Veritas Data Insight User's Guide

6.1.2

VERITAS™

Veritas Data Insight User's Guide

6.1.2.0

Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas 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. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

https://www.veritas.com/about/legal/license-agreements

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 Veritas Technologies LLC 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. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

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

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

http://www.veritas.com

.

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

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

Contents

Section 1 Introduction 9

Chapter 1 Introducing Veritas Data Insight 10

About Veritas Data Insight 10
About data custodian 13
About permissions 14
About SharePoint permissions 15
About Box permissions 16
About audit logs 18
About migrated domains 19
Applications for Symantec Data Loss Prevention 20
Content classification using Veritas Information Classifier 20

Chapter 2 Using the Veritas Data Insight Management Console 21

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

Section 2 Data Insight Workspace 26

Chapter 3 Navigating the Workspace tab 27

About the Data Insight Workspace 27
Using the Workspace filters 31
Managing the Workspace 34
Searching the storage device hierarchy 36
Searching for users and user groups 37

Chapter 4 Analyzing data using the Workspace views 38

About information risk 38
Viewing summary of data sources 39
Viewing shares summary 41
About control points 43
About the risk score for users 43
About the Risk Dossier 45
Assessing risky users - an example scenario 49
Viewing user summary 50
Viewing details of Watchlist users 51
Viewing details of alert notifications 52

Chapter 5 Viewing access information for files and folders 53

About viewing file or folder summary 54
Viewing the overview of a data source 54
Managing data custodian for paths 55
Viewing the summary of user activity on a file or folder 57
Viewing user activity on files or folders 58
Assigning an inferred data owner as custodian 60
Assigning an active user as custodian 60
Assigning a custodian from the Permissions tab 61
Viewing file and folder activity 62
Viewing CIFS permissions on folders 63
Viewing NFS permissions on folders 64
Viewing SharePoint permissions for folders 65
Viewing Box permissions on folders 65
Viewing audit logs for files and folders 66
About visualizing collaboration on a share 68
Analyzing activity on collaborative shares 69

Chapter 6 Viewing access information for users and user groups 72

Viewing the overview of a user 72
Viewing the overview of a group 73
Managing custodian assignments for users 74
Viewing folder activity by users 75
Viewing CIFS permissions for users 76
Viewing CIFS permissions for user groups 78
Viewing NFS permissions for users and user groups 79
Viewing SharePoint permissions for users and user groups 79

Viewing Box permissions for users and user groups 81
Viewing audit logs for users 81

Section 3 Data Insight reports 84

Chapter 7 Using Data Insight reports 85

About Data Insight reports 85
How Data Insight reporting works 87
Creating a report 88
About Data Insight security reports 89
Activity Details report 89
Permissions reports 90
Ownership Reports 107
Create/Edit security report options 109
Data Insight limitations for Box permissions 119
About Data Insight storage reports 120
Activity Summary reports 121
Capacity reports 122
Data Lifecycle reports 124
Consumption Reports 126
Create/Edit storage report options 131
About Data Insight custom reports 140
About DQL query templates 141
Creating custom templates for DQL queries 149
Create/Edit DQL report options 149
Considerations for importing paths using a CSV file 154

Chapter 8 Managing reports 155

About managing Data Insight reports 156
Viewing reports 156
About stale information in reports 158
Filtering a report 158
Editing a report 159
About sharing reports 159
Copying a report 160
Running a report 160
Viewing the progress of a report 161
Customizing a report output 162
Configuring a report to generate a truncated output 163
Sending a report by email 164
Automatically archiving reports 165

Canceling a report run 166
Deleting a report 166
Considerations for viewing reports 167
Organizing reports using labels 167

Section 4 Remediation 169

Chapter 9 Configuring remediation workflows 170

About remediation workflows 170
Prerequisites for configuring remediation workflows 176
Configuring Self-Service Portal settings 176
About workflow templates 178
Managing workflow templates 178
Create/Edit Entitlement Review workflow template 179
Create/Edit DLP Incident Remediation workflow template 181
Create/Edit Ownership Confirmation workflow template 183
Create/Edit Records Classification workflow template 184
Creating a workflow using a template 187
Create Entitlement Review workflow options 188
Create DLP Incident Remediation workflow options 192
Create Ownership Confirmation workflow options 196
Create Records Classification workflow options 197
Managing workflows 200
Viewing details of submitted workflows 201
Extending the deadline of a workflow 201
Copying a workflow 202
Managing submitted workflows 202
Canceling or deleting a workflow 203
Auditing workflow paths 203
Monitoring the progress of a workflow 206
Remediating workflow paths 209

Chapter 10 Using the Self-Service Portal 211

About the Self-Service Portal 211
About Entitlement Review 212
Logging in to the Self-Service Portal 213
Using the Self-Service Portal to review user entitlements 214
Using the Self-Service Portal to manage Data Loss Prevention (DLP) incidents 216
Using the Self-Service Portal to confirm ownership of resources 217
Using the Self-Service Portal to classify sensitive data 217

Chapter 11 Managing data 219

About managing data using Enterprise Vault and custom scripts 219
About Retention categories 220
About post-processing actions 221
Managing data from the Shares list view 221
Managing inactive data from the Folder Activity tab 223
Managing inactive data by using a report 224
Archiving workflow paths using Enterprise Vault 225
Using custom scripts to manage data 226
Pushing classification tags while archiving files into Enterprise Vault 227
About adding tags to files, folders, and shares 229
Using the metadata framework for classification and remediation 230

Chapter 12 Managing permissions 233

About permission visibility 233
About recommending permission changes 234
About recommending permissions changes for inactive users 235
Reviewing permission recommendations 236
Analyzing permission recommendations and applying changes 236
Making permission changes directly from Workspace 238
Removing permissions for Entitlement Review workflow paths 240

Appendix A Command Line Reference 241

mxcustodian 242

Index 245

Section 1

Introduction

- Chapter 1. Introducing Veritas Data Insight
- Chapter 2. Using the Veritas Data Insight Management Console

Chapter 1

Introducing Veritas Data Insight

This chapter includes the following topics:

- About Veritas Data Insight
- About data custodian
- About permissions
- About SharePoint permissions
- About Box permissions
- About audit logs
- About migrated domains
- Applications for Symantec Data Loss Prevention
- Content classification using Veritas Information Classifier

About Veritas Data Insight

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

With Veritas Data Insight, users can monitor file access to automatically identify the data user of a file based on the access history. This method enables more efficient remediation and data management.

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

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. Veritas 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 13.
- Data leak investigation
  In the event of a data leak, you may want to know who saw a particular file. On the Veritas Data Insight Management Server, you can view detailed information and an audit history of who accessed the data.
  See “About audit logs” on page 18.
- 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 14.
See "About SharePoint permissions " on page 15.

- Manage inactive data

  Data Insight enables better data governance by letting you archive inactive and orphan data using 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 219.

- Provide advanced analytics about activity patterns

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

  See "About the Data Insight Workspace" on page 27.
  See "About visualizing collaboration on a share" on page 68.

- Permission remediation

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

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

- Content classification

  Data Insight lets you classify content on data sources that it monitors by providing means to define classification rules (policies) that let you specify values (tags) that you can assign to any matching items. The classification feature works in conjunction with the policy framework provided by Veritas Information Classifier to assign tags to files.

  For example, a content scan may search for items whose contents include a credit card number and assign a tag of "PII" (for "personally identifiable information") to any that do.

  For information about setting up classification and initiating classification requests, see the *Veritas Data Insight Classification Guide*.

- 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 211.

- 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, Azure AD, or any other implementation that keeps user records. 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. For SharePoint Online, you can assign custodians at the account, site collection, and folder level, while for Microsoft OneDrive custodians can be assigned at the account, user account, or folder level. 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 55.

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 242.

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

About permissions

Veritas 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).

Note: Data Insight does not fetch permissions information for SharePoint Online, Microsoft OneDrive, and Documentum data sources.

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

Note: Data Insight does not fetch permissions information for the SharePoint Online data source.

About Box permissions

Data Insight enables visualization and analytics of permissions assigned on Box resources. Visibility into Box permissions enables you to ensure security, minimize the possibility of a data breach, and ensure that the right people have access to the right data.

Box permissions work a little differently than the permissions set on a file server. On a file server, you can specify a different permission at each level of the folder hierarchy. In case of Box resources, the users and groups are assigned access levels that provide a set of permissions on a folder. Typically the subfolders have the same access level as the parent folder .The permissions associated with an

access level are nothing but the actions allowed to the users or groups on that Box resource (folder). The access level assigned to a user or group on a parent folder automatically cascades to the child folder(s), unless a sub-folder is specifically assigned a different access level.

Table 1-1 describes the various access levels in Box.

Table 1-1 Box Permissions

Access level	Permission
Editor	View, download, upload, edit, delete, copy, move, rename, generate shared links , make comments, assign tasks, create tags, and invite/remove collaborators. Users with this access level can not delete or move root level folder.
Viewer	Preview, download, make comments, and generate shared links. Users with this access level can not add tags, invite new collaborators, upload, edit, or delete items in the folder.
Previewer	Preview the items in the folder using the integrated content viewer. Users with this access level can not share, upload, edit, or delete any content.
Uploader	Upload and see the names of the items in a folder. They will not able to download or view any content.
Previewer-Uploader	Preview files using the integrated content viewer as well as upload items into the folder. Users with this access level can not download, edit, or share, items in the folder.
Viewer-Uploader	Preview, download, add comments, generate shared links, and upload content to the folder. They will not be able to add tags, invite new collaborators, edit, or delete items in the folder.
Co-owner	All of the functional read/write access that an Editor has. Users with this access level can manage users in the folder. A Co-Owner can add new collaborators, change access levels of existing collaborators, and remove collaborators. However, a co-owner cannot manipulate the user with owner permission on the folder or transfer ownership to another user.
Owner	All rights.

For the latest list of Box permissions, refer to Box documentation.

Data Insight displays the access levels for users and the paths on which unique permissions are set. Data Insight does not distinguish between privately owned

and collaborative folders in the folder and user centric views. A lock icon on a folder signifies unique permission, otherwise nherited from owner.

See “Data Insight limitations for Box permissions ” on page 119.

About audit logs

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

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

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

- If a trustee (user or group) is allowed or denied permission on a path.
- If a trustee's permissions are removed on a path.
- If a trustee is given additional permission or denied certain permission on a path. For example, if a user 'X' has Read and Write permissions on a folder. If the user is also subsequently allowed Modify permission on the folder, Data Insight records an Permission Change event.

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

You can use these access events for the following purposes:

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

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

See “Viewing audit logs for files and folders ” on page 66.

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 a user's SID and SID history to compute the effective permissions and to display user activity information. When Data Insight calculates effective permissions of a user, it considers that user's SID and sIDHistory along with the SID and sIDHistory of all the groups that the user is a member of. This emulates the way Windows determines effective permissions.

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*.

Content classification using Veritas Information Classifier

To understand how Data Insight classifies files to detect sensitive information using Veritas Information Classifier, see the *Veritas Data Insight Classification Guide*.

Chapter 2

Using the Veritas Data Insight Management Console

This chapter includes the following topics:

- About the Veritas 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 Veritas Data Insight Management Console

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

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

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

Header

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

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

Tabs

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

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

Navigation pane

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

Content pane

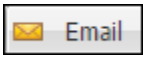
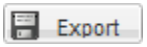
The Veritas Data Insight Console's main display area, or content pane, displays information about folders, files, users, configuration data, and events. The information displays in a variety of tabular and graphical formats. You can also perform tasks like exporting data to a file and emailing the data 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
	The settings icon is used in assigning custodians.
	Screen refresh. Veritas recommends using this refresh button instead of your browser's **Refresh** or **Reload** button.
	Email the data on the current screen to one or more recipients. If the current screen's data cannot be sent as an email, the icon is unavailable.
	Exports all data on a panel on the current screen to a `.csv` file.
	Exports all data on the current screen to a `.csv` file.
	Submits request to the Enterprise Vault server to archive the selected folders.
	The action selector icon displays a menu with the following two options: ■ Archive files using Enterprise Vault. ■ Submit request to invoke a custom action on selected paths.
	Submit request to invoke a custom action on selected paths.

Logging in to the Data Insight Management Console

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

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

   The Management Console appears.

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

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

   The Management Console appears.

Logging out of the Data Insight Management Console

To log out

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

Accessing online Help

Veritas 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.

Section 2

Data Insight Workspace

- Chapter 3. Navigating the Workspace tab
- Chapter 4. Analyzing data using the Workspace views
- Chapter 5. Viewing access information for files and folders
- Chapter 6. Viewing access information for users and user groups

Chapter 3

Navigating the Workspace tab

This chapter includes the following topics:

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

About the Data Insight Workspace

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

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

The dashboard helps you do the following:

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

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

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

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

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

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

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

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

Table 3-1 Workspace Dashboard tiles

Tile	Description
Data Sources	Displays all the configured data sources such as filers, SharePoint web applications, Documentum repositories, and cloud storage accounts. The data sources are listed in order of their risk score. Depending on the view that you select, the tile displays the following information: ■ Number of sensitive files on the data source. ■ The number of shares with sensitive data on them. ■ The risk score assigned to a share after considering the number of open shares, active user count, and the number of sensitive files on the share. ■ The size of inactive data on a data source. ■ The number of active users on the data source. See "Viewing summary of data sources" on page 39.
Shares	Displays all shares that Data Insight monitors. Depending on the view that you select, the tile displays the following data: ■ The number of sensitive and active files on a share and the number of open shares. ■ The risk score of a share considering the active user count and the sensitive file count of the share, and the maximum permitted user count for the share. A higher count of active users and sensitive files contributes to a higher risk for a share. See "About information risk" on page 38. ■ The activity (number of accesses) on the share. ■ The total files on the share and the total size of the data on the share. See "Viewing shares summary" on page 41. You can manage inactive data from the **Shares** list view. See "Managing data from the Shares list view" on page 221.

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

Tile	Description
Users	Displays all configured users in Data Insight. The tile displays the following information: ■ The risk score of a user based on parameters such as abnormal access pattern, accesses made on sensitive data, and the number of alerts raised against the user. See "About the risk score for users" on page 43. ■ The number of shares on which the user has permissions. ■ The number of sensitive files that are accessed by the user. ■ Th total accesses by the user across all configured devices in he last 15 days (default). ■ The number of unique files accessed by the user in the last 15 days (default). See "Viewing user summary" on page 50.
Watchlist	Displays the list of users on the administrator's watch list, sorted according to the risk score assigned to them. For information about configuring a the watch list settings, see the *Data Insight Administrator's Guide*. See "Viewing details of Watchlist users" on page 51. **Note:** The **Watchlist** tile and list views are only visible to the user assigned the Server Administrator role.
Alerts	Displays the summary count of alert notifications raised against configured policies and the severity of the alerts. See "Viewing details of alert notifications" on page 52. **Note:** The **Alerts** tile and list views are only visible to the user assigned the Server Administrator role.

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

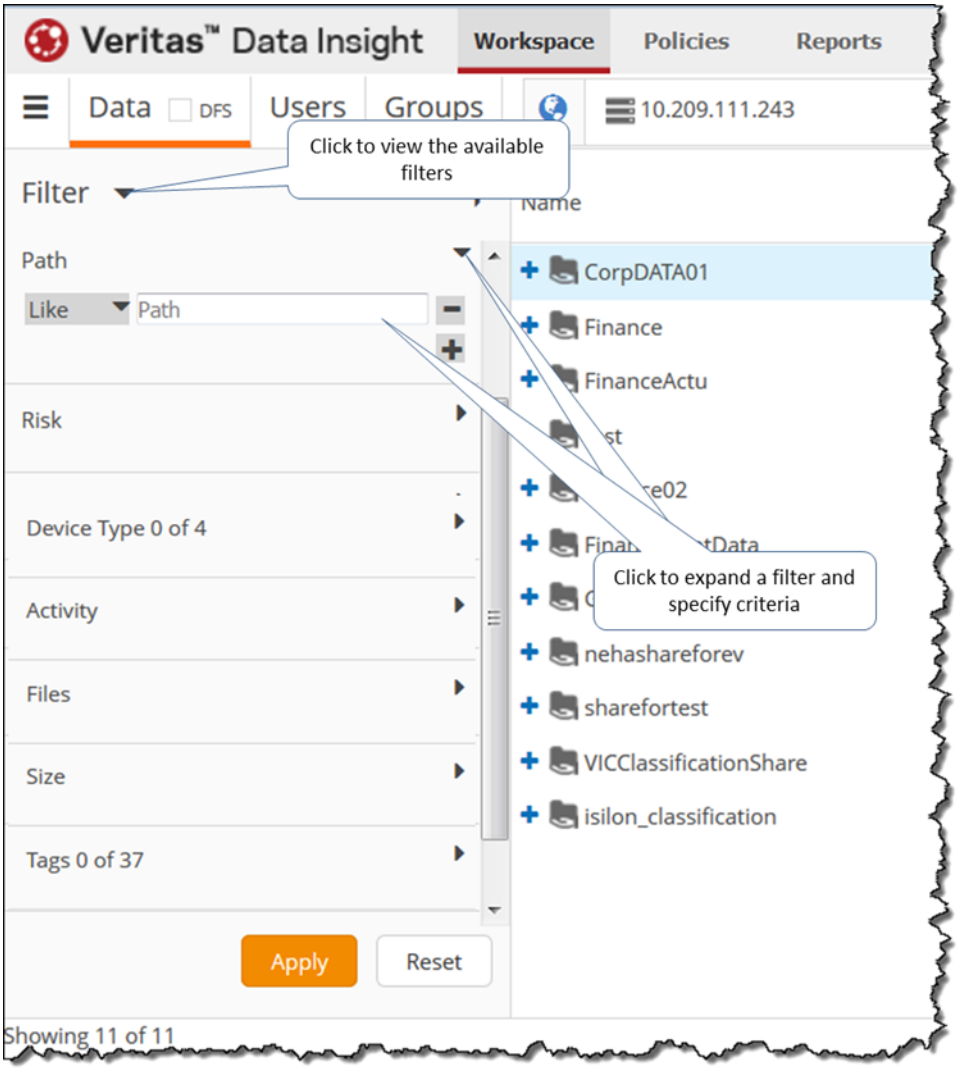
See "Managing the Workspace" on page 34.

See "Using the Workspace filters" on page 31.

Using the Workspace filters

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

Figure 3-1 Workspace filters



To use the filters

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

   The filter panel expands to show the available filters.

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

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

   If a filter has many possible values, you can enter specific value in the search bar for that filter.

   For example, if there are multiple tags, you can enter that name of the tag that you are interested in the **Tags** filter. Or select the tag(s) to review the files that match the selected tags.

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

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

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

Filter	Description
Disabled	Displays disabled users, filers, shares, or equivalent data sources.
Deleted	Displays all users that have been deleted from the directory service. This filter is only available on the **Users** list view.

Filter	Description
Custodian	On the **Data**and **Shares** list view, the filter displays all users who are assigned as custodians on paths. On the **Users** list view, select **Custodian** check box to displays all paths on which a user is assigned as custodians.
Control Point	Displays the number of control points across configured shares or site collections. On the **Shares** list view, select the **Control point** check box to display all paths in the file system hierarchy where the permissions differ from that of the parent folder or where the active users differ significantly from active users of its sibling folders.
User Name / **Group Name**	Displays analytics pertaining to the specific user or group.
Open Shares	This filter option is only available on the **Data Sources** and **Shares** list view. On the **Data Sources** list view, you can further refine the condition by selecting the size of the share and the number of files on the open shares. Displays all open shares across all configured filers or on selected filers.
Path	For a share, enter the full or part of the path name, IP address, or URL as the case may be.
Risk	Use the slider to enter a value for the risk score. The threshold for the risk score for users and data sources is 50. A risk score more than 50 may be a cause for concern. This filter condition is available for the **Data Sources**, **Shares**, and **Users** list view.
Device Type	Select the type of device for which you want to view analytics.
Activity	Use the slider to specify the number of accesses. For example, you can use the **Activity** filter with the **Device Type** condition to search for all NetApp filers that have accesses between 50000 and 700000. On the **Data** list view, you can also select the type of activity for which you want to view analytics - None (No activity), Collaborative, or Single user.

Filter	Description
Files	Use the slider to choose the number of sensitive, active, or inactive files in a content repository. For example, you can use the **Files** criteria along with the **Device Type** filter to find the number of sensitive files on a Box share.
Size	Use the slider to choose the size of active and inactive files. The size criteria refers to the logical size of the files. For example, you can choose to view analytics for active files that more than 2 GB in size.
Tags	Select one or more policies that are matched by files or folders being monitored by Data Insight. For example, you can search for all files that violate the conditions specified by the US-PII policy and match the tags configured for that policy.
Domain	From the list of configured domains, select the domain for which you want analytics data. Click **More** to display all domains configured in Data Insight. Or enter the name of a domain in the search bar to search for a specific domain.
Owner	Enter the name or part of a name of the owner of a file or folder. The criteria for computing the owner of a data resource is configured in the Workspace Data Owner Policy. For more information, see the *Veritas Data Insight Administrator's Guide*.
Custom attributes	Select one or more values for all or any custom attribute. The attributes that are displayed as filters depend on the custom attributes that are configured in Data Insight.

Managing the Workspace

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

See "About the Data Insight Workspace" on page 27.

The list views on the **Workspace** tab provide advanced analytics about configured data sources and users that Data Insight monitors.. The list views also provide a

high-level summary of the configured storage devices and users from the perspective of space utilization, activity, number of sensitive files, and permissions.

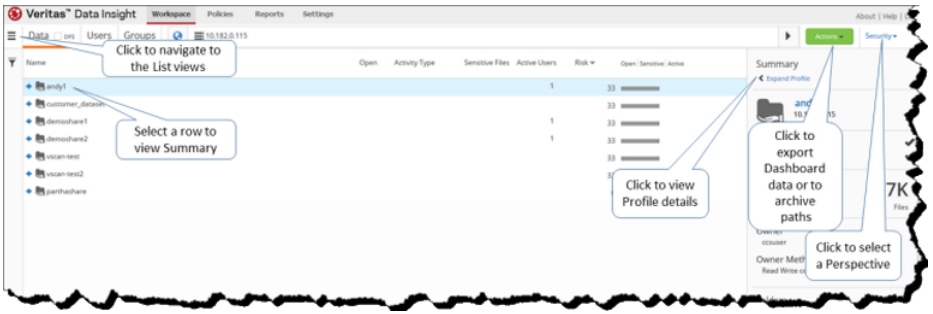
You can further navigate to the underlying profile views that provide analytics on activity and permissions from the list views.

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

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

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

Figure 3-2 Working with the list-views



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

Changing your current View

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

To change the currently displayed view

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

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

2. Select **Create View**.

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

To extract the contents of the dashboard

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

See "Using the Workspace filters" on page 31.

Searching the storage device hierarchy

.

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

You can navigate shares, sites, and folder hierarchy.

To search for a storage device

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

You can view the sibling paths of the filer, share/site collection/equivalent data source (such as a OneDrive user account or a Documentum repository), or folder on the path that you type in the **Go to** bar. Click the drop-down arrow to view the list of all the siblings of a particular entity. You can also apply the filter on a sibling path to directly access a particular entity.

See "Viewing the overview of a data source " on page 54.

Searching for users and user groups

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

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

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

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

Using filters	To search for users or groups, click the filter icon and select your filtering criteria. See "Using the Workspace filters" on page 31. Use the **Domain** condition to filter default Windows Built-in users and groups, such as the Everyone group, unresolved SIDs, and users and groups from migrated domains. Unresolved SIDs result when users or groups are deleted in the directory service, and Data Insight cannot map them to users or groups in the Data Insight users database. See "About migrated domains" on page 19.
Using the Go To bar on the Dashboard and list views	Enter the name or security identifier (SID) value of a user or group.

See "Viewing the overview of a user" on page 72.

See "Viewing the overview of a group" on page 73.

Chapter 4

Analyzing data using the Workspace views

This chapter includes the following topics:

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

About information risk

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

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

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

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

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

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

See “Viewing shares summary” on page 41.

