This chapter includes the following topics:

- [About recommending permission changes](#)

About recommending permission changes

Data Insight allows you to leverage the activity data provided by the audit logs and information about permissions on a path to make recommendations for permission changes. You can use the audit logs to identify inactive users and recommend revoking of access rights to users and groups that do not have activity on a path.

Data Insight can recommend that a user be removed from a group, or a group be denied permission on a path, if the user or group is inactive on the path for the selected time period. However, Data Insight does not provide recommendations to modify well-known groups such as Everyone or Administrators.

Data Insight recommends that a user's permission be revoked if the user is inactive on a path. A user can be inactive on a path for multiple reasons. They are as follows:

- If a user leaves the organization and the user's Active Directory account is disabled. Disabled user accounts are indicated by a greyed-out user icon against their names in the tree-view panel on the **Workspace** tab.
- If the user is part of a group that has permissions on the path, but the user does not have any direct activity on the path.

A group can be considered inactive if it inherits permissions on a path as a part another group which has activity on that path, but the group itself does not have any activity on the path.

The permission change recommendations help you evaluate the integrity of the assigned permissions. You can monitor the permissions of inactive users to eliminate access risk and lock down open access and implement recommendations by modifying security groups.

The permission recommendations are calculated after considering the effective permissions for a user or a path, which include share-level permissions.

You can configure the settings required to implement the recommendations. For more information on configuring the permission remediation settings, see the *Symantec Data Insight Administrator's Guide*.

Reviewing permission recommendations

You can view the permission changes recommended by Data Insight, and if you agree with the recommendations, choose to implement the changes.

To review permission recommendations

- 1 In the Management Console, click **Workspace > Folders**.
- 2 Drill down to the path for which you want to view the permission recommendation.
- 3 Click the **Permissions** tab. Or right-click the folder in the navigation pane and select **Permissions > Recommendations**.
- 4 Review the suggested changes.
- 5 Click the Export icon at the top-right corner of the recommendations panel to save the data to a .csv file.

Users with the server administrator role can take further action on the recommendations after analyzing them.

For information on configuring permission recommendation and applying the recommended changes, see the *Symantec Data Insight Administrator's Guide*.

Analyzing permission recommendations and applying changes

Data Insight displays recommendations for permission changes on paths on the **Workspace > Folders > Permissions > Recommendations** tab.

Users with the Server Administrator role can directly take action on the recommended changes from the Data Insight Management Console after reviewing the recommendations made by Data Insight. You can choose to analyze the recommendations to evaluate the effects of the membership changes before you decide to accept the changes. Such analysis helps you review the following:

- The other paths that are affected by the change in permissions.

- Active users who may lose access to certain paths because they are part of the group whose permission is revoked.

You can also configure a Group Change Analysis report on the **Reports** tab to analyze the effects of permission changes outside the scope of the recommendations made by Data Insight.

See [“Group Change Analysis”](#) on page 75.

To analyze and apply permission recommendations

- 1 In the Management Console, click **Workspace > Folders**.
- 2 Drill down to the path for which you want to view the permission recommendation.
- 3 Click the **Permissions** tab. Or right-click the folder in the navigation pane and select **Permissions > Recommendations**.

- 4 Review the recommendations.

If the recommendations include changes to the group, the **Analyze Group Change(s)** button is enabled.

- 5 Click **Analyze Group Change(s)** to run a Group Change Analysis report for the recommended changes.

If you do not agree with any of the recommendations, you can delete the recommendation from the list before analyzing the changes. To remove a recommendation, click the delete button corresponding to the recommendation.

- 6 Once the report run is complete, review the Group Change Analysis report for the Data Insight recommendations.

The report is also available on the **Reports** tab.

- 7 Review the report to analyze the effects of making the recommended changes.
- 8 Click **Apply Changes** to accept the recommendations, and to start the process of raising a request to implement the changes.
- 9 You can also complete the task of making the recommended changes from the **Reports** tab as well. Do the following:

- Navigate to the **Reports** tab.
- Select the appropriate report, and select **Apply Recommendations** from **Select Action** drop-down.

