One Identity Data Governance Edition 8.2

User Guide

Contents

Introduction

This guide contains the information required to administer One Identity Manager Data Governance Edition to manage the unstructured data in your organization. It contains detailed information about the Data Governance Edition features and includes instructions to help administrators perform day-to-day administration activities.

Before you can gather information on the unstructured data in your organization, you must:

- Identify the domains that you want to access and provide the credentials that can perform operations on those resources. For more information, see Adding and editing a service account on page 61.

- Select the domains that contain the computers and data that you want to manage and assign the Service Account. For more information, see Adding a managed domain on page 62.

- Add the hosts that hold the resources that you want to manage. For more information, see Adding and configuring managed hosts on page 65.

This initial setup information is also covered in the *One Identity Manager Data Governance Edition Deployment Guide* and should already be completed.

Once you have added a managed host, you can:

- Examine a file system, SharePoint farm or other supported platforms to see what users and groups have access to it, and modify the access if required. For more information, see Browsing your environment on page 124.

- Examine a user or group to ensure they have the correct data access. For more information, see Managing account access on page 127.

- Compare account access for selected users or groups. For more information, see Comparing accounts on page 143.

- Simulate the addition or removal of users or groups from selected groups. For more information, see Simulating the effects of group membership modifications on an account on page 147.

- Calculate perceived ownership to identify potential business owners for data within your environment. For more information, see Calculating perceived owner on page 163.

- Place data under governance and leverage the self-service request attestations, policies, and reports that help you to ensure your data is in compliance. For more information, see Placing a resource under governance on page 151.

Available documentation

Data Governance Edition documentation includes the following manuals:

- *One Identity Manager Data Governance Edition User Guide*

  This guide includes Data Governance Edition administration information.

- *One Identity Manager Data Governance Edition Deployment Guide*

  This guide includes Data Governance Edition installation, configuration, and deployment information.

- *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide*

  This guide includes details about the self-service resource requests related to resources that are governed, including the file system share creation request in the IT Shop.

- *One Identity Manager Data Governance Edition Technical Insight Guide*

  This guide is intended for advanced audiences who want a deeper understanding of the Data Governance Edition components and how they communicate with each other. It also provides a description of the configuration file settings, registry key settings and PowerShell commands.

Online versions of the Data Governance Edition guides are available on the technical support web portal: https://support.oneidentity.com/identity-manager-data-governance-edition/technical-documents

For supporting One Identity Manager information, see the One Identity Manager documentation. Online versions of the One Identity Manager guides are available on the technical support web portal: https://support.oneidentity.com/identity-manager/technical-documents

Data Governance node and views

The Data Governance Edition elements are embedded into the Manager client application. The user interface elements communicate with the Data Governance service and directly with the One Identity Manager database. Communication with the database is performed in the same way as any other One Identity Manager database communication, using the authentication information provided when the user launches the client tools.

The Manager is the main administration tool for configuring Data Governance Edition components and governing unstructured data to secure and control access to your organization's data. The **Data Governance** node in the Manager's navigation view provides access to the data required to perform the following tasks:

- Configure Data Governance Edition, including:
  - Configuring Data Governance service accounts for managed domains
  - Adding and configuring managed hosts
  - Deploying Data Governance agents
- Manage resource access
- Manage account access
- Manage and set security permissions for network objects
- Manage and set SharePoint security permission levels
- Bring data under governance
- Define classification levels for use in classifying governed data

From the Data Governance navigation view, the following main views become available to configure and manage your Data Governance Edition deployment:

- Info system view
- Service accounts view
- Managed domains view
- Managed hosts view
- Agents view
- Security index view
- Governed data view

- Classification view
- Background operations view

In addition to these main views, the following Data Governance Edition views are available to manage resource access, account access and governed data:

- Resource browser
- Manage access view
- Accounts view

Info system view

Selecting **Info system** in the Data Governance navigation view displays dashboards for viewing general statistics and the overall status of your Data Governance Edition deployment in real-time.

NOTE: In addition, you can view these dashboards using the Data Governance server landing page (https://*<DGEServerIPAddress>*:8723/server/home).

NOTE: The Data Governance Edition statistics displayed in these dashboards are calculated on an hourly schedule. To change the schedule, edit the hourly schedule defined in the **QAM statistics** schedule in the Designer (**Getting Started** | **Edit schedules** or **Base Data** | **General** | **Schedules**).