Viewing summary of data sources

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

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

- The total number of files on the open shares on a data source.
- The disk space occupied by the open shares.
- Number of sensitive files present in a data source.
- Number of users with activity on the data source.

- Risk score assigned to the shares or site collections under the data source.
  The bubble chart is divided into ten buckets, with each bubble signifies a risk range. The higher five buckets are orange and signify a higher risk range. The size of the bubble signifies the percentage of shares or site collections on a data source that are in a particular risk range.
  See "About information risk" on page 38.
- Total activity reported for the data source.
- Total number of files with activity and the number of active users.
- Total number of files contained, the disk space occupied by the contents, the inactive users, and inactive data size on the data source.

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

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

- Details of the attributes of the users who have activity on the data source.

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

- Details of active, inactive, and sensitive files.
- The overview of the data source
  See "Viewing the overview of a data source " on page 54.
- Details of custodians assigned for the data source.
  See "Managing data custodian for paths" on page 55.

See "Managing the Workspace" on page 34.

See "About the Data Insight Workspace" on page 27.

Viewing shares summary

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

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

- Information whether a share is an open share.
- The type of activity that is reported for the share. For example, none (no activity), single user, multi-user, or collaborative activity.
- Number of sensitive files present on the share.
- Total number of active users.
- The risk score of a share considering the maximum number of users with permissions on the share, the active user count, and the sensitive file count of the share. A higher count of users who access the share and sensitive files on the share contribute to a higher risk for a share.
  See "About information risk" on page 38.
- Total access count reported on the share.
- Total number of active files present in the share.
- Total files present in the share.
- Disk-space occupied by the share.
- Inactive data size.

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

- Information whether the share is an open share.
  For information about open shares and configuring an open share policy, see the *Veritas Data Insight Administrator's Guide*.
- Whether the share is a control point.
  See "About control points" on page 43.
- The owner of the data source and the Workspace Data Owner Policy that is used to compute the owner.
- Total disk-space occupied by the share.
- Total number of files present on the share.
- Details of the user who owns the share.
- Counts of folders, active users, and control points present in the share.
- Counts of active, inactive, and sensitive files present in the share.
- Risk-score for the share.
- The tags assigned to the files on the share. This is a consolidated list of tags derived from Veritas Information Classifier and Symantec Data Loss Prevention.
- The custodian assigned on share.
- Attributes of the users who have activity on the data source.

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

See "Managing data from the Shares list view" on page 221.

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

- View overview information for the share or site collection.
  See "Viewing the overview of a data source " on page 54.
- View and assign custodian
  See "Managing data custodian for paths" on page 55.
- View details of user activity on the paths.
  See "Viewing user activity on files or folders" on page 58.
- View details of activity by configured users on the paths.
  See "Viewing file and folder activity" on page 62.
- View the details of permissions on the paths.
  See "Viewing CIFS permissions on folders" on page 63.

- View audit logs.
  See “Viewing audit logs for files and folders ” on page 66.

About control points

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

Control points can be any of the following:

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

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

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

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

About the risk score for users

Data Insight enables you to monitor malicious activity in your storage environment. Data Insight profiles all users by assigning a risk-score to every configured user. It displays the riskiness of a user in terms of a numerical score that ranges from 0 to 100. Higher the risk score of a user, higher is the perceived risk posed by the user.

The risk score places each user at a relative distance from other users and orders them in accordance with how risky a user is in comparison to other users.

A risky user typically displays anomalies such as:

- The fraction of the total number of data sources that a user has permissions on. (Access)

- Abrupt deviation in activity pattern where deviation on activity on sensitive files is given more weightage. (Anomaly)
- Abnormal increase in number of alerts against the user. (Alerts)

Note that the user risk score is computed by considering the individual scores of different parameters for the last 15 days by default. The user risk score is calculated on a daily basis and stored for the last 180 days.

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

- Identify potentially malicious users.
- Review the permissions that are granted to the users.
- Review if a risky user is a custodian on any storage resource.
- Review the top active and sensitive data that is being accessed by the risky user.
- Add a user with a high risk score to a watchlist to enable you to closely monitor the user's activities.

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

Table 4-1 Components for computing user risk score

Components	Descriptions
Deviation in accesses pattern on sensitive and non-sensitive files.	The overall deviation score is the weighted sum of the deviation values for sensitive and non-sensitive files.
Number of alerts against the user.	Percentage of alerts for a user against the total number of alerts, weighted by the severity of the policy that was violated.
Number of shares the user has read/write access on.	Percentage of shares on which the user has read access, against the total shares across all the storage devices.
Number of shares the user has write access on.	Percentage of shares on which the user has write access, against the total shares across all the storage devices.
Number of shares the user is custodian on.	Percentage of shares for which the user is a custodian, against the total shares across all the storage devices.

Table 4-1 Components for computing user risk score *(continued)*

Components	Descriptions
Deviation in the number of unique files that are accessed by the user. (Considering sensitive and non-sensitive files)	Overall score is the weighted sum of unique files that are accessed during past 15 days.
Deviation in the number of unique files that are accessed by the user. (Considering sensitive files only)	Overall score is the weighted sum of unique files that are accessed during past 15 days.
Deviation in the number of distinct DLP policies violated by the files accessed by the user.	Overall score is weighted sum of DLP policies. The weights are proportional to the severity level of the policies.

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

The User Risk Dossier provides the next level of details of the factors that contribute towards the user risk score.

See "About the Risk Dossier" on page 45.

See "About the Data Insight Workspace" on page 27.

See "Viewing user summary" on page 50.

About the Risk Dossier

The Risk Dossier for a user provides the next level of detail into the user risk score. The Risk Dossier displays visualizations that provide more insight into the factors that contribute to the risk score and explains why a user is considered risky. The Risk Dossier also helps you investigate reasons for a spike in the risk score in the past by answering questions such as:

- What is the historical risk landscape for a user?
- Why is risk score high for a user on a given date?
- What contributes to the risk score?
- How can we mitigate the risk?

You can navigate to the user Risk Dossier from any of the following pages in the UI.

- On the **Users** tile of the Data Insight Dashboard, click the graph icon.

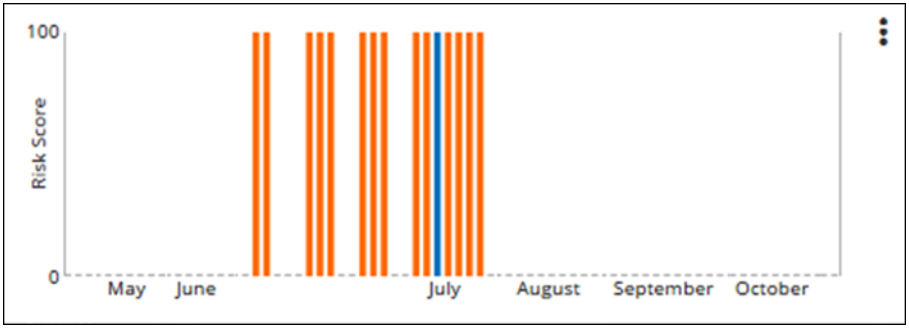
- Click **Workspace** > **Users**. On the **Users** list page, select a user and click **Expand Profile**, and then click **Risk Dossier**.
- Alternately, on the **Users** list page, click the graph icon in the **Summary** panel to maximize the risk dossier view. Close the view to return to the previous page.

Note: The Risk Dossier view is visible only to the users assigned the Server Administrator role.

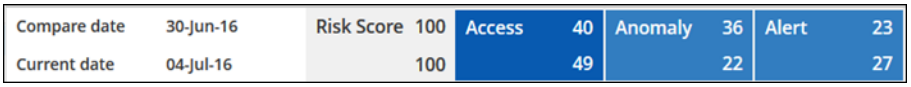
Risk Dossier visualizations

The Risk Dossier tab provides the following visualizations for a user's risk score:

- The risk history graph shows the risk score of a user for the configured analytics period. The graph gives you an idea of how the risk score for a user is moving. A sudden spike in the risk score may warrant an investigation. You can click on a date on the risk history graph to know the composition of the risk score for the Access, Anomaly, and Alerts factors as of that date.
  See "About the risk score for users" on page 43.



- Cards that display the breakup of a user's risk score on a date selected in the **Risk History** graph, with details of the individual scores of the different factors that constitute the risk score (Access, Anomaly, and Alerts). The cards also let you compare the risk score factors for a historical date with the factors as of the current date.
  Click on any of the three risk score factors, namely Access, Anomaly, and Alerts to get to further details about the nature of the risk score factor contributing to the score on that day.



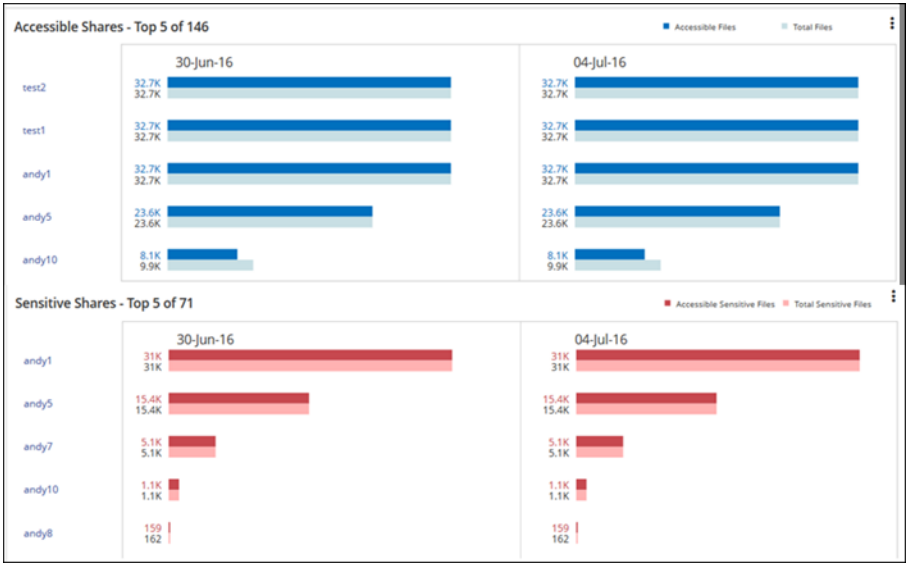
- The user risk factor (Access) displays the potential for damage from a high-risk user. The view provides a bar graph that displays the top accessible and sensitive shares and compares the number of accessible files to total files. The graph

also compares the access information from the current date with that on a historical date. Additionally, it provides the count of accessible shares.

To further assess the permissions on a share, click on the share names in the **Accessible Shares** or the **Sensitive Shares** graphs to navigate to the permissions view for that user for the share.

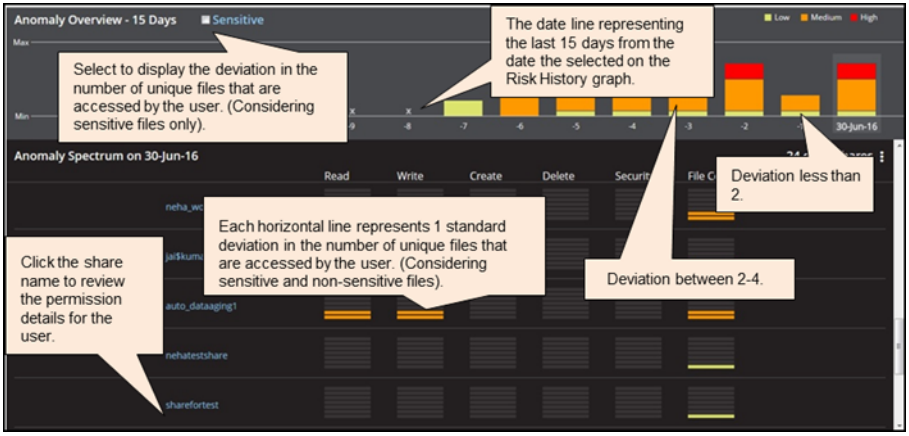
The graphs provide the following insight into what is at stake if a user were to become malicious:

- The **Accessible Shares** graph shows the top five shares based on the number of accessible files by the user in a particular share. This graph gives you an idea of the amount of data that a high risk user has access to. You can use the information to protect against any malicious activity that the user may perform. You can also perform a comparative analysis of the number of files accessible to the user during the current date and a historical date on the risk history graph.
- The **Sensitive Shares** graph gives you a comparative analysis of the total sensitive files on the top 5 sensitive shares and the number of sensitive files that the user can access on those shares.



- Data Insight takes into account the deviation in the activity pattern (anomaly) observed in the last 15 days for calculating the risk score for a user. The anomaly spectrum displays the deviation (over average of the last 180 days) for each counter that Data Insight monitors - read, write, create, delete, security, and file count.

Click on a day in the **Risk History** graph and the anomaly spectrum is calculated for the last 15 days from the current day.



- Click on the **Alerts** card to review the alerts raised against the selected user. The **Alerts Overview** graph displays the frequency of alerts based on severity (low, medium, high) for the last 15 days from the date selected on the Risk History graph.
  The list of policies that the user has violated along with the policy configuration details are also displayed below the graph.



You can choose to disable the user risk dossier computation which provides the data for the Risk Dossier graphs. Run the following command on the Management Server to set a global configuration property:

```
configdb -O -J disable_dossier -j true
```

The Risk Dossier database is deleted by default after 3 months. The purging period can be changed by running the following command on the Management Server.

```
configdb -O -J purge_dossier_months -j <number in months>
```

For example, to set the purging period to 3 months, run the command:

```
configdb -O -J purge_dossier_months -j 6
```

Note: If you configure a higher purge period, you will need to provision more storage on the Management Server for storing the dossier data.

Assessing risky users - an example scenario

This section explains the use of the user risk dossier with the help of an example.

The **Workspace** > **Users** list view shows a group of users with a high risk score. Or the risk history graph for a user displays an upward trend in the moving average of the risk score.

Use the risk dossier to dive into the details of the reasons for the high risk score. and to do a comparative analysis of the factors contributing to the risk score between a date in last six months and the current date.

The next steps should be to ascertain why the users display a high risk score. Select a potentially high-risk user based on the risk score (for example, a risk score of more than 90 for a user may warrant some investigation). For this user, determine the following:

- The number of alerts generated for that user. Investigate the policies that the user has violated and the severity of the policies that has led Data Insight to generate an alert.
- The anomalies - the shares and the access types (op codes) for which deviations are observed. You can either investigate the user by looking at the user's audit history for that day. You can also generate access details report for that user only for that day.
- The shares on which the user has access. One of the reason for a high risk score can be that the user has access to a large number of shares. The access could be provided through various groups.
- Run the **Risky Users Group DQL** query to get the groups through which the user has access to those shares.
- Explore the user attributes of the above user to get a hint of the groups that the person should be in.

  Run the **Risky Users Outlier** DQL query to identify any outlier user with respect to the user attributes compared against all high-risky users.

  Typically, Administrator users may show up in the report output due to high access. But the high access to any other type of user should be investigated.

Once you have determined the reasons for a high risk score, you can do the following to further drill down and take remediation actions:

- Click on the share name in the **Access** > **Accessible Shares**/ **Sensitive Shares** to navigate to the **Permissions** tab or the **Anomaly Spectrum** graph to navigate to the Audit Logs tab .
- To get exact details of the permissions due to which the user has high access, create a Permission Search report scoped on selected shares to report on all groups that the user is part of which may have granted permission to the user on some of these shares. You can then evaluate whether the user has excessive privileges. The report may help you understand if the user is accidentally added to a group which may have given the user excessive privileges.
- Explore group memberships and if required, use the custom action framework (**Settings** > **Permissions** > **Remediation**) to change group memberships to align user accesses if found to be excessive. It can also be used to change CIFS permissions, if required.
  For more information about configuring permissions remediation, see the *Veritas Data Insight Administration Guide*.

Viewing user summary

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

The following details are displayed:

- The grouping attribute of the user.
  For more information about configuring the primary grouping attribute, refer *Veritas Data Insight Administrator's Guide* .
- The total activity by the user across configured devices for the last 15 days .
- The number of number of unique files accessed by the user in the last 15 days.
- The risk-score of the user.
  An orange bar graph denotes a risk score of more than 50.
  See “About the risk score for users” on page 43.

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

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

- The status of the user - whether the user is disabled or deleted.
- The attributes configured for the user.
- The risk score assigned to a user.
- The top shares the user has activity on.

- A graphical representation of the user's activity profile over the configured advanced analytics period.
- The breakdown of the type of accesses made by the user, such as the number of reads, writes, deletes, etc.
- The Data Loss Prevention (DLP) policies that the user has violated in the last 15 days.
  Data Insight integrates with DLP to pull data classification information. However, the classification information can also be imported into Data Insight by using a CSV file.

Click the graph icon next to the risk score on the list view and the **Summary** panel to open the Risk Dossier for a selected user.

See "About the Risk Dossier" on page 45.

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

- The overview of the user's attributes, such as display name of the user, the SID, the attributes configured for the user, and the groups the user belongs to.
  See "Viewing the overview of a user" on page 72.
- The details of the paths on which the user is assigned as custodian.
- The details of accesses made by the user, arranged by time and by folders.
  See "Viewing folder activity by users" on page 75.
- The permission details for a selected user.
  See "Viewing SharePoint permissions for users and user groups" on page 79.
- Audit logs for the user.
- See "Viewing audit logs for users " on page 81.

Viewing details of Watchlist users

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

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

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

- The primary grouping attribute configured for the user.
- The number of shares on which the user has activity.
- The number accesses made by the user.
- The number of shares on which the user has permissions.
- The number of files accessed by the user.
- The number of sensitive files accessed by the user.
- The risk score of the user.
  See "About the risk score for users" on page 43.

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

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

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

See "Viewing user summary" on page 50.

See "About the Data Insight Workspace" on page 27.

Viewing details of alert notifications

The Alerts list-view displays the following details:

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

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

Chapter 5

Viewing access information for files and folders

This chapter includes the following topics:

- About viewing file or folder summary
- Viewing the overview of a data source
- 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 Box permissions on folders
- Viewing audit logs for files and folders
- About visualizing collaboration on a share

About viewing file or folder summary

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

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

Viewing the overview of a data source

To view the attributes of a folder

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

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

   - The physical and logical size of the data.
   - The date on which the file or folder was created and the name of the creator
   - The date on which the file or folder was last modified.
   - In case of a file, the date on which it was last accessed.
   - The last Read and Write activity on the path based on the access events received by Data Insight. If the data repository has not been scanned for any reason, **Data not available** is displayed.
   - If the path is a control point, the date on which and the reason why the folder is identified as such.
     See “About control points” on page 43.
   - The list of assigned or inherited custodians.

- The list of all the files contained in the folder.

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

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

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

See "Managing data custodian for paths" on page 55.

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 equivalent data source or a folder:

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

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

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

To assign a custodian do the following

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

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

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

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

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

5 To assign a specific user as a custodian for the path, click the Settings icon and, from the drop-down list select **Add Custodian** > **Select User**.

6 Enter the name of the user in the Search field. Select the appropriate user from the search results, and click **OK**.

You can filter users by domain or by using attribute-based queries.

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

8 To assign a custodian based on user or group attributes, click **User** or **Group** radio button or enter a user/group name in the search bar.

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

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

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

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

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

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

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

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

To delete a custodian do the following

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

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

3. Click a folder. The **Summary** panel populates to display additional details. Click the profile arrow. The **Summary** panel expands to display the profile view.
4. On the **Overview** tab of a resource, you can view the list of custodians assigned or inherited for that path. You can delete custodian assignments for a path in the following two ways:
   - Select the assigned custodian and click the delete icon.
   - To explicitly remove all custodian assignments for a path, click the custodian icon and select **Remove all**.

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

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

Viewing the summary of user activity on a file or folder

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

1. From the **Workspace** tab, navigate to the **Data Sources** list-view.
2. Expand a data source to display a list of configured shares, site collections, or equivalent.
3. Expand a share, site collection, or equivalent to view the folders, sites, document libraries, or picture libraries present within the share or the site collection.
4. Click a folder. The **Summary** panel populates to display additional details.
5. Click **Expand Profile** on the **Summary** panel to display the underlying folder-centric views.
6. By default, the **Overview** tab displays the a summary of the selected data repository.
7. Click **User Activity**.
8. By default, the **Summary** sub-tab displays the following attributes of the folder for the last six months from the current date:

- The user who created the file or folder.
- The user who last modified the file or folder
- The inferred data owner.
- The last access date.
- The total access count of the inferred data owner, including the number of read events and write events.
- A graphical view of the total access count for the top five users of the selected file or folder.
  Click on a section of the pie-chart to view the detailed audit logs for a user.
  See "About audit logs" on page 18.
  See "Viewing audit logs for files and folders " on page 66.
- A tabular view of the access pattern of the top five users of the selected file or folder.

9 To view the summary of the user activity for the folder for a specific time period, enter the start and end dates in the **To** and **From** fields, and click **Go**.

Viewing user activity on files or folders

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

To view user activity on a file or folder

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

2 Expand a data source to display a list of configured shares, site collections, or equivalent.

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

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

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

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

6 Click **User Activity**.

7 By default, the **Summary** sub-tab displays the following attributes of a selected path for the last six months from the current date:

- The user who created the file or folder.

- The user who last performed the write activity on 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 *Veritas Data Insight Administrator's Guide*.

  Note: All Activity Count includes all activities except permission change.

  You can also assign an inferred data owner as custodian for that location.
  See "Assigning an inferred data owner as custodian" on page 60.
- The last date on which any activity was done this path.
- The total activity count of the inferred data owner, including the number of read 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 18.
  See "Viewing audit logs for files and folders " on page 66.
- A tabular view of the access pattern of the top five users of the selected file or folder.

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

The page 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 60.

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

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

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

Note: If a domain, say A, migrates to domain B, then **Inactive Users** tab shows inactive user accounts from domain B. The view takes into account the activity of each user from both the domains.

---

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

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

Assigning an inferred data owner as custodian

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

To assign a custodian

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

2 Expand a data source to display a list of configured shares, site collection or equivalent.

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

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

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

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

6 Click the **User Activity** tab.

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

8 Right-click the inferred data owner, and select **Add as Custodian**. For assigning a custodian, See “Managing data custodian for paths” on page 55.

Assigning an active user as custodian

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

To assign an active user as a custodian

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

   By default, the **Overview** tab displays the a summary of the selected data repository.
6. Click **User Activity** tab.
7. Click the **Active Users** sub-tab to display a list of active users.
8. From the list displayed, right-click the user you want to assign as a custodian and select **Add as Custodian**.
9. Click the **Overview** tab for the path to verify whether the user is added to the list of custodians for that path.

See "Managing data custodian for paths" on page 55.

Assigning a custodian from the Permissions tab

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

To assign a custodian

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

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

6 Click **Permissions** tab.

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

See "Managing data custodian for paths" on page 55.

Viewing file and folder activity

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

To view activity on a file or folder

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

2 Expand a data source to display a list of configured shares, site collections or equivalent.

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

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

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

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

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

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

- **By Time** - Click this sub-tab to view the number of Read, Write and Other activity on the selected file or folder for a specified time period. You can also view a graphical representation of the activity counts during each month in a specified time range.
- **By Subfolders and Files** - Click this sub-tab to view the Read, Write, and Other activity 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 activity 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 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 223.

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

See "Using custom scripts to manage data" on page 226.

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

Viewing CIFS permissions on folders

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

To view the permissions on folders

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

2 Expand a data source to display a list of configured shares, site collections, or equivalent.

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

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

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

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

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

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

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

7 Click the **Include share level permissions** check box to include share-level permissions when computing effective permissions.

Note: If you select the **Include share level permissions** option, Data Insight replaces any user/group that has explicit permissions on the path and has migrated to a new domain, with the corresponding new account.

---

8 Click **File System Access Control List** to view a list of all the users or groups, who have an Access Control Entry (ACE) defined on that folder. The ACE can be inherited or explicitly defined.

9 Click **Share-level permissions** to view a user's or a group's share-level permissions.

10 Click **Advanced permissions**, in each sub-tab, to view the details of the operation that a user or a group is allowed or denied on that folder.

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

See "About permissions " on page 14.