The permission changes are handled as configured on the **Settings** tab. For information about configuring permission remediation, see the *Symantec Data Insight Administrator's Guide*.

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 inactive data from the Folder Activity tab](#)
- [Managing data from the Context Map view](#)
- [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 61.
- The files that appear inside the following types reports:
 - **Access Details** reports
 - **Access Summary** reports
 - **DQL** reports
 - **Data Lifecycle** reportsSee [“Managing inactive data by using a report”](#) on page 63.
- Paths listed in the **Context Map** view on the **Workspace** tab.
See [“Managing data from the Context Map view”](#) on page 62.

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 60.
- 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 61.

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 59.

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 59.

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 data from the Context Map 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 Context Map view

- 1 In the Management Console, click the **Workspace** tab.
- 2 Click **Context Map**.

Data Insight displays the **Context Map** view for all configured storage devices. You can drill down the folder hierarchy to select the path for which you want to archive or otherwise manage using custom scripts.

- 3 Select the check boxes for the paths that you want to manage.

- 4 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*.

- 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 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.

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](#)

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 or the Data Insight Management Server, depending on the type of workflow request.

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.

What you can do with the Self-Service Portal

[Table 8-1](#) describes the tasks that custodians and data owners can accomplish using the Self-Service Portal.

Table 8-1 What you can do with the Self-Service Portal

| Task | Description |
|--------------------|---|
| Entitlement Review | <p>Review the user permissions on the resources that the custodians own, attest to the permissions, or suggest changes to the permissions.</p> <p>See “Using the Self-Service Portal to review user entitlements” on page 68.</p> |

Table 8-1 What you can do with the Self-Service Portal (*continued*)

| Task | Description |
|--|---|
| Remediate Data Loss Prevention (DLP) incidents | <p>Data Insight uses DLP FlexResponse plug-ins to fetch incidents on sensitive paths on the NAS devices that Data Insight monitors.</p> <p>Security administrators create workflows to distribute incidents to custodians for the purpose of remediation. The custodians or data owners receive email alerts to remediate the resources that violate configured DLP policies. The custodians can then log in to the portal, view sensitive paths that are assigned to them and the policies that these files violate, and take configured actions on the incidents assigned to them</p> <p>Once the custodians submit the request for remediation, the DLP engine executes the request, and sends a response back to the Data Insight Management Console.</p> <p>See “Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents” on page 69.</p> |
| Confirm ownership of resources | <p>Custodians are assigned the data resources that they own for the purpose of remediation from the Data Insight console. The Ownership Confirmation workflow enables custodians to verify that they indeed own the resources. They can view the list of resources they own, and confirm or decline the ownership of these resources from the Self-Service Portal.</p> <p>See “Using the Self-Service Portal to confirm ownership of resources” on page 70.</p> |

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.

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 67.

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.

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.

See [“Logging in to the Self-Service Portal”](#) on page 67.

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 67.

Using Data Insight reports

This chapter includes the following topics:

- [About Data Insight reports](#)
- [About Data Insight security reports](#)
- [About Data Insight storage reports](#)
- [About Data Insight custom reports](#)
- [Viewing report details](#)
- [Filtering a report](#)
- [Creating 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](#)
- [Archiving of reports automatically](#)
- [Canceling a report run](#)
- [Deleting a report](#)

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 79. |
| Access Details Reports | See “Access Details report” on page 74. |
| Permissions Reports | See “Permissions reports” on page 74. |
| Capacity Reports | See “Capacity reports” on page 79. |
| Ownership Reports | See “Ownership Reports” on page 76. |
| Custom Reports | See “About Data Insight custom reports” on page 86. |
| Data Lifecycle Reports | See “Data Lifecycle reports ” on page 80. |
| Consumption Reports | See “Consumption Reports” on page 83. |

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 74.
- Permissions reports
See [“Permissions reports”](#) on page 74.
- Ownership Reports
See [“Ownership Reports”](#) on page 76.