The **Info system** view in the Manager includes three One Identity Manager statistics (as indicated in the table) and these are calculated based on the schedule defined in the **Calculate statistics** schedule. The **Calculate statistics** schedule is disabled by default and must be enabled in order to calculate these One Identity Manager statistics. These statistics are not available on the Data Governance server landing page.

Table 1: Data Governance Edition statistics

Statistic / Metric	Description
Managed Hosts	Pie chart shows the number of computer objects found in your environment, indicating the number that are managed hosts and the number that are not yet managed (unmanaged).
	NOTE: This statistic does not include SharePoint Farm, DFS Root or NFS managed hosts.
Managed Host Status	Pie chart shows the number of managed hosts by status (OK vs. Not OK).
	NOTE: This statistic does not include SharePoint Farm, DFS Root or NFS managed hosts.

Statistic / Metric	Description
Managed Host Type	Pie chart shows the number of managed hosts defined in your Data Governance Edition deployment, broken down by host type.
Managed Hosts with Resource Activity	Pie chart shows the number of managed hosts that are collecting resource activity (Enabled) and the number of managed hosts that are not collecting resource activity (Disabled). NOTE: Since resources on Cloud managed hosts cannot collect resource activity, those resources are always included as **Disabled**.
Managed Hosts Without Governed Data	Graphic shows managed hosts that have resources that have not been placed under governance. The graphic uses the following thresholds: • Green: Less than 25% of all managed hosts have data that is not being governed. • Orange: Between 25% and 75% of all managed hosts have data that is not being governed. • Red: More than 75% of all managed hosts have data that is not being governed. The total number of managed hosts with ungoverned data is displayed under the graphic. NOTE: On the Data Governance server landing page, this is a pie chart showing managed hosts with data that has not been placed under governance.
Governed Data Without Business Owners	Graphic shows governed data without an assigned business owner. The graphic uses the following thresholds: • Green: Less than 25% of all governed data does not have a business owner assigned. • Orange: Between 25% and 75% of all governed data does not have a business owner assigned. • Red: More than 75% of all governed data does not have a business owner assigned. The total number of governed data without an assigned business owner is displayed under the graphic.

Statistic / Metric	Description
	NOTE: On the Data Governance server landing page, this is a pie chart showing governed data without an assigned business owner.
Governed Data by Resource Type	Pie chart shows the number of governed resources, broken down by resource type.
Published vs Unpublished Governed Data	Pie chart shows the number of governed resources that are published to the IT Shop and the number of governed resources that are not published.
	NOTE: Since resources on NFS and Cloud managed hosts cannot be published to the IT Shop, those resources are always included as **Unpublished**.
Published Data with Organizational Restrictions	Pie chart shows the number of published resources belonging to a restriction list, broken down by organizational structure (department, location, or cost center).
Security Index by Account Type	Pie chart shows the number of accounts with direct access points that have been scanned by a Data Governance agent, broken down by account type: • Azure AD Group • Azure AD User • Domain Group • Domain User • Machine Local Group • Machine Local User • Other • SharePoint Group • SharePoint Identity • SharePoint Online Group • SharePoint User • Unix Group • Unix Owner
Attestations	Pie chart shows the number of attestations cases, broken down by Overdue, Outstanding, Closed overdue, and Closed in time cases.

Statistic / Metric	Description
	NOTE: This statistic does not include Cloud managed hosts.
	NOTE: This is a One Identity Manager statistic. In order to calculate and update this statistic, you must enable the **Calculate statistics** schedule in the Designer (**Getting Started** | **Edit schedules** or **Base Data** | **General** | **Schedules**). Once enabled, data for this graphic is updated based on the defined schedule.
Policy violations (current)	Graphic shows the number of current policy violations. The graphic uses the following thresholds: • Green: Zero violations • Red: One or more violations The total number of violations is displayed below the graphic.
	NOTE: This statistic does not include Cloud managed hosts.
	NOTE: This is a One Identity Manager statistic. In order to calculate and update this statistic, you must enable the **Calculate statistics** schedule in the Designer (**Getting Started** | **Edit schedules** or **Base Data** | **General** | **Schedules**). Once enabled, data for this graphic is updated based on the defined schedule.
Compliance Rule Violations (current)	Graphic shows the number of current compliance rule violations. The graphic uses the following thresholds: • Green: Zero violations • Red: One or more violations The total number of violations is displayed below the graphic.
	NOTE: This statistic does not include Cloud managed hosts.
	NOTE: This is a One Identity Manager statistic. In order to calculate and update this statistic, you must enable the **Calculate statistics** schedule in the Designer (**Getting Started** | **Edit schedules** or **Base Data** | **General** | **Schedules**). Once enabled, data for this graphic is updated based on the defined schedule.