Viewing NFS permissions on folders

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

To view the permissions on folders

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

2 Expand a data source to display a list of configured shares, site collections, or equivalent.

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

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

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

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

6 Click **Permissions**.

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

Viewing SharePoint permissions for folders

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

To view SharePoint permissions

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

   By default, the **Overview** tab displays the a summary of the selected data repository.
6. Navigate to the path for which you want to view the permission details.
7. Click **Permissions**.

   A summary of the users and the roles assigned to them appears. The roles include the tasks that a user is allowed to perform.
8. Select a role assigned to a user to view all the permissions assigned to that particular role.

Viewing Box permissions on folders

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

You can see Box permissions after the localuserscan job and the Active Directory scan have run.

See "About Box permissions" on page 16.

To view Box permissions

1. From the **Workspace** navigate to the **Data Sources** list-view.
2. Expand a configured Box account to display a list of configured user accounts.

   The different user accounts correspond to folders on a file share.
3. Expand a user account to view the folders that the user has access to.
4. Click a folder. The **Summary** panel populates to display additional details.

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

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

6 Click **Permissions**.

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

The permissions view for folders shows the users and groups that have permissions on the selected folder and the access level that the user or group has. However, for groups, Data Insight does not display the number of users that are part of the group. If the Box user is not mapped to a user in Active Directory, only the user's email ID is displayed and you can not cross launch to other tabs using the right-click menu. Also, such users will not appear in Entitlement Review report and User/Group Permissions report.

To view the members that are part of a Box group that has permission on the folder, right-click the group name and select **Members**. You can also generate a Entitlement Review report to review the members that are part of a Box group.

Box does not allow assignment of permissions at the All Files folder-level, account user name-level and share-level. As a result, Data Insight does not display any permissions for these levels.

Viewing audit logs for files and folders

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

To view audit logs for files and folders

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

See "About viewing file or folder summary" on page 54.

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

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

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

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

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

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

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

8 Click **Go**.

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

9 The audit logs provide the following information:

- The name of the user who generated the event.
  In case of an Permission Change event, Data Insight displays the name of a fictitious user. You can view the details of the event in the **Other Info** column, however the name of the user is displayed as _DI_PERMCHG_DUMMY_USER_.
  See "About audit logs" on page 18.
- The name of the file that is accessed.
- The path of the file.
- The type of access event.
  In case of a folder on a SharePoint site, the SharePoint access type such as checkout, view, check in, write, update, delete, and move to Data Insight meta access types - Read, Write, Create, Delete, and Rename.
  Permission Change events are represented by the access type - PERMCHANGE.
- The type of file
- The access count
- The IP address of the computer from which the file was accessed.
  Currently, you cannot view the IP address of the computer from which the file was accessed for Windows File Servers, VxFS filers, and SharePoint sites.

In case of an Permission Change event, the IP address is displayed as 0.0.0.0.

- The start and end time for the time window in which the event occurred.

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

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

To filter the audit logs

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

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

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

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

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

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

About visualizing collaboration on a share

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

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

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

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

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

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

- Analyze the activity pattern among users and groups and identify the level of collaboration on a share.
- Identify the pattern of collaboration between different cluster groups.
- Collaborative activity on a share.
- Identify weakly-connected users who are not collaborating within a folder, but have activity on the share.
- Visualize the various organizational units that may be collaborating on a share.
- Identify and analyze outlier users based on organizational units and other attributes.
- Export the graph along with information about user attributes and degree of collaboration to an output file.

Analyzing activity on collaborative shares

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

Viewing the pattern of collaboration on a share

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

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

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

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

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

   - The number of active users collaborating on the share
   - The number of sensitive files on the share
   - The number of weakly-connected users, if any
   - The list of cluster groups in the graph
   - The primary attribute that is configured for users in each cluster group, and the number of users for each attribute value.
6. Click a cluster group to view the top folders under which the users in the cluster are collaboraitng. You can also view the number of users for each attribute value in the cluster group.

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

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

8 To further analyze the data

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

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

---

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

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

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

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

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

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

Chapter 6

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 Box permissions for users and user groups
- Viewing audit logs for users

Viewing the overview of a user

To view the attributes of a user

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

3. Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.
4. By default, the **Overview** tab displays the following summary of the selected user:
   - The list of all the groups of which the user is a member.
     You can view the groups of which the user is a primary member and the groups in which the user has inherited the membership. The differentiation between direct and indirect group membership enables you to make relevant permissions changes.
     For information about configuring permission remediation, see the *Veritas Data Insight Administrator's Guide*.
   - The directory domain attributes of the user.
5. Click **Export** to export the information on the page to a `.csv` file.
6. You can also assign or delete custodian assignments from the **Overview** tab.

   See "Managing custodian assignments for users " on page 74.

See "About the Risk Dossier" on page 45.

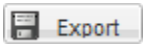
Viewing the overview of a group

To view the attributes of a user group

1. From the drop-down menu on the **Workspace** tab, select **Groups**.
2. On the **Groups** list view page, select a group. The **Summary** panel populates to display additional details about the group.
3. Click **Expand Profile** on the **Summary** panel to display the underlying user-centric views.
4. By default, the **Overview** tab displays the following summary of the selected group:
   - The directory attributes of the group.
   - A list of the other groups of which the selected group is a member. The view also displays the differentiation between the selected group's direct and indirect membership of other groups.

- A list of the members in the group.

5 Click an icon to do the following:

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

Managing custodian assignments for users

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

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

To assign a custodian location

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

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

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

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

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

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

6. You can drill down the **Physical** or **DFS** hierarchy to view the children data locations for which the user is a custodian.
7. To assign the user as the custodian for a particular path, click the Custodian icon and select **Add Location**.
8. Select the **Physical** or **DFS** radio button.
9. Select the location, and click **OK**.
10. To view a list of all the data locations in a domain on which the user is a custodian, click the **View All Assignments** button. A list of all the paths for which the user is a custodian is displayed.

To remove all custodian locations

1. On the **Custodian** tab, click the data custodian icon and select **Remove All**.
2. Click **Yes** on the confirmation message.

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

To view/export custodian information for a user

1. To view a list of all the data locations in an enterprise on which the user is a custodian, click the Custodian icon, and select **View All Assignments**. A list of all the paths for which the user is a custodian is displayed.
2. Click the Email icon to email custodian assignment information to desired email recipients.
3. Click the Export icon at the bottom of the page to export the data on the screen to a `.csv` file.

Viewing folder activity by users

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

To view user activity on a file or folder

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

   By default, the **Overview** tab displays the a summary of the selected user.
4. Click **Activity**. Or right-click the user in the navigation pane and select **Activity**.

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

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

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

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

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

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

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

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

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

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

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

Viewing CIFS permissions for users

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

See “About permissions ” on page 14.

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

To view the permissions assigned to a user

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

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

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

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

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

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

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

Viewing CIFS permissions for user groups

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

See “About permissions ” on page 14.

To view the permission assigned to a user group

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

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

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

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

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

Viewing NFS permissions for users and user groups

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

To view the permissions assigned to a user or user group

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

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

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

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

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

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

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

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

Viewing SharePoint permissions for users and user groups

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

Note: Data Insight does not fetch permissions for the SharePoint Online data source.

To view the SharePoint permissions assigned to a user

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

   By default, the **Overview** tab displays a summary of the selected user
4. Click **Permissions**. Or, right-click the user in the navigation pane, and select **Permissions**.
5. Enter the URL of the site in the **Select Share or Site Collection** field and click **GO**. Or, click the search icon and from the **Select Resource** widget select a URL and click **OK**. A pop-up displays the list of children of the selected. It also displays the roles for the selected users.

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

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

   At the share-level in the hierarchy, you can also filter the paths using other predefined filters, such as disabled share or site collections where the user has permissions.
6. A summary of the permissions that are assigned to the user on the selected site collection appears. It includes the following details:
   - The path at which the access control entry has been defined for the user or the group to which the user belongs.
   - The type of role.
   - Unique permissions defined on:

      The folder and its descendants.

      The descendants.

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

Viewing Box permissions for users and user groups

You can view details of the Box permissions for a user or group on the **Permissions** tab.

See "About Box permissions" on page 16.

To view the Box permissions assigned to a user or group

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

   By default, the **Overview** tab displays a summary of the selected user
4. Click **Permissions**. Or right-click the user in the navigation pane, and select **Permissions**.
5. Use the device filter in the content pane to search for specific devices where the selected user has permissions. The **Devices with permission** filter is applied by default. The filter pane displays the list of devices on which the selected user has permissions. Or, click the drop-down to select a specific type of storage device where the user has permissions.
6. The effective permissions view shows the paths with unique permission levels. The view shows the all folders that the user has access to and the user's permission level on that path. All folders under that path will have the same permission and thus are not displayed individually. If a sub-folder's permission is changed, that path is displayed in the list of paths.

   A summary of the permissions that are assigned to the user on the selected folder appears. If more than one user is collaborating on the folder, Data Insight does not display any information on how the sharing occurred (by using a shared link or by invitation), and also does not give any detail on whether link is publicly available, and whether it has any expiry date.

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 18.

To view the audit logs for users

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

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

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

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

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

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

   - The name of the file that is accessed.
   - The path of the file.

- The type of access event.
  In case of a folder on a SharePoint site, the SharePoint access type such as checkout, view, check in, write, or update.
- The type of file.
- The access count.
- The IP address of the computer from which the file was accessed.
  Currently, you cannot view the IP address of the computer from which the file was accessed for Windows File Servers, VxFS filers, and SharePoint sites.
- The start and the end time of the access events.

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

Section 3

Data Insight reports

- Chapter 7. Using Data Insight reports
- Chapter 8. Managing reports

Chapter 7

Using Data Insight reports

This chapter includes the following topics:

- About Data Insight reports
- How Data Insight reporting works
- Creating a report
- About Data Insight security reports
- Create/Edit security report options
- Data Insight limitations for Box permissions
- About Data Insight storage reports
- Create/Edit storage report options
- About Data Insight custom reports
- Considerations for importing paths using a CSV file

About Data Insight reports

Data Insight includes several report categories which enable you to do the following:

- Monitor activity on the filers, SharePoint web applications, Documentum repositories, and cloud storage resources
- Make decisions about the best way to use the storage on configured resources
- Analyze the permissions assigned to users and groups to make appropriate remediation decisions.
- Create custom reports using Data Insight Query Language (DQL).

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 data source has not been completed at least once, the data in the reports may not be accurate.

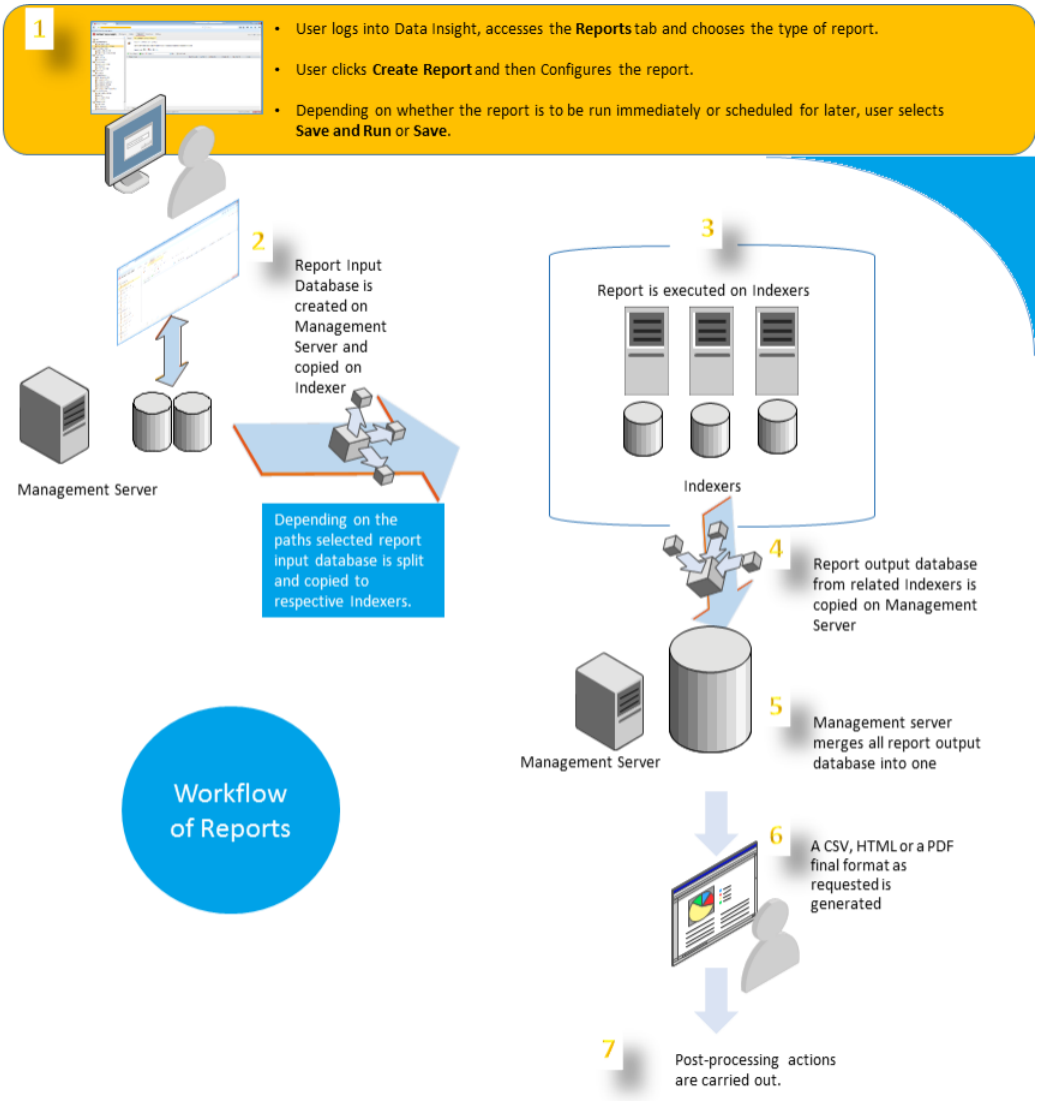
Reports are available for the following categories:

Activity Summary Reports	See "Activity Summary reports" on page 121.
Activity Details Reports	See "Activity Details report" on page 89.
Permissions Reports	See "Permissions reports" on page 90.
Capacity Reports	See "Capacity reports" on page 122.
Ownership Reports	See "Ownership Reports" on page 107.
Custom Reports	See "About Data Insight custom reports" on page 140.
Data Lifecycle Reports	See "Data Lifecycle reports " on page 124.
Consumption Reports	See "Consumption Reports" on page 126.

See "About stale information in reports" on page 158.

How Data Insight reporting works

Figure 7-1 Workflow of Data Insight reports



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 109.

See "Create/Edit storage report options" on page 131.

See "Create/Edit DQL report options" on page 149.

See "Create Permissions Search report" on page 92.

See "Creating a Permissions Query Template" on page 94.

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.

Note: When you create a report, you can specify the path where you want to copy the report output to. You must specify the path which already exists; Data Insight does not create a new folder when copying a report. Check the number of network connections that are allowed on the folder. If the folder is in use by any application including Windows Explorer, copying the report may fail. Also, ensure that the Windows Secondary logon service is enabled on the Management server.

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

See "Considerations for viewing reports" on page 167.

About Data Insight security reports

Use Data Insight security reports to view and export the activity details for the configured data sources and by the configured users.

You can view custodian reports for various data locations.

You can create security reports for the following categories:

- Activity Details reports
  See "Activity Details report" on page 89.
- Permissions reports
  See "Permissions reports" on page 90.
- Ownership Reports
  See "Ownership Reports" on page 107.

Activity Details report

Use the Activity Details reports to view the type of access events by selected users or groups on selected files or folders. The report also provides information about the custom attributes of the users who have activity on the selected data resources.

Table 7-1 Activity Details reports

Report type	Description
Activity Details report for paths	Use this report to get details of access on one or more files or folders during the selected time window for all configured users and groups. Optionally, you can scope the report to one or more users or groups to get activity information for the selected users on the selected data resources.
Activity Details report for users or groups	Use this report to get detailed accesses by one or more users or by members of one or more groups during the selected time window. Optionally, you can also include one or more users, as an input parameter for this report to display only the activities by the selected users.

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

- Data Insight does not expand built-in groups like Everyone or Authenticated Users. Authenticated Users group is not a true Active Directory group. Users

are added to this group dynamically as they authenticate and log in to a domain. Since this is a dynamic group, Data Insight does not get membership information for this group during an Active Directory scan. Thus, activity information about such users and groups is not captured in these reports even if these groups to users or groups are selected when configuring the reports.

- Data Insight captures the IP address of the source machine (the location from which activity is generated) only in the case of NetApp CIFS and EMC CIFS paths. For rest of the devices such as Windows File Server, SharePoint, NFS paths, the Activity Details report returns the IP address as 0.0.0.0.
- At this time, Data Insight does not relate an Permission change event with a specific user. Thus, when configuring an Activity Details for Paths report, Permission Change events are not reported if you select a specific user or group. To get information about all Permission Change events, you must select **User Selection** > **All Users/Groups** option when configuring the report. If you do not make any selection on the **User Selection** tab, Data Insight creates the report for all users by default.
- Activity details reports are not supported for Documentum paths.

Permissions reports

Note: Data Insight does not fetch permissions data for the SharePoint Online, Microsoft OneDrive, and Documentum data sources. You will not be able to create permissions reports for these data sources.

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

Drill down the summary table to view the detailed report.

Inactive Users

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

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

Note: If a domain, say A, migrates to domain B, then **Inactive Users** report shows inactive user accounts from domain B. The report takes into account the activity of each user from both the domains.

Path Permissions

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

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

This report takes input parameters in the following two ways:

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

Permissions Search report

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

You can create templates to search for the following:

Access Control Entries (ACEs) in an ACL	The ACE that identifies a trustee, specifies the access rights - allowed or denied for that trustee on an object (on a path). The ACE Search report returns individual ACEs that match or violate the rules in the template.

Access Control List (ACL)	The ACL is a list of access control entries for a file or folder. The ACL Search report returns the entire ACL that match or violate the rules in the template, although the rules evaluate the ACEs within the ACL.

See "About Permissions Query templates" on page 93.

See "Creating a report " on page 88.

See "Create Permissions Search report" on page 92.

See "Creating a Permissions Query Template" on page 94.

See "Creating custom rules" on page 99.

Create Permissions Search report

Use this dialog to create an instance of a report.

Table 7-2 Create Permissions Search report options

Option	Description
Report Information	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Description** - A short description of the data that is contained in the report. ■ **Output Format** - Select the format in which you want to generate the report. You can select one or all of the given output formats. ■ **Schedule** - Select the schedule at which you want the report to run. ■ **Maximum Reports to preserve** - Select the number of report outputs you want the system to preserve. The default value to preserve the report outputs is now unlimited.
Configuration	From the **Select Template** drop-down, click **Manage Templates** to create a template. See "Creating a Permissions Query Template" on page 94. See "Creating custom rules" on page 99. **Include custom attributes of user** - Select the check box to include custom attributes in the report output. From the drop-down list, select a configured custom attribute. By default, the check box is cleared. For more information on configuring the custom directory attributes, see the *Veritas Data Insight Administrator's Guide*.

Table 7-2 Create Permissions Search report options *(continued)*

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

About Permissions Query templates

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

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

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

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

- Review access to trustees on shares and folders.

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

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

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

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

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

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

See “Create Permissions Search report” on page 92.

See “Creating a Permissions Query Template” on page 94.

See “Creating custom rules” on page 99.

Creating a Permissions Query Template

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

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

To create a Permissions Query Template

1. On the Management Console, click **Reports** > **Permissions Reports** > **Permissions Search**.
2. On the Create Permissions Search Report page, click the **Configuration** tab.
3. From the **Select Template** drop-down, select **Manage Templates**.
4. On the **Manage Templates** page, do the following:
   - **Name** - Enter a logical name for the template.
   - Before you can select a predefined rule or create a custom rule, you must select whether you want to search for a specific Access Control Entries (ACEs) or Access Control Lists (ACLs) that match or violate the rules that are defined in the template.
     From the drop-down, select **ACE/ACL** that **Match/Do not match Any/All/ Exactly** rules in the template.
     These options dictate how the rules are evaluated when the report is run.
     See "Using the match-type criteria" on page 96.
   - **Rule** - Click the **Add Rule** drop-down to select one or more predefined rules.
     Or click **Add Rule** > **Custom Rule** to create a rule with custom conditions.
     See "Creating custom rules" on page 99.
     The following predefined rules that are available for selection.

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

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

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

See "About sharing a Permissions Query Template" on page 105.

6 Click **Save**.

Using the match-type criteria

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

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

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

Table 7-3 ACE Search match-type criteria

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

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

For example, the template consists of the following rules:

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

Table 7-4 ACL Search Match-type criteria

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

Table 7-4 ACL Search Match-type criteria *(continued)*

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

Creating custom rules

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

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

To create a custom rule

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

   See "Creating a Permissions Query Template" on page 94.
3. Enter a logical name for the template.
4. From the drop-down, select whether you want to create a custom rule to search for ACLs or ACEs.
5. Select the match type criteria for evaluating the rules.

   See "Using the match-type criteria" on page 96.
6. Select **Add Rule** > **Custom Rule**.
7. On the **Custom Rule** panel, you can select options from the high-level categories, **Permissions** and **Trustee**.

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

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

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

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

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

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

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

Permissions

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

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

Table 7-5 describes how these options can be combined to create a search rule.

Table 7-5

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

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

Trustee

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

Table 7-6

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

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

Example custom rules

Table 7-7 describes the various options that you must select to create custom rules for different scenarios.

Table 7-7 Example scenarios and corresponding custom rules

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

Table 7-7 Example scenarios and corresponding custom rules *(continued)*

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

See "Creating a Permissions Query Template" on page 94.

Permissions Query Template actions

The following actions are allowed for a Permissions Query Template:

- Edit a template.
- Delete a template.
  See "Editing or deleting a Permissions Query Template" on page 104.
- Copy a template.
  See "Copying a Permissions Query Template" on page 105.
- Share a template.
  See "About sharing a Permissions Query Template" on page 105.

Editing or deleting a Permissions Query Template

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

To edit an existing template

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

You can also delete an existing template.

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

To delete a template

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

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

Copying a Permissions Query Template

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

To copy a template

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

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

About sharing a Permissions Query Template

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

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

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

Using Permissions Search report output to remediate permissions

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

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

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

To remove permissions

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

   See "Creating a Permissions Query Template" on page 94.

2. Create a Permission Search report by selecting a template.

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

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

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

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

Entitlement Review

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

The Entitlement Review report provides the following information:

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

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

User/Group Permissions

The User/Group Permissions report displays the permissions assigned to selected users or groups on the selected paths. It also takes into account migration information and SID history while computing permissions.

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

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

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

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

Note: The Group Change Impact Analysis report also takes into account all the permissions based on SID history. It takes into account all the activity performed from the current and all previous domains.

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

Ownership Reports

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

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

Data Custodian Summary

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

- The name of the custodian.
- The account name of the custodian, for example, user@domainname.com.
- The data source, for example a 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:

- Activity 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. Veritas does not recommend using browser-based plug-ins or extensions to open the large database files that are generated by the Data Inventory report.

Create/Edit security report options

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

Table 7-8 Create/Edit security report options

Option	Description
Report Information	

Table 7-8 Create/Edit security report options *(continued)*

Option	Description
	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Label** - Add a label(s) to help you categorize and easily find the report from a long list of reports. For example, Finance or Media Files. See "Organizing reports using labels" on page 167. ■ **Description** - A short description of the data contained in the report. ■ **Report type** - The type of security report. This field is populated by default. ■ **Select resources using** - Select **Paths** or **Custodian Information** radio button. Depending on the selection, you can see the data selection or custodian selection option. **Note:** This field is available only in the following five reports : ■ Activity summary report for paths ■ Data aging report ■ Inactive folders report ■ Path permissions report ■ Consumption by folders report ■ **Output format** - Select the format in which you want to generate the report. You can select one or all of the given output formats. ■ **Maximum reports to preserve** - Select the number of report outputs you want the system to preserve. If both, global value and local value is not configured, then the value is considered as ***unlimited***. In case of scheduled reports, setting up value of this parameter to **Unlimited** may fill up disk space. Configure the value appropriately by taking disk space into consideration. **Note:** You can configure a global setting to purge report outputs when they exceed a certain number. However, the value configured in the **Maximum reports to preserve** field takes precedence over the global setting. For information about data retention settings, see the *Veritas Data Insight Administrator's Guide*. ■ **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.