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 limit accesses of these users to a list of files or folders.
- Access Details report for path
Use this report to get detailed 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 limit accesses shown to the users.

Permissions reports

Use the Permission reports to get detailed information of the permissions assigned to various users, files, and folders.

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. 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.

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 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.

See [“About recommending permission changes”](#) on page 56.

See [“Reviewing permission recommendations ”](#) on page 57.

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.

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 79.
- Capacity Reports
See "[Capacity reports](#)" on page 79.
- Data Lifecycle Reports
See "[Data Lifecycle reports](#)" on page 80.
- Consumption Reports

See [“Consumption Reports”](#) on page 83.

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 path**
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*.

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 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.

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.

Duplicate Files

Use this report to get a summary of duplicate files in the same share. Two files are considered to be duplicates if they have the same logical file size and the same file extension. Data Insight, while creating the report, considers only those file extensions that have been configured to be part of a file group in the configuration database. Also, 0-byte files are not considered when this report is run.

Duplicate File reports contain the following details about the duplicate files:

- The name of the file with its path.
- The owner of the file.
- The user account of the file owner.
- The business unit to which the file owner belongs.
- The owner of the business unit.
- The DFS path for the file.
- Logical size of the file that is specified in megabytes.
- Time when the file was last accessed.
- Time when the file was created.

- Time when the file was last modified.
- The number of times the file was read.
- The number of times the file was written.

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.

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*.

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*.

See [“Create/Edit DQL report options”](#) on page 114.

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 91.

See [“Creating a report ”](#) on page 93.

Data Insight provides the following default query templates:

Table 9-1

| 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. |

Table 9-1 (continued)

| Category | Name | Description |
|-----------------|-------------------------------------|--|
| Data Management | All files with a specific extension | <p>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.</p> <p>Modify the template to add other extensions to get results that suit your needs.</p> |
| Data Management | Files in a confidential folder | <p>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.</p> <p>Modify share name and folder name search criterion to get results that suit your needs.</p> |
| Data Management | Files with undefined file group | <p>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.</p> |
| Data Management | Folder summary by file type | <p>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.</p> <p>Modify the share name to get results that suit your needs.</p> |
| Data Management | Stale file list | <p>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.</p> <p>Modify the duration and the share name to get the results that suit your needs.</p> |

Table 9-1 (continued)

| Category | Name | Description |
|-----------------|--|--|
| Data Management | Storage usage by user attribute | <p>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.</p> <p>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.</p> |
| Risk Analysis | Sensitive files on a filer | <p>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.</p> <p>Modify the device name with valid filer name in your environment to get the results that suit your needs.</p> |
| Risk Analysis | Sensitive files that are active | <p>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.</p> <p>Modify the activity period and policy to get the output that is valid for your environment.</p> |
| Risk Analysis | Sensitive files with violated policies | <p>The query lists all the sensitive files in a share and the associated DLP policy that are violated.</p> <p>Modify the share name to get the output that is valid for your environment.</p> |

Table 9-1 (continued)

| Category | Name | Description |
|---------------|---|--|
| Risk Analysis | Department-wise summary of risky behavior | <p>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.</p> <p>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.</p> <p>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.</p> |
| Risk Analysis | Recent suspicious activity | <p>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.</p> <p>Modify the recent access time range and inactivity time range in your environment to get results that suit your needs.</p> |
| Forensics | Share access details | <p>This query provides the audit details on a share for a specified time range.</p> <p>Modify the time range and share name to get results specific to your environment.</p> |
| Forensics | User access details | <p>The query provides the details of accesses by a specified person on a share during a specified time range.</p> <p>Modify the person name, time range, and share name to get the results to suit your needs.</p> |