Service accounts view

Selecting **Service accounts** in the Data Governance navigation view populates the **Service Accounts** result list with the service accounts registered with the Data Governance server. From the **Service Accounts** result list, you can add, edit or remove service accounts.

Double-clicking a service account in the **Service Accounts** result list displays the **Service account** overview which is a graphical representation of the information available, including the domains associated with the selected service account. From this view, you can also perform the following tasks against the selected service account.

Table 2: Service accounts view: Tasks

Task	Description	For more information
New	Click the **New** right-click command or toolbar button to create a new service account. Clicking the **New** command or toolbar button displays the **Service Accounts** view allowing you to define a new Data Governance Edition service account. To create a new service account, enter the following information: • **Active Directory account**: Select the Active Directory account to be used as a service account. • **Password**: Enter the password associated with the selected account. • **Comments**: (Optional) Enter descriptive text regarding the selected account. When a service account is added to Data Governance Edition, it is granted the required Log On as a Service local user rights on the Data Governance server.	Adding and editing a service account
Delete	Use the **Delete** right-click command or toolbar button to remove the selected service account.	
Change master data	Use the **Tasks	Change master data** right-click command or **Edit** toolbar button to display the service account master data page to change the password	Adding and editing a service account

Task	Description	For more information
	or comment associated with the selected service account.	
Assign domains	Use the **Tasks | Assign domains** right-click command to view, add, or modify the domain assignments for the selected service account.	Adding a managed domain

Managed domains view

Selecting **Managed domains** in the Data Governance navigation view populates the **Managed domains** result list with all the managed domains defined for the current Data Governance Edition deployment.

NOTE: The link between a service account and an Active Directory domain makes it a "managed domain."

For more information on the managed domains view tasks, see the *One Identity Manager Administration Guide for Active Directory Domain*.

Managed hosts view

Selecting **Managed hosts** in the Data Governance navigation view populates the **Managed Hosts** result list with all of the managed hosts deployed in the current Data Governance Edition deployment.

Selecting this node also displays the **Managed hosts** view in the right pane which lists all of the computer objects found during the topology harvest or Active Directory synchronization, and SharePoint synchronization if applicable. From this view, you can see the status of each managed host as well as the host computers that are not yet being managed by Data Governance Edition.

Double-clicking a managed host in either the result list or **Managed hosts** view launches the **Resource browser** allowing you to view data on the managed host.

The following table describes the default information displayed for each computer object found.

Table 3: Managed hosts view: Default layout

Column Title	Description
Host Name	The name of the host computer that may be the target of collection.

Column Title	Description
Domain	The fully qualified domain name of the domain in which the host computer belongs.
Status	The current status of the managed host. In addition to providing the current status of managed hosts, it also indicates when a host computer is not being managed by Data Governance Edition. For more information, see Verifying managed host system status on page 115. NOTE: The **Managed Hosts** result list only displays computer objects that are being managed by Data Governance Edition; therefore, it does not include the computer hosts with a status of **Not Managed**.
Data Status	For managed hosts, the current state of the data available from the host computer. For more information, see Determining the state of the data on page 117.
Host Type	The physical configuration of the host computer: • Distributed File System Root • EMC Celerra/VNX Device • EMC Isilon Device • EMC Isilon NFS Device • NetApp OnTap Cluster Mode CIFS Device • NetApp OnTap Cluster Mode NFS Device • NetApp OnTap 7-Mode CIFS Device • NetApp OnTap 7-Mode NFS Device • OneDrive for Business • SharePoint Farm • SharePoint Online • Windows Computer • Unknown/Generic Host Type NOTE: The NFS host types are displayed after they have been added as managed hosts using the **Manage NFS host** task. NOTE: The cloud provider host types (for example, SharePoint Online and OneDrive for Business) are displayed after they have been added as managed hosts using the **Manage Cloud host** task. NOTE: Unknown is displayed for hosts that can be added as generic managed hosts. You must update the

Column Title	Description
	"additionalOperatingSystems" configuration setting in order to see unknown host types. For more information, see Adding a generic managed host on page 71. After a host with an "unknown" host type is added as a generic managed host, the **Host Type** will change to **Generic Host Type**.
Agent Errors	Indicates how many critical errors are associated with an agent monitoring the selected managed host. For more information, see Viewing agent errors on page 120.