Table 7-8 Create/Edit security report options *(continued)*

Option	Description
	Note: When you specify a path in this field, select a folder that already exists. Data Insight does not create a new folder. Copying a report may fail if the folder is in use by any application, including Windows Explorer. To test a connection, check the number of connections allowed on the folder. If you have just created a folder and the folder is open in Windows explorer, the test connection will fail for default settings since the default number of connections allowed on a folder is one. ■ **Select Credentials to access "Copy output to" path** - Select a credential from the drop-down menu, so that Data Insight can direct the report output to the specified location. Aditionally you can use the option for adding a new set of credentials if the required credentials are not already added. The credentials must have folder-level read, write, create and delete permissions on the external computer where the report output is copied. ■ **Overwrite option** - Selecting this option overwrites the earlier report output files. If you clear this check box, Data Insight creates a new folder with a report run ID for every report run, and saves the report in the new folder.

Table 7-8 Create/Edit security report options *(continued)*

Option	Description
Configuration	

Table 7-8 Create/Edit security report options *(continued)*

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

Table 7-8 Create/Edit security report options *(continued)*

Option	Description
	to a new domain, with the corresponding new account. ■ **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. **Note:** This option is available only for Entitlement Review report. ■ **Select columns to hide in output** - Select the columns that you do not want to display in the report. ■ **Truncate output if record exceeds**- Enter the number of records(rows) after which the report output is truncated. See "Configuring a report to generate a truncated output" on page 163. ■ **Department mapping** - You can map the department through the options available in the drop-down list . The generated report maps the department on the basis of the option you choose. ■ **Filter**- This option is available only for the Data Inventory Reports. Use the filter to specify the following : ■ **Time filter**- From the drop down, select an option to consider all the files that are last accessed or modified before a given time. ■ **File Group**- Select this option to specify the file groups, to be considered for generating the report output. ■ **File Type**-Select this option to specify file types to be considered for generating the report output. Specify the extensions of the file types to be considered in a comma separated list. ■ **DLP Policy**-Select a DLP policy to be considered for generating the report output.

Table 7-8 Create/Edit security report options *(continued)*

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

Table 7-8 Create/Edit security report options *(continued)*

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

Table 7-8 Create/Edit security report options *(continued)*

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

Table 7-8 Create/Edit security report options *(continued)*

Option	Description
Remediation	Use this tab to instruct Data Insight to execute predefined actions on a report output. Select **Take action on data generated by report** to enable automatic processing of data generated by a report. Select any of the following: ■ **Archiving (Enterprise Vault)** - Select this option to archive data using Enterprise Vault. If you select this option you must specify a retention category and a post-processing action. You can add classification tags while archiving files into Enterprise Vault to enable faster search from Enterprise Vault. Select the **Add Custom Index Property** check box. You can select a **Property type** from the drop-down box like Text, Integer, or Date. Depending on what you select, text boxes corresponding to Set, Name and Value appear. You must specify the name of the property set, the name of the property and the value of the property which will constitute the classification tag that will be pushed while archiving files into Enterprise Vault. See "Pushing classification tags while archiving files into Enterprise Vault" on page 227. ■ **Custom Action 1** / **Custom Action 2** - Select this option to specify a custom action defined by a custom script. See "About managing data using Enterprise Vault and custom scripts " on page 219.

Some limitations exist when creating certain Permissions reports for Box resources. See "Data Insight limitations for Box permissions " on page 119.

Data Insight limitations for Box permissions

The following limitations exist in the current Data Insight implementation of Box permissions.

- Data Insight primarily displays a user's access level, and whether the access level is assigned directly or through a Box group. However for folders on which users are collaborating, Data Insight does not display any information on how the sharing occurred (by using a shared link or by invitations), and also does not give any detail on whether link is publicly available, and whether it has any expiry date.
- In the Entitlement Review report, the following is not supported:

  - Selection of users on the **User Selection** tab. This is applicable for CIFS paths also.
  - It does not show correct permissions if a user has two different permissions on the same folder. As per Box, this is not valid scenario.
- Earlier Box allowed two different permission levels to be assigned on a folder to the same user or group. However, now Box has disabled this functionality. Thus, on a given path, if user or group has two permission levels where permissions are same or different then Data Insight does not support reporting of permissions on such paths.
- The following limitations exist in the Entitlement review report:
  - Use the **Access Control List** option to fetch Box permission information. Selection of **Effective Permissions** option returns the same results as Access Control List. Also,
  - If you select user account as a path and configure Full Depth when creating the report, then the report returns permissions for only folders owned by that user account.
  - The options **Only share level permissions**, **Include Share Level ACLs for effective permission computation** and **Show advanced permissions** are not applicable for Box permissions.
- The option **Show advanced permissions** is not applicable when configuring User Group Permissions report.
- When creating a report, if you select **Current folder** as depth, the output will be blank for the All files and user name folder and for share-level selection.
- Data Insight does not support creation of Records Classification workflows for Box paths.
- You cannot upload the following Box paths using a CSV file when creating Data Insight reports:
  - Box paths where users are collaborating.
  - Box paths that contains special characters.

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:

- Activity Summary Reports
  See “Activity Summary reports” on page 121.
- Capacity Reports
  See “Capacity reports” on page 122.
- Data Lifecycle Reports
  See “Data Lifecycle reports ” on page 124.
- Consumption Reports
  See “Consumption Reports” on page 126.

Activity Summary reports

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

- Activity 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 activities.

- Activity summary report for paths

  Use this report to get total number of activities 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 activities on selected paths to those users.

  This report takes input parameters in the following two ways:

  - Path driven reports - give activity 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.

Note: You will not be able to create activity reports for the Documentum data source.

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. and to identify where storage can be used more efficiently.

Note: Capacity reports do not support SharePoint, VxFS, Hitachi NAS (HNAS), Box, EMC Isilon, EMC Unity, VNX, and EMC Celerra file servers.

Table 7-9

Report type	Description
Filer Utilization	The Filer Utilization report displays a summary of the space used and the free space available on configured Network Attached Storage systems. Use this report to get storage utilization on filers.

Table 7-9 *(continued)*

Report type	Description
Filer Growth Trend	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. Use this report to get the trend of space utilization on filers during the selected time period. The report provides 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.

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, Hitachi NAS (HNAS), Box, EMC Isilon, EMC Unity, VNX, 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, Hitachi NAS (HNAS), Box, EMC Isilon, EMC Unity, VNX, 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 *Veritas Data Insight Administrator's Guide*.

Inactive Data by Owner

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

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

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

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

Data Aging

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

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

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

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

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

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

This report takes input parameters in the following two ways:

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

Inactive Folders

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

This report takes input parameters in the following two ways:

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

Consumption Reports

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

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

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

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

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

- Data Insight computes the number of records as the top N files based on the file size for every data owner or for every device path in the report input.
  For example, during report configuration the input path is one share, \\<Filer 1>\<Share 1> and the Number of records = 5.
  In this case the report computes the owner of each file on the share, and lists the top 5 files based on size for every data owner.
  Let us say Share 1 has total 30 files, such that 10 files are owned by UserA, 10 by UserB and 10 by UserC. In this case, the report displays 15 files. (The top 5 files based on size owned by UserA, UserB, and UserC.
  For example, during report configuration the input path, \\<Filer 1>\<Share 1>, \\<Filer 1>\<Share 2>, and the Number of records = 10.
  Let us say Share 1 has total 20 files, such that 10 files are owned by UserA and 10 by UserB.
  Share 2 has total 20 files, 10 files owned by UserA and 10 files by UserC. In this case, the report displays the following output:. (The top 5 files based on size owned by UserA, UserB, and UserC for every share.
  - UserA: Top 10 files (files from Share 1+ files from Share 2 based on size)
  - UserB: Top 10 files (from Share 1)
  - UserC: Top 10 files (from Share 2)
- The report does not return deleted files and files with size 0KB in the output.
- For SharePoint file path, size on disk is not applicable; report will always return size on disk as zero.

Potential Duplicate Files

Potential Duplicate Files report helps you to identify the duplicate files within a given share. It enables you to take informed decisions about reclaiming storage. Note

that duplicate file detection is per share only. Data Insight does not detect duplicate files across shares.

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

This report provides a graphical summary of the following:

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

Consumption by Folders

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

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

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

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

This report takes input parameters in the following two ways:

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

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

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

Consumption by Department

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

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

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

Consumption by File Group

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

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

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

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

Create/Edit storage report options

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

Table 7-10 Create/Edit storage report options

Option	Description
Report Information	

Table 7-10 Create/Edit storage report options *(continued)*

Option	Description
	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Label** - Add a label(s) to help you categorize and easily find the report from a long list of reports. For example, Finance or Media Files. See "Organizing reports using labels" on page 167. ■ **Description** -A short description of the data contained in the report. ■ **Report type** - The type of security report. This field is populated by default. ■ **Select resources using** - Select **Paths** or **Custodian Information** radio button. Depending on the selection, you can see the data selection or custodian selection option. **Note:** This field is available only in the following five reports : ■ Activity summary report for paths ■ Data aging report ■ Inactive folders report ■ Path permissions report ■ Consumption by folders report ■ **Output format** - Select the format in which you want to generate the report. You can select one or all of the given output formats. ■ **Maximum reports to preserve** - Select the number of report outputs you want the system to preserve. If both, global value and local value is not configured, then the value is considered as ***unlimited***. In case of scheduled reports, setting up value of this parameter to **Unlimited** may fill up disk space. Configure the value appropriately by taking disk space into consideration. **Note:** You can configure a global setting to purge report outputs when they exceed a certain number. However, the value configured in the **Maximum reports to preserve** field takes precedence over the global setting. For information about data retention settings, see the *Veritas Data Insight Administrator's Guide*. ■ **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. **Note:** When you specify a path in this field, select a folder that already

Table 7-10 Create/Edit storage report options *(continued)*

Option	Description
	exists. Data Insight does not create a new folder. Copying a report may fail if the folder is in use by any application, including Windows Explorer. To test a connection, check the number of connections allowed on the folder. If you have just created a folder and the folder is open in Windows explorer, the test connection will fail for default settings since the default number of connections allowed on a folder is one. ■ **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 7-10 Create/Edit storage report options *(continued)*

Option	Description
Configuration	

Table 7-10 Create/Edit storage report options *(continued)*

Option	Description
	Select the conditions to configure the report: ■ **Inactivity Period** - From the drop-down, select the duration of inactivity for files. Only the files that have remained inactive for the selected duration are included in the report. This field is only available for the Inactive users report. ■ **Bucket Size (Months)** - Enter the bucket interval that you want to include in the report. ■ **Include custom attributes of user** - By default, the check box is cleared. Select the check box to select the custom attributes from the drop-down list. For more information on configuring the custom directory attributes, see the *Veritas Data Insight Administrator's Guide*. ■ **Include data owner in report output** - Select the order of the criteria for computing the owner of the data. This field is available only for select report types. ■ **Activity Time Period** - Enter the time range for which you want data to be included in the report. Select **Duration** to indicate the last n hours/days/weeks/months/year. Select **Date Range** to specify a specific time range. ■ **Folder depth** - This option is available only for the Consumption by Folders report. Select the subfolder levels to be included in the report. This option is useful when you want to limit the total output in the report. ■ Select **Current Folder**, to include the information about only the selected paths. ■ Select **Next level sub directories** radio button to include information about the first-level children of the selected paths. ■ **Folder depth for selection of paths to report against** - Select the depth of subfolders to be included in the report from the drop-down list. This option is useful when you want to limit the total output in the report. From the drop-down, ■ Select **Current folder** to include information about only the selected paths. ■ Select **Specify Depth** and enter the level at which you want to include the folders. This filed is available only for the following reports: ■ Activity Summary for Paths ■ Activity Summary for Users/Groups ■ Enter the **Number of records** you want to include in the report output.

Table 7-10 Create/Edit storage report options *(continued)*

Option	Description
	The report computes the number of records as the top N files based on the file size for every data owner, for every device path in the report input. From the top N files, (for example, in case of Inactive Folders report) the report will display the top N files that have remained inactive for the configured duration. The default is 25 records. In case of Consumption by folders report, this option appears only if you enable the check box **Show details in reports**. ■ **Department mapping** - You can map the department through the options available in the drop-down list . The generated report maps the department on the basis of the option you choose. ■ **File type** - Enter comma-separated file type in this field. You can enter the file type in this field for the file group that is not pre-configured for the type of file you want to include in the report output. This option is available for the following reports: ■ Consumption by File Group ■ Consumption by File Group and Owner ■ Inactive Data by File Group ■ **File groups** - Select a file group from the drop-down list. This option is available for the following reports: ■ Consumption by File Group ■ Consumption by File Group and Owner ■ Inactive Data by File Group **Note:** You can select either a file type or a file group in the report output. ■ **Select columns to hide in output** - Select the columns that you do not want to display in the report. ■ **Truncate output if record exceeds**- Enter the number of records (rows) after which the report output is truncated. By default, the value you specify in this field applies to all the report types for whichData Insight supports truncation. See "Configuring a report to generate a truncated output" on page 163.

Table 7-10 Create/Edit storage report options *(continued)*

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

Table 7-10 Create/Edit storage report options *(continued)*

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

Table 7-10 Create/Edit storage report options *(continued)*

Option	Description
Remediation	Use this tab to instruct Data Insight to execute predefined actions on a report output. Select **Take action on data generated by report** to enable automatic processing of data generated by a report. Select any of the following: ■ **Archiving (Enterprise Vault)** - Select this option to archive data using Enterprise Vault. If you select this option you must specify a retention category and a post-processing action. You can add classification tags while archiving files into Enterprise Vault to enable faster search from Enterprise Vault. Select the **Add Custom Index Property** check box. You can select a **Property type** from the drop-down box like Text, Integer or Date. Depending on what you select, text boxes corresponding to Set, Name and Value appear. You must specify the name of the property set, the name of the property and the value of the property which will constitute the classification tag that will be pushed while archiving files into Enterprise Vault. See "Pushing classification tags while archiving files into Enterprise Vault" on page 227. ■ **Custom Action 1** / **Custom Action 2** - Select this option to specify a custom action defined by a custom script. See "About managing data using Enterprise Vault and custom scripts " on page 219.

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 *Veritas Data Insight SDK Programmer's Guide*.

Detecting ransomware attack using query templates

Data is constantly vulnerable to unknown threats from malware variants such as ransomware, that continue to evolve. Protecting your data against these variants

requires you to promptly detect the malicious attack and effectively perform a remediation course.

Veritas Data Insight periodically collects audits of the read, write, and rename activities performed on the files in the monitored storage environment. With the ransomware reports, you can capture the count of write and rename activities performed on the files by each user. If the count is higher than the specified threshold value, then the files on which the activities occurred could be exploited. The threshold value is the count of write and rename activities that you permit per user on files present in a data source. For example, when ransomware inflicts a file, it encrypts and renames the file to include a unique extension. When the Write Rename sensor query is executed on a data source, it fetches the count of write and rename activities performed by users on files within 24 hours. If it detects any user who performed more than 100 write and rename activities, the files on which the activities happened are termed as potentially exploited, and the users who are configured on the **Notifications** page are alerted.

By default, the threshold value is set to 100. This indicates that whenever any user performs 100 rename or write activities within 24 hours, the files accessed by that user could be infested.

The threshold value can be set by running the following command on the Management Server.

```
configdb -O -J ransomware.path.count -j <value>
```

For example,

```
configdb -O -J ransomware.path.count -j 72
```

Note that if the threshold value is low, then the reports might capture the authentic write and rename activities that happen as part of the routine tasks. Thus, it is recommended to consider these tasks when configuring the threshold value.

You must configure the ransomware report schedule to run once every 4 hours such that it runs along with the indexer schedule. This ensures that the ransomware query gets sufficient event logs for processing.

See “About DQL query templates” on page 141. for more information about different types of ransomware reports.

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 149.

See “Creating a report ” on page 88.

Data Insight provides the following default query templates:

Table 7-11 Data Insight Query Language templates

Category	Name	Description
Data Management	Folder creation details	The query fetches the details about the creator and the date of creation for every first-level folder in the environment.
Data Management	All files with a specific extension	The query fetches details of files with specific extensions in your storage environment. You can use this query to find, for example, all media files. The query helps you find data that does not comply with your organization's policy, and reclaim storage on your device. Modify the template to add other extensions to get results that suit your needs.
Data Management	Capacity by extensions	The query and the provided advanced SQL queries help in identifying the storage capacity used by specific file extensions.
Data Management	Files in a confidential folder	The query lists all the files under a specified folder in a share. In this example, the folder has the word "confidential" as part of its name. Modify share name and folder name search criterion to get results that suit your needs.
Data Management	Files with undefined file groups	The query lists all the file extensions 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. Use the advanced query to narrow down the results to specific extensions.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
Data Management	Folder summary by file type	The query fetches the folder level summary of counts and size used by different file-types in a share. Only the files which are direct member of a folder will be used for computation. Only those file-types that are part of Data Insight file groups will be listed. For all other file types, it will be combined under empty "" file type. Modify the share name to get results that suit your needs.
Data Management	Stale file list	The query lists the files that have not been accessed for the past one year. You can use this report to make better archiving decisions. Modify the duration and the share name to get the results that suit your needs.
Data Management	Storage usage by user attribute	The query lists the consumption of storage on NAS devices based on the user attribute, department. The consumption is determined by calculating the owner of the file and mapping the owner to the corresponding department. Modify the filer name and user attribute to get the results that suit your needs. Additionally, you can modify the owner calculation by specifying access dates and order of the policy for computing the data owner.
Data Management	Duplicate Files in Share	This query along with the advanced SQL queries help in identifying duplicate files within a share by name, by size of files, and by modified time. Additionally, you can specify conditions to match copy string in file name to further tune the advanced SQL. These options are part of commented portion in Advanced SQL query in template.
Data Management	Stub Files	This query lists all stub files assuming that stub size equals 4 kb.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
Data Management	Archived Files	The query lists all such archived files with the specified attributes. The attribute metadata is stored by the file system and can be used to find out the amount of reclaimable storage and take decisions about removal or archiving.
Risk Analysis	Sensitive files on a filer	The query lists all files which are marked sensitive by the Symantec Data Loss Prevention (DLP). These files can be further analyzed and acted upon as per organization's security measures. If DLP is configured and incidents are reported against a configured report ID, this report lists the sensitive files automatically. Alternatively, you can import sensitive file information to Data Insight using a CSV file. Modify the device name with valid filer name in your environment to get the results that suit your needs.
Risk Analysis	Sensitive files that are active	The query lists all the active sensitive files that violate a certain DLP Policy. In addition to file details, it also provides you the information on the number of active users on the files. Modify the activity period and policy to get the output that is valid for your environment.
Risk Analysis	Sensitive files with violated policies	The query lists all the sensitive files in a share and the associated DLP policy that are violated. Modify the share name to get the output that is valid for your environment.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
Risk Analysis	Department-wise summary of risky behavior	The query fetches the summary of the users belonging to other departments who have assessed sensitive files owned by a specific department. For example, you may want to know the users belonging to any non-HR department accessing files owned by the HR department. This query computes the potentially risky behavior on a specific share during a specific time range. The files are classified as being sensitive by DLP policies. Note that sometimes the report may flag legitimate accesses as risky behavior. Use your discretion to eliminate such false alarms. Modify the share name, time range, DLP policy string, user department attribute, and department name in the query to get valid results in your environment.
Risk Analysis	Recent suspicious activity	This query fetches the details of the inactive sensitive files that were accessed recently. For example, it can get the list of sensitive files that were inactive for last year but were accessed in last 5 days. It also provides you information about the person who accessed the file most recently. The sensitive file information is fetched from DLP. Alternatively, you can import sensitive file information to Data Insight using a CSV file. Modify the recent access time range and inactivity time range in your environment to get results that suit your needs.
Risk Analysis	Last Accessed - Time Range	The query lists all files that are accessed between 1 year and 3 years.
Risk Analysis	Groups contributing to high risk	The query finds out common groups across users who have risk score > 90 and who are contributing to the high level of permissions. Use the query to analyse whether the users should be part of the group or the excessive permissions to the group should be reconsidered.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
Risk Analysis	Risky Users Outlier	The query gives the count of high-risk users based on their custom attributes. The users are listed in the ascending order of their risk score. Use the query to find any unusual user with a risk score > 90. Typically, the high-risk users may include service or administrator accounts due to the high level of permissions assigned to these accounts.
Forensics	Share access details	This query provides the audit details on a share for a specified time range. Modify the time range and share name to get results specific to your environment.
Forensics	User access details	The query provides the details of accesses by a specified person on a share during a specified time range. Modify the person name, time range, and share name to get the results to suit your needs.
Forensics	Top users of sensitive files	The query lists top ten users who have accessed sensitive files in your storage environment within a specified time-range. Modify the time range to get valid result in your environment.
Forensics	Folders with maximum access counts	The query fetches the list of top ten folders that are accessed in a share during a specific time range. Modify the share name and time-range to get valid result in your environment.
Forensics	Users with maximum access counts	The query fetches the list of top ten users who have accessed a share during a specific time range. Modify the share name and time-range to get valid result in your environment.
User / Group Management	Group membership details	The query provides the details about a specified security group, its member groups, and users in the group. Modify the group name and domain name to get the results that are valid for your environment.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
User / Group Management	Deleted or disabled groups	The query lists all the disabled or deleted security groups in the environment.
User / Group Management	Deleted or disabled users	The query lists all the disabled or deleted users in the environment.
User / Group Management	Groups with disabled users	The query lists all the groups with disabled users in the environment.
User / Group Management	Empty groups	The query provides a comma-separated list of security groups, their details and SIDs of its member users. To list the empty groups for clean-up, execute following query on the output: `SELECT * FROM groups WHERE memberusers_sid = ''`
User / Group Management	Circular groups	The query lists any security groups in the environment which are members of each other forming group loopings.
Data Protection	Open shares	The query lists all paths in your environment that have excessive permissions along with the reasons for their openess.
Data Protection	Shares with permissions to Everyone group	The query lists shares in the environment that have permissions to the "Everyone" group.
Permission Management	Paths with direct permissions to disabled users	The query provides the details about the paths that have explicit access to disabled users.
Permission Management	Box folders owned by a given user	The query lists all box folders owned by a given user. It excludes all shared folders.
Classification	Files to send for classification	Creates a report of all files that are accessible to more than 1000 users. Use the DQL report to send file paths in the output for classification.
Classification	Classified files with a specific extension	Creates a report of all files with a specific extension (for example, PST) and a specific tag name (for example, US-PII). You can either use the query to identify tags associated with specific files or to push these files to Enterprise Vault for archiving.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
Classification	All PII files	Creates a report of all files that are tagged as Personally Identifiable Information (PII). These are files that may contain sensitive information such as Social Security, credit card, and drivers' license numbers.
Classification	Classify active users files	Creates a report listing all files that have been accessed by users identified as active by Data Insight. You can then use this report to submit these files for classification.
Classification	Classified files summary	Creates a report that summarizes all files that have already been classified.
Ransomware	WriteRename sensor	The query lists all the write and rename activities performed in the data source within 24 hours. An SQL query is used to fetch the per user activity (write) count performed on the file before it was renamed. If the activity count is higher than the configured threshold, only then a notification is sent to the users configured on **Reports** > **Edit** > **Notifications**. See "About Data Insight custom reports" on page 140. for information about how to configure the threshold value. **Note:** Do not modify the query or table names in the query as it might interfere with the notification process.
Ransomware	Activity by rename extensions	The query fetches the count of files that are renamed by per user, and have unique file extensions. For example, the query extracts the number of files that are renamed, and which have the extension as docx, pdf, xlsx.
Ransomware	Rename count for parent folders	The query fetches the top-level directories in the share, site collection, or equivalent, and the number of write and rename activities performed in each of these repositories by per user. Use this report to detect malicious activities performed on the parent folder in a share or equivalent.