Table 9-1 (continued)

| Category | Name | Description |
|-------------------------|------------------------------------|---|
| Forensics | Top users of sensitive files | <p>The query lists top ten users who have accessed sensitive files in your storage environment within a specified time-range.</p> <p>Modify the time range to get valid result in your environment.</p> |
| Forensics | Folders with maximum access counts | <p>The query fetches the list of top ten folders that are accessed in a share during a specific time range.</p> <p>Modify the share name and time-range to get valid result in your environment.</p> |
| Forensics | Users with maximum access counts | <p>The query fetches the list of top ten users who have accessed a share during a specific time range.</p> <p>Modify the share name and time-range to get valid result in your environment.</p> |
| User / Group Management | Group membership details | <p>The query provides the details about a specified security group, its member groups, and users in the group.</p> <p>Modify the group name and domain name to get the results that are valid for your environment.</p> |
| 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 | <p>The query provides a comma-separated list of security groups, their details and SIDs of its member users.</p> <p>To list the empty groups for clean-up, execute following query on the output:</p> <pre>SELECT * FROM groups WHERE memberusers_sid = "</pre> |
| User / Group Management | Circular groups | The query lists any security groups in the environment which are members of each other forming group loopings. |

Table 9-1 (continued)

| Category | Name | Description |
|-----------------------|---|--|
| Data Protection | Open shares | The query lists all paths in your environment that have excessive permissions along with the reasons for their openness. |
| 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

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.

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.

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 94.

See [“Create/Edit storage report options”](#) on page 105.

See [“Create/Edit DQL report options”](#) on page 114.

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*.

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 9-2 Create/Edit security report options

| Option | Description |
|--------------------|-------------|
| Report Information | |

Table 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|--------|---|
| | <p>Enter information in the following fields:</p> <ul style="list-style-type: none">■ 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. <p>Note:</p> <p>This field is available only in the following five reports :</p> <ul style="list-style-type: none">■ Access summary report for paths■ Data aging report■ Inactive folders report■ Path permissions report■ Consumption by folders report <ul style="list-style-type: none">■ 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.■ 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 |

Table 9-2 Create/Edit security report options (continued)

| Option | Description |
|--------|---|
| | <p>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.</p> <ul style="list-style-type: none">■ 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 9-2 Create/Edit security report options (continued)

| Option | Description |
|---------------|-------------|
| Configuration | |

Table 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|--------|---|
| | <p>Select the conditions to configure the report.</p> <ul style="list-style-type: none">■ 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 <i>Symantec Data Insight Administrator's Guide</i>.■ 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,<ul style="list-style-type: none">■ Select Current folder, to include the folders from the current directory. |

Table 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|--------|--|
| | <ul style="list-style-type: none">■ Select Full to include all the folders.■ Select Specify Depth and enter the level at which you want to include the folders. <p>You can add folder depth for the following reports:</p> <ul style="list-style-type: none">■ Path Permissions■ User/Group Permissions■ Inferred Owner■ Entitlement Review <ul style="list-style-type: none">■ 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 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. <p>Note: This option is available only for Entitlement Review report.</p> <ul style="list-style-type: none">■ 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 119. |

Table 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|--------|---|
| | <ul style="list-style-type: none">■ 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 :<ul style="list-style-type: none">■ 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 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|--------|---|
| | <ul style="list-style-type: none">■ Results-This option is available only for the Data Inventory Reports. Use this option to specify the following:<ul style="list-style-type: none">■ 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 Attributes that you have selected from the Department Mapping drop-down.■ Summary and Sensitive file details-Select this option to create a report which displays:<ul style="list-style-type: none">■ 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 attributes 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:<ul style="list-style-type: none">■ The details of the all the files.■ The summary of all the files grouped by business unit owner, or any other custom attributes 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. |

Table 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|---------------------|---|
| Data Selection | <p>Do the following:</p> <ol style="list-style-type: none">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. <p>This option is available for the following reports:</p> <ul style="list-style-type: none">■ Access Details for Paths■ Access Summary for Paths■ Path Permissions■ Entitlement Review |
| Custodian Selection | <p>For data custodian driven reports Data Insight creates a report output for each selected custodian at the time of generating a report.</p> <p>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.</p> |