In addition to the default columns, you can add the following columns to the view using the **Column Chooser** command.

NOTE: Right-click the column header and select **Column Chooser** to add hidden columns to the display. In the **Customization** dialog, double-click the required column or drag and drop it onto the column header bar.

To hide a column, right-click the column header and select **Remove This Column**. The column is now listed in the **Customization** dialog and can be re-added to the view as explained above.

Table 4: Managed hosts view: Hidden columns

Column Title	Description
Forest DNS Name	Full DNS name of the forest where the host computer resides.
Host DNS Name	Full DNS name of the host computer.
Keywords	For managed hosts, free-form text tags that can be displayed to allow for arbitrary grouping and sorting of hosts.
Managed Host Id	For managed hosts, the value (GUID) assigned to the managed host.
Management Method	For managed hosts, indicates whether the host is managed locally or remotely.
Most Recent Activity	For managed hosts, the most recent time (UTC) that detailed security information was collected by any of the agents for this host.
Operating System	For managed hosts, the operating system running on the host computer.
Starts With	First character from the host computer's name. This is useful for grouping or sorting.

Managed hosts view tasks

From the **Managed hosts** view, you can check the current state of all your managed hosts using the status column. In addition, from this view, you can add managed hosts, edit host settings, get all logs, view all resources under governance for a managed host, remove a managed host, or display the Resource browser.

NOTE: If you are assigned the **Data Governance | Operators** role, you will have read-only access to this page and will not be able to perform the tasks listed below.

The following tasks are available regardless of the host computer selected in the **Managed hosts** view.

Table 5: Managed hosts views: Tasks always available

Task	Description	For more information
Customize default host settings	Launches the **Customized default host settings** dialog to view or modify the default settings for a given host type. The default settings specified are used for managed hosts added in the future.	Customizing default host settings
Get All Logs	Launches the **Browse for Folder** dialog to specify where to export the server log and agent deployment logs.	Getting server logs
Manage Cloud host	Launches the **Managed Host Settings** dialog allowing you to specify the configuration settings for defining a new cloud provider host, such as SharePoint Online. This dialog also allows you to enter the Office 365 domain and administrator login credentials to be used to authenticate to the Data Governance Edition API cloud proxy.	Adding a cloud managed host
Manage DFS host	Launches the **DFS Managed Host Settings** dialog allowing you to specify the DFS domain and root to be managed.	Adding a Distributed File System (DFS) root managed host
Manage NFS host	Launches the **Managed Host Settings** dialog allowing you to add an NFS host to be managed for a supported EMC or NetApp storage device with NFS file system protocol enabled.	Adding an NFS managed host
Refresh	Retrieves and displays the latest data for managed hosts.	

Task	Description	For more information
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options

When you select a host that is not yet managed from the **Managed hosts** view, you can perform this additional task.

Table 6: Managed hosts view: Tasks for unmanaged hosts

Task	Description	For more information
Manage host Manage multiple hosts	Launches the **Managed Host Settings** dialog allowing you to specify the configuration settings for defining a new managed host.	Adding and config-uring managed hosts

When you select a managed host from the **Managed hosts** view, you can perform the additional tasks.

Table 7: Managed hosts view: Tasks for managed hosts

Task	Description	For more information
Accounts view	Displays the security index information returned by Data Governance agents for the selected managed host. NOTE: Not available for NFS managed hosts.	Browsing your environment Accounts view
Edit host settings	Launches the **Managed Host Settings** dialog allowing you to view or edit the configuration settings for the selected managed host. You can also use this task to add, remove or change the agents used for scanning remote managed hosts.	Editing managed host settings Removing agents
Governed data	Displays the **Governed data** view to view all of the resources within the selected host that have been placed under governance.	Managing governed data details Governed data view
Refresh governed data	Retrieves the latest data available for resources placed under governance on the selected managed host.	