Table 7-11 Data Insight Query Language templates *(continued)*

Category	Name	Description
Ransomware	Activity by create extensions	The query lists all the files that are created in the last 24 hours by per user. Use this query to identify files created by an infected or risky user.
Ransomware	List file patterns	This query lists the files that contain a specific string in the file name. For example, ransomware appends a unique extension to the encrypted files. With this query, you can fetch all the files that contain the specified extension.
Ransomware	Trace malicious executable	The query lists the duplicates of the ransomware executables residing on your system.

Creating custom templates for DQL queries

To create custom templates for DQL queries

1. Create a text file with the following information on separate lines:

   name: <The name of the query template>

   desc: {<The description of the query template>}

   version: <The Data Insight version for which the query template is valid>

   category: <The category to which the query belongs. For example: Data Management, Forensics etc.>

   query:{<The DQL query text>}

   Note: The desc, the version and the category information are optional. The curly braces in the desc line can be omitted in case of single line descriptions.

2. Give the file a suitable name and save it with a `.template` extension at the following location on the Management Server:

   `<DATADIR>/templates/dql`

Create/Edit DQL report options

Use this dialog to create an instance of a DQL report.

Table 7-12 Create/Edit DQL report options

Option	Description
Report Information	Enter information in the following fields: ■ **Name** - A logical name for the report. ■ **Label** - Add a label(s) to help you categorize and easily find the report from a long list of reports. For example, Finance or Media Files. See "Organizing reports using labels" on page 167. ■ **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. If both, global value and local value is not configured, then the value is considered as ***unlimited***. **Note:** You can configure a global setting to purge report outputs when they exceed a certain number. However, the value configured in the **Maximum reports to preserve** field takes precedence over the global setting. ■ **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. **Note:** When you specify a path in this field, select a folder that already exists. Data Insight does not create a new folder. Copying a report may fail if the folder is in use by any application, including Windows Explorer. To test a connection, check the number of connections allowed on the folder. If you have just created a folder and the folder is open in Windows explorer, the test connection fails for default settings since the default number of connections allowed on a folder is one. ■ **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 7-12 Create/Edit DQL report options *(continued)*

Option	Description
Query	Write your DQL query in the space provided. You can provide multiple DQL queries separated by a space or a newline. This creates a DQL output with multiple tables for corresponding to each DQL queries. While writing the query you must adhere to the syntax and guidelines of the Data Insight Query Language (DQL). For more information about creating DQL queries, see the *Veritas Data Insight Programmer's Reference Guide*. Click **Use Template** to use the queries provided by Data Insight as templates. Click tthe drop-down to select a category and a template. Once you have selected a template, you can edit it as per your needs. See "About DQL query templates" on page 141. You can use a CSV file to feed a bulk input to a query. Click **Choose file** to browse to the CSV file containing the bulk input and click **Upload** the file. For details on how to use the content of CSV file as arguments in a query, refer to the *Veritas Data Insight Programmer's Reference Guide*.

Table 7-12 Create/Edit DQL report options *(continued)*

Option	Description

	Optionally, click **Advanced Options** > **Run SQL commands on generated DQL output database**. This displays a text area where you can type the SQL commands that enable you to access and manipulate the DQL output database. The feature enables you to do the following:
	
	Click **View DQL output database schema** to view the schema of the tables which get generated by DQL.
	
	Click **Check DQL syntax** to view syntax errors for your DQL query.
	
	Following is an example of a query to get a report that provides the distribution of files and storage per extension in a share. Replace <*Share Name*> with the name of the share in your environment.
	
	DQL Query
	
	`from path`
	
	`get extension, count(extension), sum(size)`
	
	`where path.msu.name = "<Share Name>"`
	
	`and type = "file"`
	
	`and isdeleted = 0`
	
	`group by extension`
	
	Advanced Options
	
	`create table Cap_EXT(path_rowid INTEGER,`
	`extension TEXT, no_files INTEGER, size_MB INTEGER);`
	
	`insert into Cap_EXT`
	
	`select path_rowid,`
	`COALESCE(NULLIF(extension,''),`
	`'Unclassified File Group')`
	`, "count(extension)",`
	
	`round("sum(size)"/1024.0/1024.0, 2) from path`
	
	`order by "sum(size)" desc;`
	
	Following is an example of a query to get a report that provides the classification results for all files that are tagged as containing Personally Identifiable Information (PII).
	
	DQL Query

Table 7-12 Create/Edit DQL report options *(continued)*

Option	Description
	For more examples, refer to the *Veritas Data Insight Programmer's Reference Guide.*
Notification	Enter email addresses of users you want to send the report to. If the size of the attachment is above the configured limit, an email is sent without the attachment. You can configure the size of the attachment under **Settings** > **SMTP Settings.**
Remediation	Use this tab to instruct Data Insight to execute predefined actions on a report output. Select **Take action on data generated by report** to enable automatic processing of data generated by a report. Select any of the following: ■ **Archiving (Enterprise Vault)** - Select this option to archive data using Enterprise Vault. If you select this option you must specify a retention category and a post-processing action. You can add classification tags while archiving files into Enterprise Vault to enable faster search from Enterprise Vault. Select the **Add Custom Index Property** check box. You can select a **Property type** from the drop-down box like Text, Integer, Date or Classification property. Depending on what you select, text boxes corresponding to Set, Name and Value appear. In case of Classification property, the Value field does not appear because the classification tag is considered as the value for Classification property. You must specify the name of the property set, the name of the property and the value of the property which constitute the classification tag that are pushed while archiving files into Enterprise Vault. See "Pushing classification tags while archiving files into Enterprise Vault" on page 227. ■ **Custom Action 1** / **Custom Action 2** - Select this option to specify a custom action defined by a custom script. ■ **Classify**- Select to submit the output file paths in the report for classification. For information about setting up classification and initiating classification requests, see the *Veritas Data Insight Classification Guide*. See "About managing data using Enterprise Vault and custom scripts " on page 219.

Considerations for importing paths using a CSV file

The following considerations apply when you import paths for a report using a CSV file:

- When using a CSV file to upload paths, specify the path name with a comma followed by the input type in the file. The input type enables Data Insight to classify the paths.
  For example, `http://sharepoint1/sites/Marketing, SiteCollection`.
  Veritas Data Insight supports the following input types:
  - Filer
  - DFSFiler
  - WebApp
  - DFSPathPartial
  - Share
  - DFSPathLink
  - SiteCollection
  - Folder
  - Site
  - File

  For more information, see https://www.veritas.com/support/en_US/article.000107668.
- Ensure that the paths in the CSV do not have double quotes (for example,`\\filer1\share1\foo\bar"kkk.txt`) as they will not be uploaded for the report configuration.

Chapter 8

Managing reports

This chapter includes the following topics:

- About managing Data Insight reports
- Viewing reports
- Filtering a report
- Editing a report
- About sharing reports
- Copying a report
- Running a report
- Viewing the progress of a report
- Customizing a report output
- Configuring a report to generate a truncated output
- Sending a report by email
- Automatically archiving reports
- Canceling a report run
- Deleting a report
- Considerations for viewing reports
- Organizing reports using labels

About managing Data Insight reports

From the **Reports** Home page or the list page, you can perform the following tasks:

- View the summary of all the reports.
  See “Viewing reports” on page 156.
- Run a report.
  See “Running a report” on page 160.
- Filter a report.
  See “Filtering a report” on page 158.
- View the details of a report that is run.
- Edit a report.
  See “Editing a report ” on page 159.
- Copy a report.
  See “Copying a report” on page 160.
- Delete a report.
  See “Deleting a report” on page 166.
- Cancel a report.
  See “Canceling a report run” on page 166.
- Send a report by email.
  See “Sending a report by email” on page 164.
- View the progress of the report run.
  See “Viewing the progress of a report” on page 161.
- Take various remediation actions on the report output.
  See “Managing inactive data by using a report” on page 224.
  For information on using DQL reports to classify files, see the *Veritas Data Insight Classification Guide*.

Viewing reports

On the Reports listing page, you can view the following details:

- The name of the report.
- The label(s) associated with the report. Use the labels to organize the reports and easily find reports from a long list of existing reports.
- 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.

Note: The **Reports** tab is visible only to those users who have the View privilege on.

Click the down arrow on the column header to show the hidden columns.

You can also manage the generated reports from the Reports Home page or the list page.

Viewing report details

On the `Report Details` page, you can view the input parameters that are given to run a report and the report run history. You can also download a report output from this page.

To view the Data Insight report details

1. From the **Select Action** drop-down, click **View** to view details of a particular report.
2. On the **Report Details** page, review the following information:
   - A summary of the input parameters used to configure the report.
   - The report run ID.
   - The date and time for every instance of the report run.
   - The status of the report at the time of the last run.
   - The last successful output formats of the report.
   - The size of the report.
   - The date and time the report was modified.
   - The user account that modified the report

The **Select Action** drop-down on the **Report Details** panel, provides options to email or delete the report and undertake various remediation actions on the report output.

See “About managing Data Insight reports” on page 156.

See “About stale information in reports” on page 158.

See “Considerations for viewing reports” on page 167.

About stale information in reports

When a report is run, Data Insight indicates in the report output those paths for which the audit or metadata information is likely to be stale. Data Insight tracks the time of the last metadata scan/audit that was processed by the Indexer. If the last metadata scan for a path processed by the Indexer is older than 7 days, or the last audit processed is older than 5 days, the report output warns the user about the potentially stale information in the output.

If metadata has not been recently updated, it could mean that the information about paths (lsuch as size, permissions) in the report output might not be up-to-date or missing all- together. Similarly, if audit events have not been processed for some time, it could mean that the audit details in the report output or the ownership calculations that depend on audit activity of users may not be accurate.

You can disable stale information warnings if required by setting the following global property:

`matrix.reports.stale.index.warning.enabled` *`Value: true/false`*

Similarly, you can configure the allowable limit of stale data in the report output by setting the following global property:

`matrix.reports.stale.index.warning.days.scan` *`Value: Grace period in days`*

To set the global property

- Issue the following command on the Management Server:

  ```
  configdb.exe -O -J <name> -j <value>
  ```

  For example:

  ```
  configdb.exe -O -J matrix.reports.stale.index.warning.enabled -j
  false
  ```

Filtering a report

When you click on the **Reports** tab, the home page displays by default.

The Reports home page lists all the available reports for the logged in user. You can perform all reports-related tasks from the home page except creating new reports.

Use the filter on the Reports home page or list page to search for reports on the basis of report name, report label, or report run status. To filter a report on the basis of report status, you must specify the entire report status string for example, success, failure, partial success, or cancelled.

Editing a report

After you create an instance of a report, you can edit the input parameters for generating a report. For example, you might want to edit the users or paths that are selected for the report. Or you might want to change the schedule to run the report.

To edit a report

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Select the report you want to edit, and in the **Select Action** drop-down, click **Edit**.
3. On the Edit report screen, make the necessary changes.
4. Click **Save**.

About sharing reports

You can choose to share reports that you create with other Data Insight users. This functionality enables you to allow users to run reports that are already created by the Report Administrator and other users, and reduces the overhead of having to create the same reports.

Following conditions apply to reports that are shared among Data Insight users:

- You cannot share ownership reports with users other than Report administrators and Server administrators.
- Users who have access to the **Reports** tab can view a shared report.
- Users with any Data Insight role can configure sharing of their reports. Other users can only view and run the shared reports. When you select **Select Action** > **View** for a report that has been shared by another user, you can only see report runs initiated by you and not the report runs by other users. Report runs by all users are visible in the popup only for a user with Server Administrator role or Report Administrator role.
- You can only run the reports created and shared by other users. Data Insight does not allow you to edit or delete reports shared by other users.
- You can copy a shared report created by any other user.
- When you run a shared report, that is created for all configured resources, the report is generated only for the resources (filers/cloud data sources) that you have permissions on.

- If you run a shared report that is created for resources on which you do not have permissions, the instance of the report run will fail.
- Users other than Report and Server administrators cannot run custodian-based reports.

See “Creating a report ” on page 88.

See “Considerations for viewing reports” on page 167.

Copying a report

You can make a copy of a report from a report that is already created.

To copy a report

1. Click the **Reports** tab of the Data Insight Management Console. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Select the report you want to copy, and in the **Select Action** drop-down, click **Copy**.
3. In the dialog box enter a name for the copy of the report.
4. Click **Copy**.

Running a report

On the Reports home page, select the report that you want to run. Every report is generated at the schedule that you specify at the time of creating the report. However, you can also generate a report without waiting for the scheduled run.

To run a report

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Do one of the following:
   - Click the check box next to the report to select multiple reports, and click **Run**.
   - Or, select the report that you want to generate. In the **Select Action** drop-down, click **Run**.
3. You can view the progress of the report run on the Reports listing page.

By default, you can run two reports at a time. You can configure this value to execute more than two reports at one time. For details, see the *Veritas 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.

Viewing the progress of a report

To view the report progress

1. Click a report type to view the configured reports of that type.
2. 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.

3 Optionally, select **Auto Refresh** to automatically refresh the progress details every 10 seconds.

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 *Activity Details for Paths* report as *Activity 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\Veritas\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 *Veritas Data Insight Administrator's Guide*.

To send a report by email

1. Do one of the following:
   - When creating a report, specify the email addresses of the recipients who you want to send the reports. The output is emailed to these recipients each time a report is generated.
   - Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.

If you want to send the latest report output through email, on the Reports home page, select the report, and in the **Select Action** drop-down, click **Email Latest**.

2 In the **Email report** popup, enter the email addresses of the recipients.

3 Click **Send**.

4 To email an older report output, in the **Select Action** drop-down, click **View**.

5 On the **Report Details** page, click the **Email** button adjacent to the report output you want to email.

6 Enter the email addresses of the recipients, and click **Send**.

Click the download report link in the received email to download the report output. You can disable this feature by setting the appropriate global properties.

Automatically archiving reports

For all the report types which support archiving actions, you can configure Data Insight to automatically archive a report once the report generates successfully. You can configure the following actions on the **Post-Processing Action** tab:

- Select a retention category on the archived data to indicate how long the data must be stored.

  Note: You must first select the data source from the **Data Selection** tab before you select any retention category.

- Select a post-processing action, such as deleting the original file and replacing it with a shortcut. The shortcut points to the new file location inside the archive.

Archiving is supported for the following types of reports:

- **Activity Details** reports.
- **Activity 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 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 *Veritas Data Insight Administrator's Guide*

See "About Retention categories" on page 220.

See "About post-processing actions" on page 221.

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 160.
2. The last run status on the Reports listing page displays the status of that report as **Canceled**.

Deleting a report

You can delete an instance of a report and all generated report outputs.

To delete a report

1. Click on the **Reports** tab. The Reports home page displays by default. The home page lists all the available reports for the logged in user.
2. Click a report type to view the instances of the report.

   A list of all instances for that report type appears in the content pane.

3 Click the check box next to the report to select multiple reports, and click **Delete**.

Select the report you want to delete, and in the **Select Action** drop-down, click **Delete**.

4 Click **OK** on the confirmation message.

Considerations for viewing reports

The following consideration applies when you try to view reports:

When you try to view PDF reports that are more than 100 MB, or HTML reports with size more than 300 MB (11 MB compressed size), a warning pop-up appears on the **Reports** list page. The pop-up indicates that if you continue to view the report, the web browser may experience some latency, or become unresponsive. You can choose to view the report in the web browser, cancel the operation, or download the report.

Note: The pop-up warning does not appear for CSV reports because when you select the CSV format, the report is downloaded on your computer.

Organizing reports using labels

Use labels to organize, easily find, and group reports from a long list of existing reports. For example, the label can denote the department that the report pertains to or the purpose of the report. You can add more than one label to a report.

You can view the labels associated with a report on the **Reports Home** page or the **Reports** list page. Use the free form filter to search for reports with specific labels.

All Data Insight users can add labels to reports.

Adding a label to a new report

You can add labels to reports from the Reports configuration wizard.

See “Creating a report ” on page 88.

Managing labels

You can apply label(s) to or remove the label(s) from existing reports.

To add a label to reports

1. From the **Reports Home** page or from the list page of a specific report, select the report outputs that you want to apply the label(s) to.
2. Click **Add Label**.
3. Name the labels. For example, HR, North America, or Media Files.
4. Click **Add**.

To edit a label

1. On the **Reports Home** page or from the list page of a specific report, select the report that you want to edit.
2. Click **Select Action** > **Edit**.
3. Make the necessary changes.
4. Click **Save**.

To remove a label

1. From the **Reports Home** page or from the list page of a specific report, select the report outputs from which you want to remove the label(s).
2. Click **Remove Label**.

   Deleting a label does not delete the reports under it.

Section 4

Remediation

- Chapter 9. Configuring remediation workflows
- Chapter 10. Using the Self-Service Portal
- Chapter 11. Managing data
- Chapter 12. Managing permissions

Chapter 9

Configuring remediation workflows

This chapter includes the following topics:

- About remediation workflows
- Prerequisites for configuring remediation workflows
- Configuring Self-Service Portal settings
- About workflow templates
- Managing workflow templates
- Creating a workflow using a template
- Managing workflows
- Auditing workflow paths
- Monitoring the progress of a workflow
- Remediating workflow paths

About remediation workflows

In large storage environments, it can become difficult to assign the responsibility of remediating data resources to data owners and custodians. Security and storage administrators have to manually inform data owners about issues with the resources that they own. Also, it can be tedious to track remediation actions on such resources.

Remediation workflows provide an easy way to fan out remediation tasks among configured custodians and data owners. The custodians are responsible for the data resources and can take a decision about the best way to remediate them. To

understand how custodians are assigned in Data Insight, refer to the *Veritas Data Insight User's Guide*.

You can use workflows to define a process to distribute remediation tasks to custodians. You can create the following workflows for different remediation tasks:

- **Entitlement Review**
  Review the user permissions on the folders that the custodians are responsible for and attest the permissions or suggest changes. The entitlement information for this workflow is generated by the Entitlement Review report.
  You can send the change request to a ticketing system or Identity and Access Management (IAM) tool, or use custom scripts to remediate the permissions.
- **Data Loss Prevention (DLP) Incident Remediation**
  View policy violations and take action on the files that violate policies. The policy information is pulled into Data Insight from Symantec Data Loss Prevention (DLP). The actions are Smart Response rules defined by DLP administrators. DLP uses the Smart Response rules to remediate the resources that violate configured DLP policies.
  Data Insight uses two DLP Web services for incident remediation - the Response Rules Listing Service and the Response Rule Execution Service. The Response Rule Listing Service provides a list of available response rules in DLP, such as delete or quarantine, for a given incident. The Response Rule Execution Service takes the response rule requests submitted by users from the Self-Service Portal and executes them in DLP. By default, the Response Rule Execution Service is disabled. You must enable the service to allow the portal users to remediate incidents.

  Note: Data Insight does not let you create an incident remediation workflow for sensitive paths that are imported into Data Insight using a CSV file. This is because the workflow requires data from DLP, such as Smart Response rules and incident IDs and severity information for paths that violate a policy.

  For more information about DLP incidents, see the *Symantec Data Loss Prevention Administrator's Guide*.
- **Ownership Confirmation**
  Confirm the ownership of files and folders in your storage environment.
- **Records Classification**
  Classify the sensitive files that must be retained for a legally mandated period. The workflow helps you classify files based on their business value and manage the life cycle of sensitive documents by applying data management rules to the classified data.

You can choose to archive the files that are marked as record and apply retention categories that define how long the files must be stored before being deleted. The files that are marked as record are retained based on the file classification policies that they violate.

You can use the workflow to trigger automatic actions only if your organization uses Enterprise Vault™ to archive data and if Enterprise Vault is configured in Data Insight.

Note: Creating workflows for the SharePoint Online, Microsoft OneDrive, and Documentum data sources is not supported.

Depending on the type of workflow, the custodian may perform the following actions:

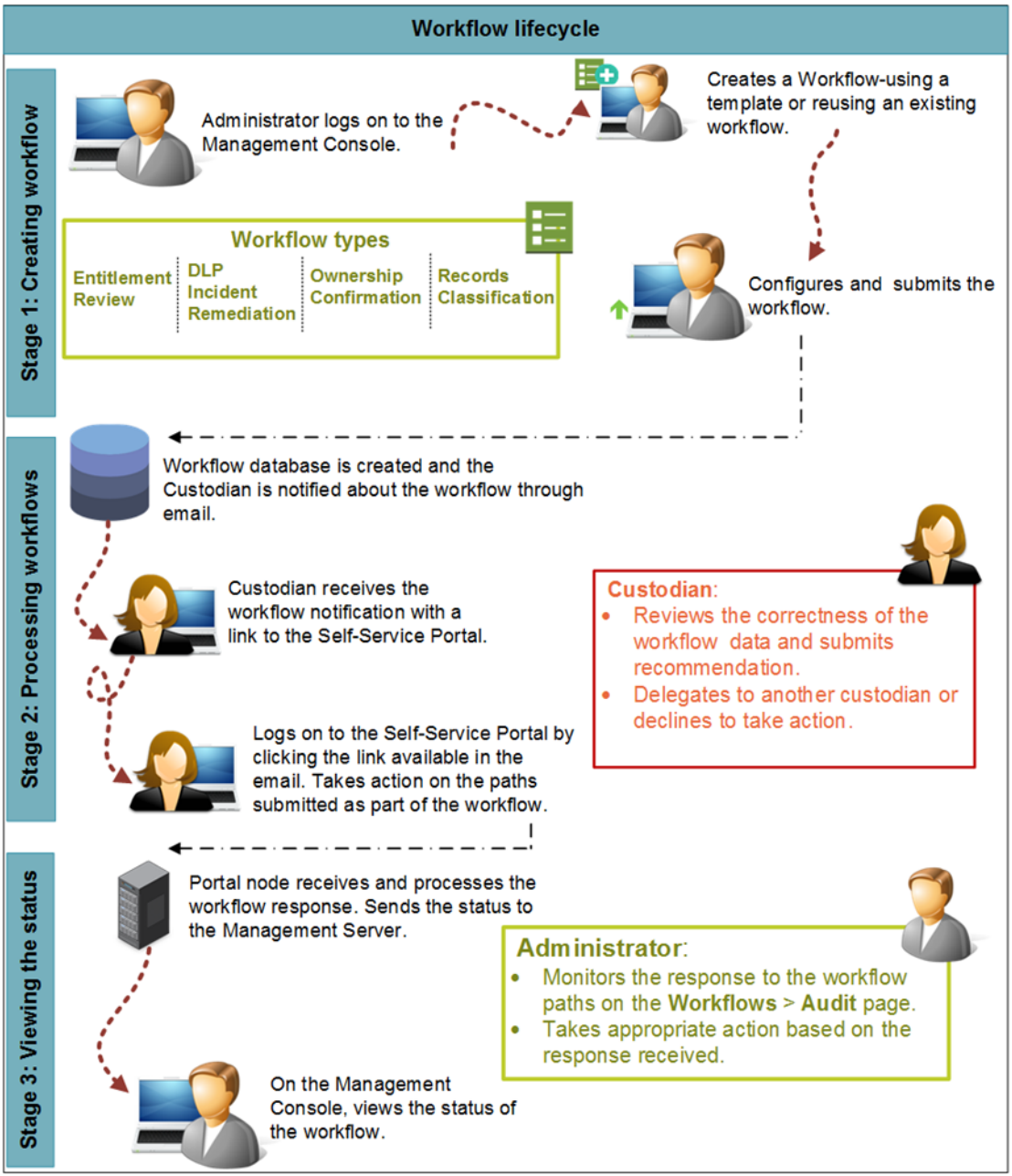
Workflow	Action
Entitlement Review	Review the user permissions on folders that the custodian owns and automatically trigger a permission remediation workflow to execute the changes. To trigger a permission remediation action, you must first configure the permission remediation settings.
DLP Incident Remediation	Choose the configured remediation actions, and submit the same for execution by the DLP Enforce Server.
Ownership Confirmation	Confirm the ownership of resources. Once the custodians confirm or deny the ownership, and the workflow is complete, the status summary is displayed in the Data Insight Management Console. A Data Insight administrator may review the status and take further actions based on it.
Records Classification	Mark a file as Record or No record. When the custodians submit their response and a file marked as Record, Data Insight automatically sends a request to Enterprise Vault™ to archive the document. and apply configured post-processing actions on the document if the following conditions are fulfilled: ■ Enterprise Vault is configured and if the option to use EV for archiving is selected when creating the workflow template. ■ Automatic response is enabled in the workflow.