Table 9-2 Create/Edit security report options (*continued*)

| Option | Description |
|----------------|---|
| User Selection | <p>From the list, click the user, group, or all users/groups radio button. The selected entities are listed in the Selected Users/Groups pane.</p> <p>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.</p> <p>Note: You can search for a particular Built-in user or group by using the Domain Filter.</p> <p>You can also filter a user or group from the Select Filter field.</p> <p>Select the All Filtered Users check box in the Selected Users/Group pane to include all filtered users in the report.</p> <p>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.</p> |
| Exclusion List | <p>Select the groups or users that you want to exclude from the scope of the report.</p> <p>Click the group or user to select it. The selected data set is listed in the Selected Groups/Users pane.</p> <p>Note: You can search for a particular Built-in user or group by using the Domain Filter.</p> |
| Notification | <p>Enter email addresses of users you want to send the report to.</p> <p>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.</p> |

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 9-3 Create/Edit storage report options

| Option | Description |
|--------------------|-------------|
| Report Information | |

Table 9-3 Create/Edit storage report options (*continued*)

| Option | Description |
|--------|---|
| | <p>Enter information in the following fields:</p> <ul style="list-style-type: none"> ■ 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. <p>Note:</p> <p>This field is available only in the following five reports :</p> <ul style="list-style-type: none"> ■ Access summary report for paths ■ Data aging report ■ Inactive folders report ■ Path permissions report ■ Consumption by folders report <ul style="list-style-type: none"> ■ 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. ■ 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 |

Table 9-3 Create/Edit storage report options (continued)

| Option | Description |
|--------|--|
| | <p>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.</p> <ul style="list-style-type: none">■ 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 9-3 Create/Edit storage report options *(continued)*

| Option | Description |
|---------------|-------------|
| Configuration | |

Table 9-3 Create/Edit storage report options (*continued*)

| Option | Description |
|--------|--|
| | <p>Select the conditions to configure the report:</p> <ul style="list-style-type: none">■ 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.■ Show details in report- Select the check box and enter the No of records you want to include in the report output.■ 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 <i>Symantec Data Insight Administrator's Guide</i>.■ 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.■ Time period for activity - 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. |

Table 9-3 Create/Edit storage report options (*continued*)

| Option | Description |
|--------|--|
| | <ul style="list-style-type: none">■ 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,<ul style="list-style-type: none">■ 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. <p>This field is available only for the following reports:</p> <ul style="list-style-type: none">■ Access Summary for Paths■ Access Summary for Users/Groups■ Number of Records - Select the number of records you want to include in the detailed report. <p>In case of Consumption by folders report this option appears only if you enable the check-box Show details in reports.</p> <ul style="list-style-type: none">■ 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. |

Table 9-3 Create/Edit storage report options (*continued*)

| Option | Description |
|--------|--|
| | <ul style="list-style-type: none">■ 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 preconfigured for the type of file you want to include in the report output. This option is available for the following reports:<ul style="list-style-type: none">■ 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:<ul style="list-style-type: none">■ Consumption by File Group■ Consumption by File Group and Owner■ Inactive Data by File Group<p>Note: You can select either a file type or a file group in the report output.</p>■ 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 which Data Insight supports truncation. See “Configuring a report to generate a truncated output” on page 119. |

Table 9-3 Create/Edit storage report options (*continued*)

| Option | Description |
|----------------|--|
| Data Selection | <p>Do the following:</p> <ol style="list-style-type: none">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, folder within a share, or a DFS path to select it. The selected data set is listed in the Selected resources 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. <p>This option is available for the following reports:</p> <ul style="list-style-type: none">■ Access Details for Paths■ Access Summary for Paths■ Path Permissions■ Entitlement Review |