Task	Description	For more information
Remove	Removes the selected managed host and any associated agents from the deployment.	Removing managed hosts (and associated agents)
Rescan	Forces a rescan of all agents associated with the selected managed host.	
Resource browser	Launches the **Resource browser** which contains a live view of the data on the selected managed host. You can browse through the supported file systems and see all applied permissions and make changes where required. You can also see where the access on a resource differs from its parent and manage that access. NOTE: Double-clicking a managed host also launches the **Resource browser**.	Browsing your environment Searching for resources Resource browser
View deviations	Displays a tree view of all resources and all sub-resources below the root that have explicit security applied to them and any deviation errors encountered for the selected resource. As you select resources in the tree, you can view and manage their security. NOTE: Not available for resources on NFS managed hosts. NOTE: Not available for resources on Cloud managed hosts.	Managing security deviations

Agents view

Selecting **Agents** in the Data Governance navigation view populates the **Agents** result list with all the Data Governance agents deployed in the current Data Governance Edition deployment. Selecting this node also displays the **Agents** view in the right pane which lists all the agents, including their current status, agent activity and performance.

The following table outlines the default information displayed for each agent deployed in your Data Governance Edition deployment.

Table 8: Agents view: Default layout

Column title	Description
Agent Host	The name of the host computer running the agent software.
Agent Domain	The fully qualified domain name of the domain where the Data Governance agent that is performing the security scan resides.
Managed Host	The name of the host computer being managed. NOTE: This is the same as the Agent Host for local managed hosts, but different for remote managed hosts.
Service Display Name	The display name of the Data Governance agent service, as displayed by the Service Control Manager, that is performing the security scan.
Agent Version	The version of the Data Governance agent software that is currently deployed.
Agent Status	The current status of the agent. For more information, see Checking the agent status on page 118.
Status Detail	The current state of the data from this agent. In addition, this column provides additional information about failed agent installs or managed hosts that are in an error state due to agent issues.
Critical Error	Indicates how many critical errors are associated with the agent. For more information, see Viewing agent errors on page 120.
Agent Uptime	Indicates how much time has passed since the agent's last restart. NOTE: Agents can restart for several reasons, including restarts of their host systems, restarts of the agent service itself, or install and upgrade operations on other agents hosted on the same system.
Total Files Size	The total size of all the files in the agent instance directory.
Total Scan Time	The duration of the last full security scan. This value is not filled in until at least one full scan has been completed.
Scan Items/sec	The average rate of items indexed during the last full security scan. NOTE: An average performance of less than 1000 items per second can indicate a poor network connection between the agent and its target managed host.
Items Scanned	The number of items scanned by the agent during its last full security scan.
Items Stored	The number of items stored for this agent since the last full security scan.
Changes Processed	The number of real-time scan updates that have been processed during the scheduled scan.

Column title	Description
Changes Enqueued	The number of real-time scan updates that have been queued and are waiting to be applied to the scan data.
Activity Enabled	Indicates whether resource activity collection has been enabled on the agent.
Activity Enqueued	The number of resource activity records that have been queued and are waiting to get stored and aggregated in the Resource Activity store.
Activity Processed	The number of resource activity records that have been processed and stored in the Resource Activity store.
Aggregated Activities	The number of activities recorded by Data Governance Edition, after duplicate events have been removed. Aggregated activities are based on the granularity you have set on the managed host's **Resource Activity** page. The less granular the setting, the lower this number is.
Agent Host Type	Indicates whether the agent is local (scanning the local computer) or remote (scanning a remote managed host).
Managed Host Type	The physical configuration of the host computer: • Distributed File System Root • EMC Celerra/VNX Device • EMC Isilon Device • EMC Isilon NFS Device • Generic Host Type • NetApp OnTap Cluster Mode CIFS Device • NetApp OnTap Cluster Mode NFS Device • NetApp OnTap 7-Mode CIFS Device • NetApp OnTap 7-Mode NFS Device • OneDrive for Business • SharePoint Farm • SharePoint Online • Windows Computer

The following table describes the agent information provided in the SharePoint Metrics layout.