Once you submit a workflow from the Data Insight console, the custodians receive an email notification with a link to the Self-Service Portal. They can log in to the

portal, choose the necessary remediation actions, and submit the same for execution by the DLP Enforce Server, Enterprise Vault server, or the Data Insight Management Server, depending on the type of workflow.

Note: If you do not have a valid portal license or if your base or portal license has expired, Data Insight disables the option to create workflows.

Figure 9-1 Workflow lifecycle



See “About workflow templates” on page 178.

See “Monitoring the progress of a workflow” on page 206.

Prerequisites for configuring remediation workflows

Before you can submit a remediation workflow to the Self-Service Portal, verify that the following configuration tasks are complete:

- The Portal server is installed and registered with the Management Server. You can verify the installation on the **Settings** > **Data Insight Servers** page.
  For more information about installing the Self-Service Portal, see the *Veritas Data Insight Installation Guide*.
- The directory service domains in your organization are configured in Data Insight, and the user and user group information is imported in Data Insight.
- The mail custom attribute is configured for the directory domain. Setting this attribute enables Data Insight to send the email alerts for submitted workflows to the custodian's email address.
- Custodians are assigned on paths that are configured in Data Insight. If some paths do not have any custodians assigned to them, you can assign custodians at the time of creating the workflow request.
- The SMTP server settings are configured.
- To create DLP Incident Remediation workflows, ensure that Data Loss Prevention (DLP) is installed and the DLP settings are configured in Data Insight.
- To use Enterprise Vault for the Records Classification workflow, ensure that Enterprise Vault is configured in Data Insight, and the device names in Enterprise Vault are mapped to those in Data Insight.

See the *Symantec Data Loss Prevention Data Insight Implementation Guide* for information about using the Data Loss Prevention web services to remediate incidents.

Configuring Self-Service Portal settings

You can personalize the look and feel of the Self-Service portal to match the branding of your organization.

To configure the portal settings

1. In the Management Console, click **Workflows** > **Self-Service Portal Settings**.
2. Edit all or any of the following settings:

Session timeout	Your login session on the Self-Service Portal times out after certain period of inactivity. The default time out period is 30 minutes. To change the default timeout period, enter the time in minutes.
Branding	Customize the header section of the portal by adding the following elements: ■ To add the logo of your organization to the header, browse to the location where the image is saved, and select it. The image must be in the `.png`, `.gif` or `.jpg` formats only. It is recommended that the size of the image must be 32x32. ■ Enter the text that you want to appear in the header section of the screen. For example, you can enter the name of your organization. ■ Enter the hexadecimal values to define the font and the background colors to be used in the header area.
Login help text	Enter any information that the portal users may need to login to the portal. For example, the login credentials that are required for the portal. This information is optional.
Support information	Enter information for the portal users to get assistance with the problems that they may encounter when using the portal. Support information can include an email address or the help desk number of the local support office.

3. Click **Save**.

About workflow templates

Data Insight provides a way to create templates to help you quickly create remediation workflows for the resources that are monitored by Data Insight. Using workflow templates saves you time because you can use certain common values defined in the template to create multiple workflow instances of the same type. For resources that need remediation, the workflow template lets you define the attributes to be displayed on the Self-Service Portal and the actions that the Self-Service Portal users can take on these resources. For example, in case of a DLP Incident Remediation template, you can selectively choose the Data Loss Prevention (DLP) Smart Response rules that you want to present for action by the portal users.

Refer to the Data Loss Prevention (DLP) documentation for details about DLP policies and Smart Response rules.

You can create multiple workflow instances from a template of the same type. You can also choose to edit a template to suit your requirement before you submit a workflow. For example, you can choose to change the frequency of email reminders, or customize the default email included in the template.

You can create a template for the following types of remediation workflows:

- Entitlement review
  See "Create/Edit Entitlement Review workflow template" on page 179.
- DLP Incident Remediation
  See "Create/Edit DLP Incident Remediation workflow template" on page 181.
- Ownership Confirmation
  See "Create/Edit Ownership Confirmation workflow template" on page 183.
- Records Classification

Note: If you do not have a valid portal license or if your base or portal license has expired, Data Insight disables the option to creation of workflow templates.

See "Managing workflow templates" on page 178.

See "Creating a workflow using a template" on page 187.

Managing workflow templates

You can create multiple templates for each type of workflow. You can customize templates to define the different options that appear on the Self-Service Portal.

To create a workflow template

1. On the Management Console, click **Workflows** > **Templates**.
2. On the list page, click **Add New Template**. Select the type of workflow template that you want to create. For example, DLP Incident Remediation.
3. Specify relevant values in each of the fields and click **Save**.

   You can use the template to create a remediation workflow of the same type.

   See "Creating a workflow using a template" on page 187.

You can edit, copy, or delete an existing template.

To manage existing templates

1. On the Management Console, click **Workflows** > **Templates**.
2. Select a workflow template, and select the appropriate action:
   - To edit a template, click **Select Action** > **Edit**.
     Make necessary changes to the template, and click **Save**.
   - To copy a template, click **Select Action** > **Copy**.
     Enter the name of the new template. Data Insight creates a replica of the selected template with the new name.
   - To delete a template, click **Select Action** > **Delete**.
     Click **Yes** on the confirmation message.

     Note: You cannot delete a template if it is being used for creating a workflow.

Create/Edit Entitlement Review workflow template

Use the dialog to create a template of type Entitlement Review.

Table 9-1 Entitlement Review template options

Option	Description
Template Type	Describes the type of workflow that can be created using the template.
Name	Enter a logical name for the template.
Description	Enter a short description for the template. The description can state the kind of Entitlement Review workflow for which the template should be used.

Table 9-1 Entitlement Review template options *(continued)*

Option	Description
Welcome Text	This text appears in a pop-up when the custodian first logs in to the Self-Service Portal. You can include the specific instructions for remediation in this field.
Portal Options	Select all or any of the check boxes to display additional information on the Self-Service Portal. Some of the options are explained below: ■ **Show suggested owner** - Displays information about the inferred owner in the path summary section on the portal node. The suggested owner is inferred on the basis of the global Workspace Data Owner Policy. ■ **Show sensitive data information** - Displays the number of sensitive files in a folder and the policies that they violate. ■ **Show Groups** Display the names of the directory service groups that a user is part of. ■ **Include custom attributes of user** - Displays custom attributes of a user in the portal. From the drop-down menu, select any of the custom attributes as per your requirements. ■ **Show creator owner information** - Flags a user who has permissions on the folder as the creator owner on the Self-Service Portal. The creator owner is the user who initially created the folder. By default, a creator owner has Full Control permission on the folder. Custodians can use the information to evaluate permissions assigned to the creator owner and take appropriate remediation actions, such as remove creator owner from a path. If the **Show creator owner information** check box is cleared, the custodians will only see the users and the permissions assigned to them on the Portal UI. ■ **Allow delegation** - Allows the reviewer to delegate the review task to another user.
Email Reminder	Select the frequency, day, time for sending email reminders to the custodians.

Table 9-1 Entitlement Review template options *(continued)*

Option	Description
Customize Email	Do the following: **1** Click to customize the email that is sent to custodians when a workflow is submitted for remediation. **2** Insert the variable in the **To**, **From**, **CC**, and **Subject** fields. **3** Add the **${workflow.link}** variable in the body of the email to include the link to the portal in the request. Note that the SMTP server settings must be configured to enable Data Insight to send an email.

See "About workflow templates" on page 178.

See "Managing workflow templates" on page 178.

Create/Edit DLP Incident Remediation workflow template

Use the dialog to create a template of type Data Loss Prevention (DLP) Incident Remediation.

Table 9-2 DLP Incident Remediation template options

Option	Description
Template Type	Describes the type of workflow that can be created using the template.
Name	Enter a logical name for the template.
Description	Enter a short description for the template. The description can state the kind of DLP Incident Remediation workflow for which the template should be used.
Welcome Text	Select the check box to display a message to the portal users. Use the variables from the adjoining drop-down to create the message. This text appears in a pop-up when the custodian first logs on to the Self-Service Portal. You can include the specific instructions for remediation in this field.

Table 9-2 DLP Incident Remediation template options *(continued)*

Option	Description
Portal Options	Click the **Refresh** icon to fetch the latest rules from DLP. **DLP Smart Response** - Data Insight fetches the Smart Response rules that are configured in DLP using the DLP Response Rule Listing Service API. The Response Rule Listing Service provides the available response rules for a given incident. These rules define the actions that portal users are allowed to take on the paths that violate DLP polices, such as delete or quarantine. Data Insight fetches the Response Rules applicable to CIFS and SharePoint paths, as well as the rules that apply to cloud content sources, such as Box. Select the following: ■ From the drop-down, select the configured the applicable Smart Response Rule. ■ Select the check boxes for the file attributes that you want to display on the Self-Service Portal. The displayed attributes include information about the suggested owner (owner inferred based on the global Workspace Data Owner Policy) and the DLP policy name. The file owner information may not reflect the responsible party. The responsible party or data owner can be a line manager in the business unit, the head of a department, or an information security officer. Data Insight provides information to tie the most active user of a file to a manager or responsible party for remediation steps. ■ Select **Allow delegation**, if you want to let the custodians delegate the workflow to other users being monitored by Data Insight.
Email Reminder	Select the frequency, day, time for sending email reminders to the custodians.
Customize Email	Do the following: **1** Click to customize the email that is sent to custodians when a workflow is submitted for remediation. **2** Insert the variable in the **To**, **From**, **CC**, and **Subject** fields. **3** Add the **${workflow.link}** variable in the body of the email to include the link to the portal in the request. Note that the SMTP server settings must be configured to enable Data Insight to send an email.

See “About workflow templates” on page 178.

See “Managing workflow templates” on page 178.

Create/Edit Ownership Confirmation workflow template

Use the dialog to create a template of type Ownership Confirmation.

Table 9-3 Ownership Confirmation template options

Option	Description
Template Type	Describes the type of workflow that can be created using the template.
Name	Enter a logical name for the template.
Description	Enter a short description for the template. The description can state the kind of Ownership Confirmation workflow for which the template should be used.
Welcome Text	This text appears in a pop-up when the custodian first logs in to the Self-Service Portal. You can include specific instructions for the portal users in this field.
Portal Options	Select the following options for the file attributes that you want to display on the Self-Service Portal: ■ **Show suggested owner** - Displays a column showing the owner inferred on the basis of the global Workspace Data Owner Policy. ■ **DLP Information** - Displays the number of sensitive files in a folder and the policies that they violate. ■ **Show active user count** Displays the number of active users for the data that is being remediated.
Email Reminder	Select the frequency, day, time for sending email reminders to the custodians.
Customize Email	Do the following: **1** Click to customize the email that is sent to custodians when a workflow is submitted for remediation. **2** Insert the variable in the **To**, **From**, **CC**, and **Subject** fields. **3** Add the **${workflow.link}** variable in the body of the email to include the link to the portal in the request. Note that the SMTP server settings must be configured to enable Data Insight to send an email.

See “About workflow templates” on page 178.

See “Managing workflow templates” on page 178.

Create/Edit Records Classification workflow template

Use the dialog to create a template of type Records Classification.

Table 9-4 Records Classification template options

Option	Description
Template Type	Describes the type of workflow that can be created using the template.
Name	Enter a logical name for the template.
Description	Enter a short description for the template. The description can state the purpose of the workflow for which the template should be used.
Welcome Text	Select the check box to display a message to the portal users. This text appears in a pop-up when the custodian first logs in to the Self-Service Portal. You can include the specific instructions for remediation in this field. Use the variables from the adjoining drop-down to create the message.

Table 9-4 Records Classification template options *(continued)*

Option	Description
Portal Options	

Table 9-4 Records Classification template options *(continued)*

Option	Description
	Select the following: ■ **Record action name** - Enter a logical name for the action that is taken on the file that is marked as a record. For example, *Archive*. The action name that you configure is displayed in the **Select Action** drop-down on the Self-Service portal. When a file is marked as a record, it is archived for the configured retention period, if you choose to use Veritas Enterprise Vault™ for archiving and automatic action is enabled when you configure the workflow. You must create a `mappings.csv` file which maps the file classification policies to the retention category. The retention categories determine how long the archived data is stored before it is deleted from the storage device. Data Insight uses the sensitive file classification policy to retention category mapping to ensure that a file that violates a certain DLP policy is retained for the period configured for the mapped retention category **Note:** Ensure that `mappings.csv` is saved in the data directory at `$datadir\conf\workflow\steps\ev\mappings.csv`. A sample mappings.csv file is available for download on the workflow template page. ■ **Non-record action name** - Enter a logical name for the action that is taken on the file that is marked as non-record. For example, *Do not archive*. ■ Select the **Use Enterprise Vault for archiving** check box if your organization uses Veritas Enterprise Vault to archive and maintain data stored on network shares. **Enterprise Vault post-processing action** - From the drop-down select the action you want to apply to the file. For more information about what each post-processing action listed in the drop-down means, see the *Veritas Data Insight User's Guide*. ■ Select the check boxes for the file attributes that you want to display on the Self-Service Portal. The displayed attributes include information about the suggested owner and Data Loss Prevention (DLP) or other file classification policy name. The file owner information may not reflect the responsible party. The responsible party or data owner can be a line manager in the business unit, the head of a department, or

Table 9-4 Records Classification template options *(continued)*

Option	Description
	an information security officer. Data Insight provides information to tie the most active user of a file to a manager or responsible party for remediation steps. Select **Allow delegation**, if you want to let the custodians delegate the workflow to any other custodian.
Email Reminder	Select the frequency, day, time for sending email reminders to the custodians.
Customize Email	Do the following: **1** Click to customize the email that is sent to custodians when a workflow is submitted for remediation. **2** Insert the variable in the **To**, **From**, **CC**, and **Subject** fields. **3** Add the **${workflow.link}** variable in the body of the email to include the link to the portal in the request. Note that the SMTP server settings must be configured to enable Data Insight to send an email.

See "About remediation workflows" on page 170.

Creating a workflow using a template

You can create an instance of a workflow using an existing template or by creating a new template that precisely suits your needs.

To create and submit a workflow

1. In the Management Console, click on the **Workflows** tab and then the **Workflows** sub-tab.
2. On the list page, click **Create Workflow**, and click the type of workflow you want to create.

   On the workflow panel, enter the relevant information.
3. Click **Submit** to submit the workflow for further action by the custodians, or click **Save & Close** to save the workflow details.

See "Create Entitlement Review workflow options" on page 188.

See "Create DLP Incident Remediation workflow options" on page 192.

See "Create Ownership Confirmation workflow options" on page 196.

See "Create Records Classification workflow options" on page 197.

Create Entitlement Review workflow options

Use the dialog to create an instance of an Entitlement Review workflow. You can view the summary of the options you select in the right-hand panel of the page.

Note: Creation of Entitlement Review workflows is not supported for the Microsoft OneDrive, SharePoint Online, and Documentum data sources.

Table 9-5 Create Entitlement Review workflow

Option	Description
Workflow Information	Enter information in the following fields: ■ Name - Enter a logical name for the workflow. ■ Description - Enter a short description for the workflow. Workflow Type - Describes the type of workflow. Template - Select the template you want to use for creating the workflow. See "About workflow templates" on page 178. ■ Portal Node for Execution - From the drop-down, select the Self-Service Portal node to which you want to submit the workflow. ■ Click **Test portal connection** to test the availability of SMTP connection to the Self-Service Portal. Enter the email IDs of the recipients of the workflow request, and click **Test**. You will see a response from the SMTP server if the connection to the Portal node succeeds. ■ Action - Select **Apply configured permission remediation action automatically** to let Data Insight automatically take the configured actions by a remediation workflow. To avail this feature, you must first configure Data Insight for permission remediation. ■ Schedule - Select the start and the end date for completing the workflow.

Table 9-5 Create Entitlement Review workflow *(continued)*

Option	Description
Data Selection	Do the following: **1** Select the **Physical** radio button to view the configured file servers or SharePoint web applications. Or, select the **DFS** radio button to view the configured DFS paths in a domain. **2** From the **Resource Selection** drop-down, select one of the following options: ■ Physical or DFS paths - Select the physical or DFS paths for which you want to review the user permissions. ■ Opens Shares - Select the open shares that need to be remediated. ■ Containers - Select configured containers. Data Insight presents the paths in the containers to remediate user permissions. ■ Enter paths manually - Enter the full path that you want to remediate. ■ Upload CSV - Browse to the location of the .csv file that contains the paths that you want to remediate. Only valid paths in the .csv file are displayed in the **Selected Resources** pane. ■ Select paths having custodians - Data Insight retrieves only the list of paths that have custodian assignments. Select the paths from the list. The selected data set is listed in the **Selected Resources** pane. **Note:** Data Insight does not support NFS, SharePoint Online, Microsoft OneDrive, and Documentum for the Entitlement Review workflows. If you select a container which contains these paths, then those paths will not be sent to the custodian for review.

Table 9-5 Create Entitlement Review workflow *(continued)*

Option	Description
Resource-Custodian Selection	This panel displays the following: ■ The paths that you select under the **Data Selection** tab. ■ The paths for which custodians are already assigned and those paths for which custodians are not assigned. ■ The email address of the custodian. Data Insight displays the email address only if you have added the email custom attribute, and have also marked the attribute as email alias when you add the directory service. You can assign custodians on paths or remove already assigned custodians. For example: ■ Click **Import Custodian** to assign custodian to a selected path. Select any of the following options: ■ Upload a .csv file with custodian information. ■ Select a user who is configured in Data Insight as the custodian. ■ Select a Data Insight suggested data owner as the custodian. ■ Select a custom attribute of a Data Insight suggested data owner and assign it as a custodian. For example, you can select the manager of a user who is a suggested data owner as the custodian. ■ Click **Assign Custodian** to manually assign the custodian for a selected path. Use the domain filter to filter the users based on their directory domains. ■ Click **Remove Custodian** to remove a custodian from a selected path. ■ Click **Delete Paths** to remove the selected paths.
Exclusion List	Select the groups or users that you want to exclude from the scope of the review. Click the group or user to select it. The selected data set is listed in the **Selected Groups/Users** panel. Once you have excluded a user or a group, the activities of the user or the group on the paths will be ignored and thus will not be considered for the review.

Customizing Entitlement Review report output

The Entitlement Review report reviews user entitlements on a specified path. You can customize the report and configure it to do the following:

1. Non-expansion of certain groups.

By default, the report output displays the permissions that are assigned to specific users within groups. You can configure the report such that specific groups are not expanded and the report only displays the permissions for the group and not for all the users within the group. To configure groups for non-expansion:

- Use the sample file, `simple_permissions_attr.properties` to specify comma-separated SIDs of the groups that you do not want to expand.
- Save the file in the default data directory, `C:\DataInsight\data\console\reports\customHeaders`. You can also choose to save the file at any other location.

2. Consider global groups in the report.

   By default, the Entitlement Review report does not display permissions for certain well-known groups such as Everyone or Authenticated Users. To consider global groups in the report:

   - In the `simple_permissions_attr.properties` file, set the following property:
     `perm_wkex_sid_exclusion=1`

   Note: Global groups are not expanded.

3. Consider permission bits for tuning permissions that are displayed on the **Workspace** tab.

   By default, Entitlements Review workflow displays three permissions - Full Control, Read, and Modify. We can add more permission names to be visible in the workflow or modify current definition by using a mapping file. To display more permissions or change the default name of a permission:

- Use the `sample er_mappings.properties` file to specify the permission bits mapping to the permissions to be shown in the workflow. For example, you may want to map the Windows permission Full Control to be displayed as Full Ownership.
- Place this file under `C:\DataInsight\data\conf\workflow`.
- Ensure that you take care of the permission precedence. If there are two permission bits set for a group or user, the Entitlement Review workflow maps the custom permission name to the permission name appearing in first precedence.

Create DLP Incident Remediation workflow options

Use the dialog to create an instance of a Data Loss Prevention (DLP) Incident Remediation workflow. You can view the summary of the options you select in the right-hand panel of the page.

Note: Creation of DLP Incident Remediation workflows is not supported for the Microsoft OneDrive, SharePoint Online, and Documentum data sources.

Table 9-6 Create DLP Incident Remediation workflow

Option	Description
Workflow Information	Enter information in the following fields: ■ **Name** - Enter a logical name for the workflow. ■ **Description** - Enter a short description for the workflow. ■ **Workflow Type** - Describes the type of workflow. ■ **Template** - Select the template you want to use for creating the workflow. See "About workflow templates" on page 178. ■ **Portal Node for Execution** - From the drop-down, select the Self-Service Portal node to which you want to submit the workflow. Click **Test portal connection** to test the availability of network connection between the Data Insight Management Server and the Self-Service Portal. ■ Click **Test portal connection** to test the connection between the SMTP server and the DLP Enforce Server to the Self-Service Portal. Enter the email IDs of the recipients of the workflow request, and click **Test**. You will see a response from the SMTP server if the connection to the Portal node succeeds. ■ Select the start and the end date for completing the workflow.

Table 9-6 Create DLP Incident Remediation workflow *(continued)*

Option	Description
Data Selection	

Table 9-6 Create DLP Incident Remediation workflow *(continued)*

Option	Description
	Do the following: **1** Select the **Physical Hierarchy** radio button to view the configured file servers or SharePoint web applications. Or, select the **DFS Hierarchy** radio button to view the configured DFS paths in a domain. **2** From the Resource Selection drop-down, select one of the following options: ■ Physical or DFS paths - Select the physical or DFS paths that violate DLP policies. ■ Opens Shares - Select the open shares that need to be remediated. ■ Containers - Select configured containers. Data Insight presents the paths in the containers that violate DLP policies. ■ Policies - Data Insight displays the configured DLP policies. Select a policy to remediate the paths that violate the policy. ■ Enter paths manually - Enter the full path that you want to remediate. ■ Upload CSV - Browse to the location of the .csv file that contains the paths that you want to remediate. Only valid paths in the CSV file are displayed in the **Selected Resources** pane. **Note:** Custodians that are assigned through CSV are applicable only for the workflow. They will not be assigned to paths in Data Insight. To assign a user as a custodian for paths Data Insight, you must explicitly assign them from the Management Console. ■ Select paths having custodians - Data Insight retrieves only the list of paths that have custodian assignments. Select paths from the list. You must you run the Data Custodian Summary report to fetch recent custodian assignments. The selected data set is listed in the **Selected Resources** pane. **Note:** You can only select paths containing sensitive files if the file classification information is fetched from DLP. If the sensitive file information in your environment is imported into Data Insight using a .csv file, it does not let

Table 9-6 Create DLP Incident Remediation workflow *(continued)*

Option	Description
	you select paths for remediation. This is because the Incident Remediation workflow requires a DLP incident ID and severity information for effective remediation. For more information about DLP incidents, see the *Symantec Data Loss Prevention Administrator's Guide*.
Resource-Custodian Selection	This panel displays the following: ■ The paths that you select under the **Data Selection** sub-tab. ■ The paths for which custodians are already assigned and those paths for which custodians are not assigned. ■ The email address of the custodian. Data Insight displays the email address only if you have added the email custom attribute and have also marked the attribute as email alias when you add the directory service. For the paths that do not have custodians, you can assign custodians using the following methods: **1** Click **Import Custodian**, and select one of the following options: ■ Upload a .csv file with information about paths and corresponding custodians ■ Select a user who is configured in Data Insight as the custodian. ■ Select a Data Insight suggested data owner as the custodian. ■ Select a custom attribute of a Data Insight suggested data owner and assign it as a custodian. For example, you can select the manager of a user who is a suggested data owner as the custodian. **2** Click **Assign Custodian**, and select the custodian from the users list. You can remove custodians from selected paths or delete paths from the workflow. Do the following: **1** Click **Remove Custodian** to remove a custodian from a selected path. **2** Click **Delete Paths** to remove the selected paths from the workflow.