Table 9-3 Create/Edit storage report options (*continued*)

| Option | Description |
|----------------|---|
| User Selection | <p>From the list, click the user, group, or all users/groups radio button. The selected entities are listed in the Selected Users/Groups pane.</p> <p>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.</p> <p>Note: You can search for a particular Built-in user or group by using the Domain Filter.</p> <p>You can also filter a user or group from the Select Filter field.</p> <p>Select the All Filtered Users check box in the Selected Users/Group pane to include all filtered users in the report.</p> <p>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.</p> |
| Exclusion List | <p>Select the groups you want to exclude from the scope of the report.</p> <p>Click the group to select it. The selected data set is listed in the Selected Groups pane.</p> <p>Note: You can search for a particular Built-in user or group by using the Domain Filter.</p> |
| Notification | <p>Enter email addresses of users you want to send the report to.</p> <p>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.</p> |

Create/Edit DQL 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 9-4 Create/Edit DQL report options

| Option | Description |
|--------------------|--|
| Report Information | <p>Enter information in the following fields:</p> <ul style="list-style-type: none">■ 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 <i>unlimited</i>.■ 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 9-4 Create/Edit DQL report options (*continued*)

| Option | Description |
|--------------|--|
| Query | <p>Write your DQL query in the space provided.</p> <p>While writing the query you must adhere to the syntax and guidelines of the Data Insight Query Language(DQL).</p> <p>For more information about creating DQL queries, see the <i>Symantec Data Insight Programmer's Reference Guide</i>.</p> <p>Alternatively you can use any of the query provided by Data Insight as templates. Click Use Template. 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.</p> <p>See “About DQL query templates” on page 86.</p> <p>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.</p> <p>For details on how to use the content of CSV file as arguments in a query, refer <i>Symantec Data Insight Programmer's Reference Guide</i>.</p> |
| Notification | <p>Enter email addresses of users you want to send the report to.</p> <p>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.</p> |

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 Select the report that you want to generate.
- 3 In the **Select Action** drop-down, click **Run**.

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.

Archiving of reports automatically

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 60.

See [“About post-processing actions”](#) on page 61.

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 117.
- 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 category to view the types of reports in that category.
- 3 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.
- 4 Select the report you want to delete, and in the **Select Action** drop-down, click **Delete**.
- 5 Click **OK** on the confirmation message.

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 37
- accessibility
 - Management Console 20
 - tabs 21
 - tools 20
- Archiving
 - using Enterprise Vault 59
- archiving
 - by using reports 63
 - inactive subfolders 61
 - post-processing actions 61
 - retention categories 60
- audit logs
 - overview 15

D

- data custodian
 - overview 14

F

- filtering
 - users and user groups 26
- folders
 - assigning active user as custodian 34
 - assigning custodian 34

M

- Management Console
 - logging in 23
 - logging out 23
 - operation icons 22

O

- overview
 - access information for users and groups 25
 - managing data custodian 30
 - migrated domains 18
 - viewing access information for folders 24, 28

P

- permissions
 - assigning custodian 34
 - overview 16

R

- report
 - truncate 119
- reports
 - cancelling generation 123
 - copying 117
 - creating 93
 - DQL report dialog options 114
 - security report dialog options 94
 - storage report dialog options 105
 - customizing column names 118
 - deleting 123
 - editing 116
 - filtering 93
 - generating 117
 - overview 73
 - send by email 121
 - storage 79
 - type
 - custom 86
 - security 73
 - storage 78
 - viewing 91

S

- saving
 - CSV file 73
 - HTML file 73
 - PDF file 73
- security
 - Access Details 74
 - Access Summary 79
 - ownership reports 76
 - Permissions 74

sharepoint permissions
overview 17

V

viewing

- attributes of a group 47
- attributes of a user 46
- attributes of file or folder 29
- folder activity log 37
- report execution log 117
- reports 91
- user access details 53
- user activity on folders 49

viewing folder activity

- by time 35
- for inactive subfolders 35
- for subfolders and files 35

viewing permissions

- effective permissions 36
- File System Access Control List 36
- for groups 51
- for users 50
- share-level permissions 36

viewing user activity

- active users 32
- inactive users 32
- overview 32