Table 9: Agents view: SharePoint Metrics layout

Column title	Description
Agent Host	The name of the computer host running the agent software.
Managed Host	The name of the computer host being managed. NOTE: This is the same as the Agent Host for local managed hosts, but different for remote managed hosts.
Agent Domain	The fully qualified domain name of the domain where the Data Governance agent that is performing the security scan resides.
Service Display Name	The display name of the Data Governance agent service, as displayed by the Service Control Manager, that is performing the security scan.
Agent Version	The version of the Data Governance agent software that is currently deployed.
Agent Status	The status of the agent. For more information, see Checking the agent status on page 118.
Status Detail	The current state of the data from this agent.
Agent Uptime	Indicates how much time has passed since the agent's last restart. NOTE: Agents can restart for several reasons, including restarts of their host systems, restarts of the agent service itself, or install and upgrade operations on other agents hosted on the same system.
Total Files Size	The total size of all the files in the agent instance directory.
Critical Error	Indicates how many critical errors are associated with the agent. For more information, see Viewing agent errors on page 120.
Farm Administrators	The number of farm administrators found on the managed host. NOTE: This metric only applies to SharePoint managed hosts.
Site Collections	The number of site collections found on the managed host. NOTE: This metric only applies to SharePoint managed hosts.
Web Application Policies	The number of web application policies found on the managed host. NOTE: This metric only applies to SharePoint managed hosts.
Unique Item Level Permissions	The number of unique permission level assignments found on the managed host. NOTE: This metric only applies to SharePoint managed hosts.
Total Scan Time	The duration of the last full security scan. This value is not filled in until at least one full scan has been completed.
Item Level Scan Time	The time it took to locate all items that contain unique permissions. NOTE: This metric only applies to SharePoint managed hosts.

Column title	Description
Hierarchy Scan Time	The time it took to scan the content in all site collections found on the managed host. NOTE: This metric only applies to SharePoint managed hosts.
Scan Items/sec	The average rate of items indexed during the last full security scan. NOTE: An average performance of less than 1000 items per second can indicate a poor network connection between the agent and its target managed host.
Containers Processed	The number of containers or folders encountered and processed during the scheduled scan. NOTE: This metric only applies to SharePoint managed hosts.
Items Scanned	The number of items scanned by the agent during its last full security scan.
Items Stored	The number of items stored for this agent since the last full security scan.
Activity Enabled	Indicates whether resource activity tracking has been enabled on the agent.
Activity Enqueued	The number of resource activity records that have been queued and are waiting to get stored and aggregated in the Resource Activity store.
Activity Processed	The number of resource activity records that have been process and stored in the Resource Activity store.
Aggregated Activities	The number of activities recorded by Data Governance Edition, after duplicate events have been removed. Aggregated activities are based on the granularity you have set on the managed host's **Resource Activity** page. The less granular the setting, the lower this number is.
Agent Host Type	Indicates whether the agent is local (scanning the local computer) or remote (scanning a remote managed host).
Managed Host Type	The physical configuration of the host computer: • Distributed File System Root • EMC Celerra/VNX Device • EMC Isilon Device • EMC Isilon NFS Device • Generic Host Type • NetApp OnTap Cluster Mode CIFS Device

Column title	Description
	• NetApp OnTap Cluster Mode NFS Device
	• NetApp OnTap 7-Mode CIFS Device
	• NetApp OnTap 7-Mode NFS Device
	• OneDrive for Business
	• SharePoint Farm
	• SharePoint Online
	• Windows Computer

In addition to the default columns, you can add the following columns to the view using the **Column Chooser** command.

> NOTE: Right-click the column header and select **Column Chooser** to add hidden columns to the display. In the **Customization** dialog, double-click the required column or drag and drop it onto the column header bar.

> To hide a column, right-click the column header and select **Remove This Column**. The column is now listed in the **Customization** dialog and can be re-added to the view as explained above.

Table 10: Agents view: Hidden columns

Column title	Description
Activity Files Size	The total size of all resource activity store files on the agent. These files are deleted upon successful synchronization with the Data Governance server.
Agent ID	The unique identifier generated by Data Governance Edition to identify the agent.

Agents view tasks

From the **Agents** view you can check the current state and manage your Data Governance agents.

> NOTE: If you are assigned the **Data Governance | Operators** role, you will have read-only access to this page and will not be able to perform the tasks listed below.