Create Ownership Confirmation workflow options

Use the dialog to create an instance of an Ownership Confirmation workflow. You can view the summary of the options you select in the right-hand panel of the page.

Table 9-7 Create Ownership Confirmation workflow

Option	Description
Workflow Information	Enter information in the following fields: ■ **Name** - Enter a logical name for the workflow. ■ **Description** - Enter a short description for the workflow. ■ **Workflow Type** - Describes the type of workflow. ■ **Template** - Select the template you want to use for creating the workflow. ■ **Portal Node for Execution** - From the drop-down, select the Self-Service Portal node to which you want to submit the workflow. ■ Click **Test portal connection** to test the availability of SMTP connection to the Self-Service Portal. Enter the email IDs of the recipients of the workflow request, and click **Test**. You will see a response from the SMTP server if the connection to the Portal node succeeds. ■ **Schedule** - Select the start and the end date for completing the workflow.

Table 9-7 Create Ownership Confirmation workflow *(continued)*

Option	Description
Data Selection	Do the following select one of the following options: **1** **Select paths having custodians** - Data Insight retrieves only the list of paths that have custodian assignments. Select paths from the list. You must run the **Data Custodian Summary** report to fetch recent custodian assignments. **2** **Import Custodian CSV** - Browse to the location of the .CSV file that contains the paths that you want to remediate. Only valid paths in the .CSV file are displayed in the **Selected Resources** pane. You can download the sample CSV template or create your own in the prescribed format. **Note:** Custodians that are assigned through CSV are applicable only for the workflow. They will not be assigned to paths in Data Insight. To assign a user as a custodian for paths Data Insight, you must explicitly assign them from the Management Console. **3** Optionally, click **Select All Resources** to select all the paths to which custodians are assigned. Filter the list of displayed paths, based on custodian name or custodian attribute, and manually select the resources. Click **Re-Generate** to regenerate the custodian map and refresh the listed paths in the panel. The selected data set is listed in the **Selected Resources** pane.
Resource-Custodian Selection	This panel displays the data set selected in the **Data Selection** tab. You can review the selected paths on the basis of criteria such as custodians and custodian email. You can remove a selected path from the list. Click **Delete Paths** to remove any paths from the selected resources.

Create Records Classification workflow options

Use the dialog to create an instance of a Records Classification workflow. You can view the summary of the options you select in the right-hand panel of the page.

Table 9-8 Create Records Classification workflow

Option	Description
Workflow Information	Enter information in the following fields: ■ **Name** - Enter a logical name for the workflow. ■ **Description** - Enter a short description for the workflow. ■ **Workflow Type** - Describes the type of workflow. ■ **Template** - Select the template you want to use for creating the workflow. See "About workflow templates" on page 178. ■ **Portal Node for Execution** - From the drop-down, select the Self-Service Portal node to which you want to submit the workflow. Click **Test portal connection** to test the availability of network connection between the Data Insight Management Server and the Self-Service Portal. ■ Click **Test portal connection** to test the connection between the SMTP server and the DLP Enforce Server to the Self-Service Portal. Enter the email IDs of the recipients of the workflow request, and click **Test**. You will see a response from the SMTP server if the connection to the Portal node succeeds. ■ Select **Apply configured Record action automatically** to archive the file, apply the post-processing action, and apply the appropriate retention category to the file that is marked as record. The post-processing actions that you want to apply to files that are marked as record are configured in the workflow template. **Note:** Data Insight can take automatic action on files that are marked as record only if Veritas Enterprise Vault™ is configured in Data Insight. See "Create/Edit Records Classification workflow template" on page 184. ■ Select the start and the end date for completing the workflow.

Table 9-8 Create Records Classification workflow *(continued)*

Option	Description
Data Selection	Do the following: **1** Select the **Physical Hierarchy** radio button to view the configured file servers. **2** From the Resource Selection drop-down, select one of the following options: ■ Physical paths - Select the physical that violate policies. ■ Opens Shares - Select the open shares that need to be remediated. ■ Containers - Select configured containers. Data Insight presents the paths in the containers that violate DLP policies or policies imported through CSV. ■ Policies - Data Insight displays the configured policies. The policy information is either pulled from DLP or imported into Data Insight using a CSV file. Select a policy to remediate the paths that violate the policy. ■ Enter paths manually - Enter the full path that you want to remediate. ■ Upload CSV - Browse to the location of the .csv file that contains the paths that you want to remediate. Only valid paths in the .csv file are displayed in the **Selected Resources** pane ■ Select paths having custodians - Data Insight retrieves only the list of paths that have custodian assignments. Select paths from the list. You must run the Custodian Summary report to fetch recent custodian assignments. **Note:** You can not add DFS, NFS, or SharePoint OneDrive, and Documentum paths for the Record Classification workflow. For example, if such paths are part of a container, or a CSV file, Data Insight ignores these paths when adding the resources for the workflow. The selected data set is listed in the **Selected Resources** pane.

Table 9-8 Create Records Classification workflow *(continued)*

Option	Description
Resource -Custodian Selection	This panel displays the following: ■ The paths that you select under the **Data Selection** sub-tab. ■ The paths for which custodians are already assigned and those paths for which custodians are not assigned. ■ The email address of the custodian. Data Insight displays the email address only if you have added the email custom attribute and have also marked the attribute as email alias when you add the directory service. For the paths that do not have custodians, you can assign custodians using the following methods: **1** Click **Import Custodian**, and select one of the following options: ■ Upload a .csv file with information about paths and corresponding custodians ■ Select a user who is configured in Data Insight as the custodian. ■ Select a Data Insight suggested data owner as the custodian. ■ Select a custom attribute of a Data Insight suggested data owner and assign it as a custodian. For example, you can select the manager of a user who is a suggested data owner as the custodian. **2** Click **Assign Custodian**, and select the custodian from the users list. You can remove custodians from selected paths or delete paths from the workflow. Do the following: **1** Click **Remove Custodian** to remove a custodian from a selected path. **2** Click **Delete Paths** to remove the selected paths from the workflow.

Managing workflows

On the workflow details page, you can complete the following tasks:

- Create new workflows
  See "Creating a workflow using a template" on page 187.
- View detailed information about submitted workflows.

See "Viewing details of submitted workflows" on page 201.

- Extend the deadline of a submitted workflow.
  See "Extending the deadline of a workflow" on page 201.
- Cancel or delete a workflow.
  See "Canceling or deleting a workflow" on page 203.
- Manage workflows submitted to custodians for some other reason unable to complete the workflow.

See "About remediation workflows" on page 170.

Viewing details of submitted workflows

You can view details of workflows submitted for action by custodians on the **Workflows** list page.

To view submitted workflows

1. In the console, click the **Workflows** tab and then the **Workflows** sub-tab.
2. On the **Workflows** list page, review the following information about the submitted workflows:
   - The name of the workflow.
   - The status of the workflow.
     If there are multiple workflows listed on the page, use the **Filter** field to search for the workflow you are interested in. Or use the dynamic search option to search for workflows based on the type or their status.
     Hover the mouse over the progress bar to know the number of completed and pending requests in the workflow.
   - The date when the workflow was submitted.
   - The number of days within which the workflow request must be completed.
   - The number of custodians that have been assigned the workflow.

Extending the deadline of a workflow

You can extend the deadline of an already submitted workflow.

To extend the deadline of a submitted workflow

1. On the **Workflows** list page, click the **Select Action** drop-down corresponding to the workflow for which you want to extend the deadline.
2. Select **Extend Deadline**.

3 On the pop-up, select the new end date for the workflow.

4 Click **Extend**.

Note: Once you submit a workflow, you can only modify the deadline to complete the workflow.

See "Monitoring the progress of a workflow" on page 206.

Copying a workflow

You can replicate the workflow to create a new instance by copying a workflow. For example, if a workflow has expired or failed due to any reason, you can copy the workflow to create another workflow. All the attributes of the workflow are copied to the new workflow. When you copy a workflow, the new instance of the workflow will be in a draft state and the **Status** of the new instance of workflow would be set to **Draft**.

To copy a workflow

1 On the **Workflows** listing page, click the **Select Action** drop-down corresponding to the workflow you want to copy.

2 Click **Copy**.

3 Enter a logical name for the workflow, and click **Copy**.

Note: You can copy a workflow when the workflow is in any status.

Managing submitted workflows

You can log in to the Self-Service portal as custodian to review or delegate submitted workflows. You may log in as a custodian in the following scenarios:

- To review the correctness of the data submitted for action to the custodian.
- To delegate a submitted workflow to another custodian if the original custodian has left the organization or for any other reason is unable to complete a workflow.

Data Insight sends a notification to the custodian that the administrator has logged in to a workflow on the behalf of the custodian.

To manage submitted workflows on behalf of a custodian

1 On the **Workflows** listing page, click the **Select Action** drop-down corresponding to the workflow you want to review.

2 Select **Login as Custodian**.

3 From the **Select Custodian** pop-up, select the custodian you want to log in as.

4 Click **OK** to launch the Self-Service portal. The portal login page appears. The **Username** field is pre-populated with your network username.

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

You can review the workflow and take any action as required.

Note: The option to log in as custodian is not available if the workflow is complete or if the custodian has submitted his responses for further action for all assigned paths.

Canceling or deleting a workflow

You can cancel a submitted or in-progress workflow. For example, you can cancel a workflow, if the custodian who is required to take action has left the organization. Custodians will stop receiving email reminders to complete the workflow when you cancel it.

You can delete a workflow if the deadline for completing the tasks in the workflow has expired, or if the workflow is complete or has been canceled.

To cancel or delete a workflow

1 On the **Workflows** listing page, click the **Select Action** drop-down corresponding to the workflow you want to delete or cancel.

2 Click **Delete** or **Cancel**, as appropriate.

Note: When you delete a workflow, it will be deleted from the **Audit** listing page too. If you want to delete more than one workflow at a time, you can select the check boxes in front of the workflows by clicking on them and then select **Delete Workflow**.

Auditing workflow paths

Data Insight provides a centralized view where you can audit the information of all the workflow paths across all workflows. The **Audit** page provides an audit trail for the actions taken by custodians through the Self-Service Portal on paths across all types of workflows.

Navigate to **Workflows** > **Audit** to review the details of all paths submitted for custodian action. You can view the following details on this page:

- The list of paths submitted as a part of various workflows.
- The name of the workflow. Click the workflow name to navigate to the details page of that workflow.
- The state of a path such as successfully executed, failed, expired, executing action, or canceled.
- The recommended action that is submitted by the custodian from the Self-Service Portal for a workflow path.
- The time at which the custodian has submitted response for the workflow path.
- The date of completion of the workflow path when the status is logged as either expired, canceled, failed or success.
- The name of the custodian who has been assigned the workflow path.

In case of Entitlement Review workflows, if the Custodian has revoked the access for a user/group from a path, the **Audit** page displays only those workflow paths where users' or groups' access has been revoked and not the users or groups who have been allowed access to that workflow path. The **Custodian Action** column will display the value as **Revoke access for user/group**.

Certain columns are hidden from the view. Click the drop-down button on any column heading and select the columns that you want to display.

When the hidden columns are displayed, you can view the following details:

- The name of the device that the workflow path is located in.
- The type of workflow.
- The logon name of the custodian.
- The comment given by the custodian while delegating the remediation on a path or declining to take action on a path.
- The last response received for the workflow path when it is either failed or successful.
- The sequence of delegation by the custodian(s).
- The user or groups with permissions on paths in an Entitlement Review workflow.
- The logon name of the user who has permissions on the path in case of an Entitlement Review workflow.
- Whether or not a user is active on the path in case of an Entitlement Review workflow.
- The groups of which the user is a direct member in an Entitlement Review workflow.

- The permission granted to users on a path in an Entitlement Review workflow.
- The retention category in Enterprise Vault using which the path is archived in the Records Classification workflows.
- The policies that are violated by a workflow path.
- The severity of the incident in case of the DLP Incident Remediation or Records Classification workflows.

Note: When you hover your mouse on any column headers or values, tool-tips are displayed. If the status of a workflow path is **Failed**, the tool-tip displays the reason behind the failure.

You can take remediation actions for the paths that are part of the **Records Classification** and **Entitlement Review** workflows from the **Workflows** > **Audit** page.

See "Remediating workflow paths" on page 209.

Filtering workflow audit listing

You can refine the audit data set using the predefined and advanced filters, and sort through the workflow paths that are listed on the **Audit** page.

Use predefined filters to filter the lists by various categories such as by Device Name, Workflow Type, Custodian Action, and Status. If you select more than one category, the filter conditions are applied using the logical operator AND. For example, if you select the **Workflow Type** as **DLP Incident Remediation** and the **Status** as **Failed**, a list of all those DLP Incident Remediation workflow paths that are failed is displayed.

In addition, you can use the advanced filter at the top of the table to filter on the basis of various column names including those columns that are hidden. You must display the hidden columns to view the filter results. Select the column name and choose a value to further narrow down the results on the basis of the following operators, **equals**, and **contains**.

Note: The predefined filter options are displayed dynamically on the basis of the advanced filter that are applied for listing.

Monitoring the progress of a workflow

On the **Workflows** listing page, you can view the progress of workflows that are submitted to the Self-Service Portal. You can also view the details of the actions that are taken on all paths that are part of a workflow.

All workflow-specific jobs must run before you can see the response that the custodian submits from the Veritas Self-Service Portal on the Data Insight Console.

To view the status of a workflow

1. On the console, click the **Workflows** tab and then the **Workflows** sub-tab.

   On the **Workflows** list page, you can view the status for each workflow. The following table describes the possible status for any workflow:

Status	Description
Draft	When the workflow is saved as a draft but is not submitted to the portal server.
Submitted	When the workflow is submitted from the Management Server but is not picked up by the Portal server for processing.
In-progress	When workflow is being processed by the portal server for processing .
Completed	A workflow is marked as complete if: ■ The end date of the workflow lapses and after a day of grace period from the end date. ■ An action is taken on all the paths by all the custodians and the portal server has processed the workflow
Canceled	If you have canceled the workflow.
Grace Period	After the due date of the workflow, an extra day is given as grace period. In this case, the state of the workflow is set to **Grace Period**. If actions are still not taken by the end of the grace period, the status changes to **Completed**, and the state of the paths will be shown as **Expired**.

Status	Description
Failed	If Data Insight fails to create a workflow database based on the input that is provided for the workflow.

2. On the workflow listing page, click **Select Action** > **View**, or click the workflow link to view details of a submitted, completed, or canceled workflow.
3. On the workflow summary page, you can view the list of paths that are submitted for custodians' actions on the Self-Service Portal. The page also displays the summary of the total paths in the workflow, the percentage of paths on which an action is submitted on the portal, and the time within which the workflow must be completed.

   Select a path to review the details of the workflow.

   Depending on the type of the workflow, you can also view the following details:

   - In case of an Entitlement Review workflow, the users whose permissions were reviewed, the current permissions assigned to the user on that path, the activity status of the user, the direct groups from which permissions are inherited by the user, the custodian's recommendation - whether to allow access to the user or not, and whether the user is a creator owner on the path.
   - In case of a DLP Incident Remediation workflow, the Data Loss Prevention (DLP) policies that the paths violate, the severity of the incidents, and the incident IDs that need to be remediated. The incident ID is associated with the available response rules for a given incident.
   - In case of a Records Classification workflow, the policies that the files violate, the name of the action , the retention category being applied to the file, and the response from the Enterprise Vault™ server.
   - The custodian(s) for whose action the workflow is submitted.
   - The status for each path can be one of the following:

Status	Description
Pending	Indicates that the custodian has not taken any action on the assigned paths.
Executing Action	In case of a Records Classification workflow, this status indicates that a file is marked as record by the custodian, and the archive request is being processed by Enterprise Vault™.

Status	Description
Success	Indicates that the custodian has submitted an action and the action has been registered with the Data Insight Management Server. In case of a DLP Incident Remediation workflow, it means that Data Insight has sent the response rule request for execution to the DLP Response Rule Execution Service. In case of a Records Classification workflow, if a file is marked as record by the custodian, and if automatic action is configured, Data Insight submits the response for action to Enterprise Vault. Once Enterprise Vault archives the file and applies the post-processing actions on the file, Data Insight displays the response from Enterprise Vault on the Management Console. In this case, **Success** indicates that the archive request is completed by Enterprise Vault™. Whereas, if a file is marked as No record, or if automatic action is not enabled, **Success** indicates that the custodian has submitted the response from the Portal. In this case, Data Insight simply logs the response submitted by the custodian on the Self-Service portal.
Failed	Indicates that the action submitted by the portal user on the Self-Service Portal is not registered with the Data Insight Management Server for any reason.
Expired	- Indicates that the due date for completing the workflow has expired, and the portal users will not be able to take any action on the paths in that particular workflow,

- Depending on the type of workflow, you can also view the following information about the paths assigned for remediation:

Workflow	Details
Entitlement Review	Click the path to see the details of the user permissions on that path. For each user with permissions on the path, you can view the following information: ■ The user name ■ The login ID of the user ■ The type of permission the user has on the path. For example, read, write etc. ■ Activity status of the user, whether Active or Inactive. ■ Whether the user is allowed access on the path or not. ■ Whether the user is the creator/owner of the folder on the file system. The creator owner on a path by default has Full permissions on the path.
DLP Incident Remediation	The actions are based on configured DLP Smart Response rules, for example, Quarantine, Mark for Deletion, or Archive. For information about Smart Response rules, see the *Symantec Data Loss Prevention Administration Guide*. A possible action can also be *Delegate* if the custodian delegates the incident remediation for certain paths to another user.
Ownership Confirmation	The possible actions for any path can be *Confirm* or *Decline* ownership.
Record Classification	The possible actions for any file can be *Archive* or *Do not archive*

Remediating workflow paths

You can initiate the following remediation actions on workflow paths from the **Workflows** > **Audit** page:

- **Archive**: You can archive the paths that are part of a **Records Classification** workflow.
  See "Archiving workflow paths using Enterprise Vault" on page 225.
- **Remove permissions**: You can remove permissions for **Entitlement Review** workflow paths.
  See "Removing permissions for Entitlement Review workflow paths" on page 240.

You can view the status of remediation actions on the **Settings** > **Action Status** tab of the Management Console.

Chapter 10

Using the Self-Service Portal

This chapter includes the following topics:

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

About the Self-Service Portal

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

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

Data Insight integrates with Data Loss Prevention (DLP) to help security administrators and the information security teams in your organization to monitor and report on access to sensitive information. A Data Insight lookup plug-in retrieves information from the DLP Enforce Server about confidential information on the shares being monitored by Data Insight. DLP creates an incident for every file that violates configured DLP policies. The DLP Network Discover incident report lists

such file system shares. The usage information that Data Insight collects automatically feeds into the incident detail of files that violate DLP policies. Data Insight identifies the data owners to notify about these incidents. This method enables users to identify sensitive data along with the responsible users to enable more efficient remediation and data management.

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

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

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

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

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

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

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

About Entitlement Review

The Data Insight Administrator, can configure and initiate an entitlement review workflow from the Management Console. Once the Entitlement Review workflow

is triggered, Data Insight will send an email to the data custodian to review the permissions.

Entitlement Review workflow helps a data custodian to review the access permissions on the resources the custodian owns. It also provides insight into whether a user is the creator owner on a path with Full control permissions. The custodian can make recommendations to deny or allow access to a user or group on a path.

The custodian can recommend remediation actions, in the following cases:

- If the user or group is inactive on the path for the selected time period .
- If the custodian wants to restrict access to a user who does not have any business reason to have access on a path.

The custodian must submit the recommendations from the Self-Service Portal. Based on the custodian's recommendations, the Data Insight administrator can take the following actions:

- Revoke the user's explicit permissions on the path.
- Remove the user from the group of which she is the direct member.
- In case of user with creator owner on a path, remove the user as the current owner in the Windows' Advanced Security settings.

However, Data Insight does not provide recommendations to modify well-known groups such as Everyone or Administrators.

Logging in to the Self-Service Portal

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

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

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

To log in to the Self-Service Portal

1. Click the link contained in the email alert.

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

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

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

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

Using the Self-Service Portal to review user entitlements

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

- View a snapshot of the users whose permissions are assigned for your review.
- Review if the user has the creator owner permissions on a path.
  If the option to display the creator owner is selected in the workflow template, the **Creator Owner** column is displayed on the Portal UI with value as 'Yes' against user who is creator owner.
  Note that if the Creator Owner is a group, no value is displayed in the **Creator Owner** column.
- 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.
- Make recommendation to grant or revoke user permissions on the specified paths.
- Decline the review request or delegate the review work to another user.

To review user entitlements

1. Use the **Resources** 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.

   You can further filter the users by selecting the group they belong to or by using their directory service attribute.
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 to 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 *Veritas Data Insight Administrator's Guide*.

See “Logging in to the Self-Service Portal” on page 213.

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

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

- View a snapshot of the number of files that are assigned for your attention. The files are sorted according to the severity of incidents that are associated with them.
- Filter the list of files based on the severity of the incidents that the files have violated, the recency of the last access date, or the DLP policy that the files violate. The filters available to you depend on the options that are selected when configuring the workflow template.

  The different filters are applied together, and the list is filtered to show the data that matches the applied criteria.
- Perform a configured action on multiple files at one time. The available actions are DLP Smart Response rules configured in DLP. You can select more than one file from the list and then choose the desired action.

To remediate the files

1. Select the files that you want to remediate.

   You can choose to filter the list of files using the filter criteria at the top of the page. For example, you can prioritize the remediation of files that are associated with high severity incidents that violate a particular policy. Files that match the selected filter criteria are listed. Select the desired files from the list.
2. From the **Select Action** drop-down, select the action that you want to take on the selected files. For example, you may quarantine the files or mark the files for deletion. The listed actions are the Smart Response rules that are configured within DLP.

   For more information about Smart Response rules, see the *Symantec Data Loss Prevention Administration Guide*.
3. Click **Submit** to send the remediation request to the Data Insight Management Server for further action.

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

Using the Self-Service Portal to confirm ownership of resources

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

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

To confirm ownership

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

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

See "Logging in to the Self-Service Portal" on page 213.

Using the Self-Service Portal to classify sensitive data

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

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

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

To classify the files

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

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

Chapter 11

Managing data

This chapter includes the following topics:

- About managing data using Enterprise Vault and custom scripts
- Managing data from the Shares list view
- Managing inactive data from the Folder Activity tab
- Managing inactive data by using a report
- Archiving workflow paths using Enterprise Vault
- Using custom scripts to manage data
- Pushing classification tags while archiving files into Enterprise Vault
- About adding tags to files, folders, and shares

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 223.
- The files that appear inside the following types reports:
  - **Activity Details** reports
  - **Activity Summary** reports
  - **DQL** reports
  - **Data Lifecycle** reports

See "Managing inactive data by using a report" on page 224.

- Paths that are part of a Records Classification workflow.
  See "Archiving workflow paths using Enterprise Vault" on page 225.

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 *Veritas 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 220.
- 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 221.

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 *Veritas Enterprise Vault Administrator's Guide*.

See "About managing data using Enterprise Vault and custom scripts " on page 219.

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 219.

Managing data from the Shares list view

You can perform any data management actions, such as archive or classify files from the **Workspace** > **Shares** list view of the Data Insight Management Console.

To manage data from the Shares list view

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

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

- **Classify** - Click to submit files for classification using Veritas Information Classifier.

  For detailed information about setting up classification and classifying files, see the *Veritas Data Insight Classification Guide*.

  For information on setting up classification policies, see the *Veritas Information Classifier Online Help*.

- **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 *Veritas 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.

  You can push classification tags while archiving files into Enterprise Vault to enable faster search while searching from Enterprise Vault. Select the **Add Custom Index Property** check box . You can select a **Property type** from the drop-down box like Text, Integer or Date. Depending on what you select, text boxes corresponding to Set, Name and Value appear. You must specify the name of the property set, the name of the property and the value of the property which will constitute the classification tag that will be pushed while archiving files into Enterprise Vault.

  For more information, refer to the *Data Insight Administrator's Guide*.