When an agent is selected in the **Agents** view, you can perform the following tasks against the selected agent.

Table 11: Agents view: Tasks

Tasks	Description	For more information
Clear agent errors	Clears the error messages for the selected agent. NOTE: Task is only available when there are error messages logged for the selected agent.	
Export agent log	Launches the **Browse for Folder** dialog to specify where to export the agent logs.	Exporting agent log
Refresh	Retrieves and displays the latest agent details on the Agents view.	
Restart agent	Restarts the selected Data Governance agent.	Restarting agents
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options
Upgrade agents	Upgrades the selected agents to the latest version. NOTE: Task is only available when a newer agent version is available.	
View agent errors	Launches the event viewer to display all error messages logged for the selected agent. NOTE: Task is only available when there are error messages logged for the selected agent.	Viewing agent errors
View deviations	Displays a tree view of all resources and all sub-resources below the root that have explicit security applied to them and any deviation warnings or errors encountered for the selected resource. As you select resources in the tree, you can view and manage their security.	Managing security deviations

Security index view

Selecting **Security index** in the Data Governance navigation view populates the **Accounts** result list with all accounts that have been given direct security privileges on resources within Data Governance Edition managed hosts (from the security index). Double-clicking

an account in the result list displays the Account Overview which is a graphical representation of the information available about the selected account.

Selecting the **Security index** node also displays the **Security index** view in the right pane that provides a more complete list of accounts. This view provides details about the following accounts:

- Accounts that have been given direct security privileges on resources within managed hosts (from the security index).
- Accounts that do not have explicit permissions on any resources (not included in the security index).

NOTE: An Active Directory synchronization, and if applicable a SharePoint synchronization, must be performed to populate the **Security index** view. The information included in this view is obtained from the Active Directory Users and Groups, Local Users and Groups, SharePoint Users, Groups and Claims, and Deleted (Orphaned) Active Directory accounts.

Table 12: Security index view: Default layout

Column title	Description
Has Explicit Permissions	Indicates whether the account was discovered during an agent's security scan and is included in the security index: • **No**: Securities that do not have explicit permissions on any resources. • **Yes**: Securities that have explicit permissions defined on one or more resources. NOTE: By default, the view is grouped by the **Has Explicit Permissions** flag. Click the expansion box to the left of a group, **No (No explicit permissions on any resources)** or **Yes (Has explicit permissions on one or more resources)** to display all of the accounts grouped under each grouping.
Account (CN)	The canonical name of the account.
Account (SAM Account Name)	The logon name (sAMAccountName attribute) for the account.
Account Type	The type of account: • Azure AD Group • Azure AD User • Domain Local Group • Domain User • Global Group • Machine Local Group • Machine Local User

Column title	Description
	• SharePoint Online Group • SP Group (SharePoint Group) • SP Identity SharePoint Identity) • SP User (SharePoint User) • Universal Group • Unix Group • Unix Owner • Unix Other • Other NOTE: The Unix Owner, Unix Group and Unix Other account types are only available when the optional Unix module is installed.
Domain	The DNS domain name of the domain.
Associated Employee Name	The name of the Employee object associated with the account.

In addition to the default columns, you can add the following columns to the view using the **Column Chooser** command.

NOTE: Right-click the column header and select **Column Chooser** to add hidden columns to the display. In the **Customization** dialog, double-click the required column or drag and drop it onto the column header bar.

To hide a column, right-click the column header and select **Remove This Column**. The column is now listed in the **Customization** dialog and can be re-added to the view as explained above.

Table 13: Security index view: Hidden columns

Column title	Description
Security Identifier (SID)	The security identifier (SID) assigned to the account.
UID_Person	The ID (GUID format) assigned to the Employee associated with the account.
UID_QAMTrustee	The ID (GUID format) assigned to the account by Data Governance Edition.

Security index view tasks

When you select an account in the **Security index** view, the following tasks are enabled that can be run against the selected account to manage the account's access.

| NOTE: These security index tasks are not supported for Unix account types.