6 Click **Archive**.

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

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

Managing inactive data from the Folder Activity tab

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

To manage inactive subfolders

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

   - **Custom Index Property -** You can push classification tags while archiving files into Enterprise Vault to enable faster search while searching from Enterprise Vault. Select the check box **Add Custom Index Property**. You can select a **Property type** from the drop-down box like Text, Integer or Date. Depending on what you select, text boxes corresponding to Set, Name and Value appear. You must specify the name of the property set, the name of the property and the value of the property which will constitute the classification tag that will be pushed while archiving files into Enterprise

Vault. For more information on adding classification tags while archiving files into Enterprise Vault, refer to the *Data Insight Administrator's Guide*.

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

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

Click **Archive**.

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

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

Managing inactive data by using a report

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

- Activity Details reports
- Activity 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 *Activity 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 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 *Veritas 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.

Archiving workflow paths using Enterprise Vault

The **Workflows** > **Audit** view enables you to explicitly archive workflow paths to help you reclaim paths, comply with your organization's data retention policies, and to make the content available for e-discovery. You can only archive Records Classification workflow paths.

Note: To archive Records Classification paths, ensure that Enterprise Vault is configured in Data Insight.

For more information about configuring archive options in Enterprise Vault, see the see the *Veritas Data Insight Administration Guide*.

To be able to successfully send the archiving request, the following conditions regarding the Records Classification workflow path or paths must be fulfilled:

- You can archive only those paths whose **Status** is either **Failed** or **Success**.
- You cannot archive those paths for which the post- processing action is not specified. Also, all selected workflow paths must have the same post-processing action.

- All the selected workflow paths must have the same retention category.
- You can archive only those workflow paths for which the custodian has taken an action as **Record**.

To archive the paths, select the workflow path in **Workflows** > **Audit**, and click **Archive** located on top of the list view.

Once the archive request is created, you can monitor the request in from **Settings** > **Action Status.** page by filtering on the keyword *Workflow Audit*.

Using custom scripts to manage data

Data Insight enables you to archive inactive data on your storage devices using Enterprise Vault. However, if you use other archiving tools, or if you want to take actions such as copy your data to a cheaper storage, or delete orphan or inactive data, you can write custom scripts to manage the data.

You can initiate up to two custom actions directly from the Data Insight Management Console. You can apply the scripts to run on the following data:

- The files that are listed under **Workspace** > **Folder Activity** > **Inactive Subfolders** tab.
- The files that are listed in the following types of reports:
  - Activity Details reports
  - Activity Summary reports
  - DQL reports
  - Data Lifecycle reports
- The paths displayed in the **Workspace** > **Data** and the **Workspace** > **Shares** views.

Before you can configure Data Insight to run the custom action scripts, do the following:

- Define the action that you want to perform on the data. For example, you may choose to upload all inactive data on your storage devices to the cloud.
- Write a script to perform this action.
  For more information, see the *Veritas Data Insight Programmer's Reference Guide*.
- Place the script at a specified location on the Management Server. By default, all custom scripts must be placed at `$datadir\conf\workflow\steps\CUSTOMACTION\scripts`. Data Insight invokes

the scripts form this location when you initiate an action from the Management Console.

To configure a custom action script

1. In the Management Console, click **Settings** > **Data Management**. The Archiving (Enterprise Vault Configuration) page displays by default.
2. Click **Custom Action 1** or **Custom Action 2**.
3. On the **Custom Action** page, enter the following details:
   - The name of the custom action.
   - The name of the script, for example, `copy.pl`.
   - The credentials of the user to run the script. You can either use Local System account credentials or the credentials of a user with privileges to perform the desired action on the data. The script continues to run with Local System account, however the specified credentials are used for any network calls made by the script.
4. Select **Do not expand paths** to apply the action defined in the script to the paths selected in the view or the report. The selected paths are passed as-is to the custom script.
5. Select **Expand paths** to apply the action defined in the script to all child folders under the selected folder recursively. If you select this option to invoke an action on the folder, Data Insight passes individual files present in that path's hierarchy to the script, instead of the parent folder.
6. Select the additional data that you want to pass to the script.
7. Click **OK** to save the settings.

Pushing classification tags while archiving files into Enterprise Vault

You can add classification tags to a file that you want to archive using Enterprise Vault. When the file is archived and indexed in Enterprise Vault, the classification tag is included in the index of the file. When you search the archive, the search is carried out on the tags that are attached to the file rather than the entire Enterprise Vault database. You can also use the classification tags to reassign retention categories that determine how long archived items are stored in Enterprise Vault. You can add any number of classification tags.

A user with the Server Administrator or a Report Administrator role can add classification tags to files being archived.

To push classification tags

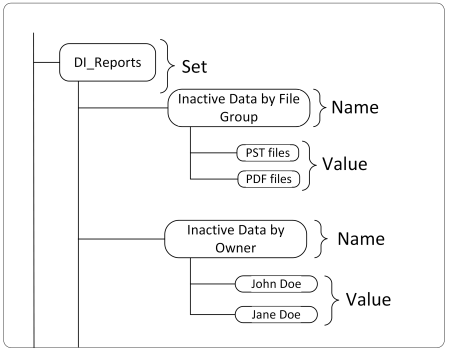
1. Click the **Reports** tab and select the report type that allows data remediation using Enterprise Vault, for example Inactive Data by File Group or DQL report.
2. Click **Create Report**.
3. On the **Create Report** wizard, enter the report input parameters and navigate to the **Remediation** tab.
4. Select the **Take action on data generated by report** check box.
5. Select the **Archiving (Enterprise Vault)** radio button.
6. Select the **Add Custom Index Property** check box.
7. Select a value from the **Property type** drop-down box. The different property types include Text, Integer, Date, and Classification property.

   Note: Classification property is only available for DQL reports.

8. Depending on what you select, three text boxes corresponding to **Set**, **Name** and **Value** appear. Enter the tag in the following format:

Field	Description
Set	Name of the property-set to which the property is added. **Note:** This name can be an already existing property set name or a new one. If it does not already exist, a new property set is created when you make an entry here.
Name	Name of the property. A property set can have a number of unique names.
Value	Value of `Set.Name`. The value can be Text, Integer, or Date type depending on the property type selected. **Note:** This field is not available when the **Property type** is set to Classification property because Data Insight applies the classification tags fetched from Veritas Information Classifier as the value of the property type.

Figure 11-1 An example of Set, Name, and Value



Note: If classification tags are selected, all classification tags applicable to the file being archived are added to the archive request. The tags are in a semi-colon separated list.

See "About managing data using Enterprise Vault and custom scripts " on page 219.

You can review the classification tags applied to the files archived in Enterprise Vault from:

- On the Data Insight Management Console, navigate to **Setting** > **Action Status** page.
- On the Enterprise Vault Console.

About adding tags to files, folders, and shares

Data Insight lets you add text-based properties (key, value pair) to file system objects such as files, folders, and shares on the file systems that it monitors. Tagging files, folders, and shares with attributes provides additional classification information that you can use for reporting and remediation.

For example, you may want to tag folders with the business name, or assign descriptors to folders that have special permission. Or, for instance, you can tag shares with department names for the purpose of chargeback.

Data Insight supports the metadata framework on CIFS, NFS, and DFS paths, and on files and folders on SharePoint servers and Enterprise Box accounts.

Use a CSV file to add metadata tags to files, folders, and shares. Data Insight parses the CSV and imports these tags into Data Insight. You may either create

the CSV file manually or use a third-party tool or script to generate the CSV with tagging information for paths.

You can generate a Data Insight Query Language (DQL) report to get the information about the tags attached to file system objects, such as, share names and paths. For example of DQL queries, see the *Veritas Data Insight Programmer's Reference Guide*.

Using the metadata framework for classification and remediation

To apply tags to files, folders, and shares, you must create a CSV file with the metadata key value pairs. You may either create the CSV file manually or use a third-party tool or script to generate the CSV with tagging information for paths.

To apply metadata tags

1. Create a CSV file with the tagging information. You can create more than one CSV file with tagging information for paths.

   To assign tags to the files, ensure that the CSV file name starts with `File_` (for example, `File_tags.csv`). Enter paths for different files with the tag name and tag values. CSV files with any other name are considered to have paths of folders.

   Note: i18n and special characters are not supported in tag names.

2. Save the CSV files in the `data/console/tags` folder in the Data Insight installation directory on the Management Server.

3 A scheduled job *TagsConsumerJob* parses the CSV file and creates a `Tags` database for each share. The job imports the tags for the paths into Data Insight. The job runs once in a day by default.

If the job is executed manually using the `configcli` command, the job forcefully consumes all the CSV files under `Tags` folder.

Whenever the job runs, it checks if the modified time of any of the CSV files under the `Tags` folder is greater than the time of the previous execution of job. If the job finds any such CSV, it processes all the CSV files under `Tags` folder. If the CSV file(s) have not been modified after the job was last executed, the job does not take any action.

The job does not accept any tag name that starts with *mx_* because they are reserved for Data Insight internal tags usage. Whenever the job processes the CSV, Data Insight deletes all existing tags (except tags starting with "mx_") from all files and folders and attaches new tags.

Note: If a path is tagged in two different CSV files with the same tag name, but with a different value, then the value in the last CSV file that is processed is applied.

---

4 To replace existing tags, update the CSV with new tags. The scheduled job replaces existing tags with the new tags. If any paths are discarded during the last run of the job, then these are logged in `$DATADIR/console/generictags_scan_status_5.0.db`.

If any paths are discarded, then these are logged in a database that stores the discarded paths during the last run of the job.

To remove all tags, delete the CSV from the `Tags` folder.

5 Create a DQL report to retrieve the tags from the database.

Here are a few example queries that you can use:

- To fetch all paths in your storage environment along with the tags (my_tag) assigned to them.

```
FROM path GET name, TAG my_tag
```

- To get all paths owned by user Joe Camel tagged with the needs_assesment tag.

```
FROM owner GET TAG owner.path.needs_assessment, owner.path.name
IF user.name="joe_camel"
```

Note: The DQL report output does not return any tag if the content does not match any predefined classification tag.

6 To verify the names of tags that are stored for a share, run the `idxreader` command on the indexer node.

```
idxreader –i $MATRIX_DATA_DIR/indexer/default/99/99
–gettags all
```

Format of CSV file

The CSV file with the metadata tags should be in the following format:

```
File/folder path, tag name, tag value
```

For example, `\\filer\share\foo,tname,tvalue`

Where, **tname** refers to the name of the tag, and **tvalue** refers to the tag value.

Note: Multiple values for a same for the same tag are not supported.

If the path or the tag name contains a comma, enclose the text in double quotes (“,”). For example, if the folder name is foo, bar, you can add the path in the CSV as follows:

```
"\\filer\share\foo,bar",t_name,t_value
```

For shares, the path should be present in the CSV file containing folder paths. Following are examples of share level paths:

CIFS/DFS	\\filer\share
SharePoint	URL of the site collection
NFS	<export path> For example, /data/finance/docs
Box	\\Box\<box name in Data Insight>

Chapter 12

Managing permissions

This chapter includes the following topics:

- About permission visibility
- About recommending permission changes
- About recommending permissions changes for inactive users
- Making permission changes directly from Workspace
- Removing permissions for Entitlement Review workflow paths

About permission visibility

Data Insight provides multiple ways to monitor the permissions on the data resources in your storage environment. It helps you ensure that the right people have the right level of access to the company's information. You can review the permissions on data resources in the following ways:

- Leverage the activity data that is provided by the audit logs and the information about permissions on a path to understand where permissions can be removed. Data Insight uses the audit log data to provides recommendations for revoking permissions of users and user groups who do not have activity on certain paths. Data Insight also lets you simulate the permission changes without affecting the production environment.
- Use Entitlement Review workflow to conduct security investigations and identify excessive permissions in your storage environment.
  See “About remediation workflows” on page 170.
- Use predefined rules or create custom rules to search for permissions in your organization that helps you control access to resources.

You can create reports to search for permissions that match the rules that are defined in a permission query template. The Permissions Search report lets you proactively search for permissions to specific groups or users on a data resource. For more information, see the *Veritas Data Insight User's Guide*.

Visibility into permissions in your storage environment helps you do the following:

- Detect the permission assignments that do not adhere to your management's policies. This helps you identify all compliance violations in your environment to ensure permission hygiene.
- Review folders, groups, and user permissions on file systems, SharePoint, and cloud storage platforms.
- Remediate permissions to control access to critical data and prevent data breaches.
- Ensure that your organisation adheres to permissions best practices.

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. Data Insight enables you to manage permissions on file servers and SharePoint sites to ensure security and compliance with best practices and company policies.

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.

Note: The permission remediation action from the **Workspace** tab can only be taken by a user with the Server Administrator role. The options to remove users or groups or to revoke permissions using reports are only visible to users with the Server Administrator role and Report Administrators who are allowed to remediate data and permissions.

You can orchestrate permission changes in the following ways:

- Recommend that the permissions of inactive users on shares and folders be revoked.

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

  See “About recommending permissions changes for inactive users” on page 235.
  See “Reviewing permission recommendations ” on page 236.

See "Analyzing permission recommendations and applying changes" on page 236.

- Use the Permissions Search report to remediate permissions.
  For more information about the Permissions Search report, see the *Veritas Data Insight User's Guide*.
- Remove direct member users or groups from a group on the **Overview** tab of the **Workspace**.
  Revoke permissions of specific trustees directly from the **Permissions** tab of the **Workspace**.
  See "Making permission changes directly from Workspace" on page 238.
- Remove permissions from the **Workflows** > **Audit** page on paths that are part of an Entitlement Review workflow.
  See "Removing permissions for Entitlement Review workflow paths" on page 240.

You can configure the settings required to implement the permissions recommendations.

Note: Data Insight does not fetch permissions for the Microsoft OneDrive, SharePoint Online, and Documentum data sources. Hence, you cannot configure permission recommendations for these data sources.

About recommending permissions changes for inactive users

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.

See “Reviewing permission recommendations ” on page 236.

See “Analyzing permission recommendations and applying changes” on page 236.

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** > **Shares**.
2. On the **Shares** list view, drill down to the path for which you want to view the permission recommendation.
3. Click the profile arrow. The Summary panel expands to display the profile view..
4. Click **Permissions** > **Recommendations**. Review the suggested changes.
5. Click **Analyze Group Changes** to trigger a Group Change Impact Analysis report.

   See “Analyzing permission recommendations and applying changes” on page 236.
6. Click the Export icon at the top-right corner of the recommendations panel to save the data to a `.csv` file.

Note: The users with Server Administrator role can take further action on the recommendations after analyzing them.

See “Making permission changes directly from Workspace” on page 238.

Analyzing permission recommendations and applying changes

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

Users with the Server Administrator and the Report 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 Impact Analysis report on the **Reports** tab to analyze the effects of permission changes outside the scope of the recommendations that are made by Data Insight.

For information about Group Change Impact Analysis report, see the *Veritas Data Insight User's Guide*.

To analyze and apply permission recommendations

1. In the Management Console, click **Workspace** > **Shares**.
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)** option is enabled.
5. Click **Analyze Group Change(s)** to run a Group Change Impact 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** icon corresponding to the recommendation.
6. Once the report run is complete, review the Group Change Impact 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.

Making permission changes directly from Workspace

You can make permission changes from the user-centric views of the **Workspace** tab. You can do the following:

- Remove a user from a group of which the user is a direct member.
- Remove a direct member group from a group.
- Revoke the permissions of a trustee who has explicit permissions on a path. If the trustee inherits permissions on a path, then the option to revoke the trustee's permission is not available.

Note: Data Insight allows only the user with the Server Administrator role to take permission remediation action from the **Workspace** tab. The options to remove users or groups or to revoke permissions is not visible to users other than the Server Administrator.

Removing a user from a group

To remove a user from a group

1. Navigate to the **Overview** tab for the user.

   The **Overview** tab for a user displays a list of all groups of which the user is a direct member.

2. Click the **Delete** icon to remove the user from a particular group. Proceed to 4.

3. Or, on the **Overview** tab for a group, do the following:

   - Select the users that you want to remove from the group.
   - The **Remove Members from Group** pop-up, displays the direct members of the groups who can be removed. It also indicates the members that cannot be removed because they are indirect members of the group.

4. On the pop-up, click **Analyze Changes** to trigger a **Group Change Analysis** report.

   This report helps you review the effects of the membership change on the user's access to other paths that the user may have permissions on.

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

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

6 Click **Submit Changes** to start the process of raising a request to implement the changes.

Removing a group from another group

To remove a group from another group

1 Navigate to the **Overview** tab of a group.

The **Overview** tab for a group displays a list of all groups of which the selected group is a direct member and the groups to which the selected group has inherited membership. Additionally, all direct and indirect members of the selected group are also displayed.

2 Click the **Delete** icon to remove the group from a particular group.

You can also select the user members or the group members that you want to remove from the selected group. Data Insight removes only the direct member groups or direct member users of that group.

3 On the pop-up, click **Analyze Changes** to trigger a Group Change Impact Analysis report.

This report helps you review the effects of the membership change on the groups's access to other paths that the group may have permissions on.

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

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

5 Click **Submit Changes** to start the process of raising a request to implement the changes.

Revoking a user's or group's permissions

You can revoke a user's or group's permissions on a path directly from the **Permissions** tab when the user or group has explicit permissions on the path.

To revoke a user's or groups permissions

1 Navigate to the **Permissions** tab of a share or folder on which you want to revoke a user's or group's permissions.

2 Click the **File System Access Control List** or the **Share-level permissions** sub-tab.

3 The users and groups that have explicit permissions on that path are listed. Click the **Delete** icon under the **Remove Permissions** column to revoke the permission.

4 Click **Yes** on the confirmation pop-up to effect the permission change.

Removing permissions for Entitlement Review workflow paths

You can remove permissions on paths that are part of an Entitlement Review workflow from the **Workflows Audit** list page.

To be able to successfully remove permissions, the following conditions regarding the Entitlement Review workflow path or paths must be fulfilled:

- You can remove permissions of only those paths whose **Status** is either **Failed** or **Success**.
- The **Custodian Action** for the workflow path should be **Revoke**.

Ensure that the settings required to implement the permission recommendations are configured before you initiate the action to remove permissions. Once all the conditions are fulfilled, the configured permission remediation action is initiated.

For information about configuring permission remediation settings, see the *Veritas Data Insight Administration Guide*.

To remove permissions

1 Navigate to **Workflows** > **Audit**.

2 Select the Entitlement Review workflow paths.

3 Click **Remove Permissions**.

4 You can monitor the request from **Settings** > **Action Status** page.

Note: Creating workflows for the SharePoint Online, Microsoft OneDrive, and Documentum data sources is not supported.

Appendix A

Command Line Reference

This appendix includes the following topics:

- mxcustodian

mxcustodian

`mxcustodian` – A script that is used to automatically assign custodians on various paths and to generate a comma separated values (csv) file with information about data custodian assignments. The `.csv` files, `mxcustodian_assign.csv` and `mxcustodian_error.csv` are saved in the current directory.

SYNOPSIS

```
mxcustodian.exe --paths <pathsfile> --ownermethod <comma-separated-list>
|default

mxcustodian.exe --paths <pathsfile> --groupscript <script>
--attr <attrname>

mxcustodian.exe --csv <csv-filepath> --verify
 [--custodian <user@domain>|<SID>]

mxcustodian.exe --csv <csv-filepath> --assign [-f] [--overwrite]

mxcustodian.exe --csv <csv-filepath> custodian
<user@domain>|<SID> --assign [-f] [--overwrite]
```

OPTIONS

- –csv<*name of input file*>

  A file with comma-separated values — path, custodian. The values are provided in the format, one path per line. The given custodians are assigned to their corresponding path.

- –assign

  Assigns custodians given in the input csv file.

- –custodian <*name of custodian*>

  A user@domain or SID value to be assigned as custodian to all input paths. Input paths must be specified using – –csv option where the file provided contains one path per line.

- –paths <*input file*>

  Input file with paths, one path per line. Depending on the method used, the computed custodians for the paths will be printed to the output file, `assignments.txt`.

`– –overwrite`

Overwrites existing custodian assignments with the assignments provided in the input csv file (using – –csv option). By default, Data Insight appends the custodian assignments in the input file to the existing assignments.

`–g – –groupscript`

Invokes the script for each path <*name of path*> in the input file given by the --csv option. The script is passed one path per invocation and prints to its standard output a group, <*name of group*>, corresponding to that path. If the script exits with 0, denoting success, the output group is used. If the script exits with a non-zero value, the path is discarded. The next input path is picked up if `--force` option is used; else this script aborts further execution

---

Note: When using the "--groupscript" option, you must keep the actual script in the folder `data/scripts/mxcustodian/`. When specifying the parameter for the --groupscript option on the command line, you must specify the fully-qualified path to the script.

Once a group for a path is obtained, the script does the following in the given order:

- Queries the directory service to get the value for the attribute for the group. The attribute can be specified using the `--attr` option.
- Generates a file containing the path and attribute entries, one entry per line.

`–f – –force`

Ignores paths that do not have a corresponding custodian specified in the input csv file, and assigns custodians for other valid paths. This option also prints all error paths in the log file.

`–a – –attr <name of attribute>`

Attribute whose value specifies the custodian for a given path. Use this option with the – –groupscript option.

`– –ownermethod default|<one or more comma-separated list of methods>`

The supported methods of computing an owner in their default order (if a default order is specified) are rw_count, read_count, write_count, creator, last_accessor, last_modifier OR 'parent_owner,<*M*>' where M is the default or any number of comma-separated methods.

– –ownermethods are calculated based on the last 3 months data/time range.

`– –verify`

Verifies and validates input paths and custodians provided using – –csv option. This command does not make any custodian assignments.

`– –outfile<`*`name of the file`*`>`

Name of the file where the results of successful custodian computation, verification, or assignments is stored. If the file name is not specified, the results go to the standard output of the command.

`– –errfile` *`name of the file`*

Name of the file where the errors in custodian computation, verification, or assignments is stored. If the file name is not specified, the results go to the standard error output of the command.

`–f – –ignore_errors`

Ignores paths that do not have a custodian in the input csv file and assigns the custodians for other valid paths. Prints all such error paths in the log file.

`–D – –debug`

Prints additional debug statements in the log file.

`–h – –help`

Prints the usage information for this command.

Index

A

access pattern map 66
accessibility
    Management Console 21
    tabs 22
    tools 22
Archiving
    using Enterprise Vault 219
    workflow data 225
archiving
    by using reports 224
    inactive subfolders 223
    post-processing actions 221
    retention categories 220
audit logs
    overview 18

C

considerations
    importing path 154
    uploading CSV file 154

D

data custodian
    overview 13

F

folders
    assigning active user as custodian 60
    assigning custodian 60

M

Management Console
    logging in 24
    logging out 24
    operation icons 23

O

overview
    access information for users and groups 37
    managing data custodian 55
    migrated domains 19
    viewing access information for folders 36, 54

P

permissions
    assigning custodian 61
    overview 14

R

Remediating
    workflow paths 209
Removing permissions
    Entitlement Review workflow paths 240
report
    truncate 163
reports
    cancelling generation 166
    considerations 167
    copying 160
    creating 88
        DQL report dialog options 149
        permission search
        See also permissions query template
        security report dialog options 109
        storage report dialog options 131
    customizing column names 162
    deleting 166
    editing 159
    filtering 158
    generating 160
    managing 156
    overview 85
    send by email 164
    storage 122
    type
        custom 140

reports *(continued)*
type *(continued)*
ransomware 140
security 89
storage 120
viewing 156

S

saving
CSV file 85
HTML file 85
PDF file 85
security
Activity Details 89
Activity Summary 121
ownership reports 107
Permissions 90
sharepoint permissions
overview 15

T

tags
archiving 227

V

Veritas Data Insight
overview 10
viewing
attributes of a group 73
attributes of a user 72
attributes of file or folder 54
folder activity log 66
report execution log 160
reports 156
user access details 81
user activity on folders 75
viewing folder activity
by time 62
for inactive subfolders 62
for subfolders and files 62
viewing permissions
effective permissions 63
File System Access Control List 63
for groups 78
for users 76
share-level permissions 63
viewing user activity
active users 58
inactive users 58
overview 58