Table 14: Security index view: Tasks

Task	Description	For more information
Account access report	Generates a report displaying the account's resource access across all managed hosts within the enterprise. Selecting this task displays the **Account Access** dialog allowing you to define the report parameters for running the Account access report. NOTE: To generate the Account access report for multiple accounts, select multiple rows in the **Security index** view, right-click and select **Account access**. The report will contain account access for all selected accounts.	Account access report Viewing selected reports within the Manager
Account activity report	Generates a report displaying all the activity for the selected account against specific managed hosts. Selecting this task displays the **Account Activity** dialog allowing you to define the report parameters for generating the Account activity report. NOTE: This report is not available for groups. NOTE: This report is not available for Cloud/Office 365 accounts.	Account activity report Viewing selected reports within the Manager
Account comparison	Displays the **Account Comparison** view allowing you to compare the resource access of two accounts. NOTE: This feature is not available for accounts that do not have a Security Identifier (SID) associated with them. NOTE: This report is not available for Cloud/Office 365 accounts.	Comparing accounts
Account simulation	Displays the **Account Simulation** view	Simulating the

Task	Description	For more information
	allowing you to simulate changes to group membership to see the access that would be granted or revoked.	effects of group membership modifications on an account
	NOTE: This feature is not available for accounts that do not have a Security Identifier (SID) associated with them.	
	NOTE: This feature is not available for Machine Local trustees.	
	NOTE: This report is not available for Cloud/Office 365 accounts.	
Manage access	Displays the **Manage Access** view that displays the managed hosts where the selected account has access. From here, you can also view detailed group membership information.	Manage access view Managing account access
	NOTE: This feature is not available for accounts that do not have a Security Identifier (SID) associated with them.	
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options

Governed data view

Selecting **Governed data** in the Data Governance navigation view displays the **Governed data** view in the right pane. The **Governed data** view provides a quick view of the resources (folders and shares) within your organization that have been placed under governance. The **Governed data** view can also be displayed by selecting **Governed data** in the tasks view or right-click menu from the following views:

- **Managed hosts** view
- **Resource browser**
- **Accounts** view

NOTE: The **Governed data** view displayed when using the **Governed data** node in the navigation view shows governed data for all managed hosts. Whereas, the **Governed data** view displayed when using the **Governed data** task from these other views shows the governed data for the selected managed host only.

The following table describes the default information displayed for each resource placed under governance.

Table 15: Governed data view: Default columns

Column Title	Description
Host Name	The name of the host computer where the governed data resides. NOTE: By default, the view is grouped by the **Host Name**. Click the expansion box to the left of a host name to display all of the governed resources grouped under each grouping.
Resource	The network path and name of the governed resource.
Domain Name	The fully qualified domain name of the domain where the Data Governance agent resides.
Display Name	The display name of the governed resource as specified on the confirmation dialog when the resource was placed under governance. NOTE: You can change the display name using the **Change governed resource master data** task.
Resource Type	The type of resource. For example: • NFS\Folder • NTFS\Folder • Windows Computer\Share • SharePoint\Folder
Ownership Set By	The user who set the ownership to its current owner.
Placed Under Governance By	The user who placed the resource under governance.
Published to IT Shop	Indicates whether the resource is available for requests through the IT Shop.
Business Owner	The business owner assigned to the governed resource. NOTE: You can change the business owner using the **Change governed resource master data** or **Set Business Ownership** task.
Published to IT Shop Date	The date and time (UTC) when the resource was published to the IT Shop.
Requires Ownership	Indicates whether the business ownership requirement was set for the governed resource. NOTE: You can change this requirement using the **Change governed resource master data** or **Set Business Ownership** task.
Date Ownership	The date and time (UTC) the current owner was set.

Column Title	Description
Set	
Last Security Collection Date	The date and time (UTC) when the governed resource's Points Of Interest (POI) security information was last collected.
Last Security Synchronization Date	The date and time (UTC) when the governed resource's Points Of Interest (POI) security information was last synchronized.
Is Stale	Indicates whether the resource is in a "stale" state. A resource is deemed stale if it has not been scanned by any of the Data Governance agents or if the resource has been moved or renamed.
Classification Level	The classification level assigned to the resource.

In addition to the default columns, you can add the following columns to the view using the **Column Chooser** command.

NOTE: Right-click the column header and select **Column Chooser** to add hidden columns to the display. In the **Customization** dialog, double-click the required column or drag and drop it onto the column header bar.

To hide a column, right-click the column header and select **Remove This Column**. The column is now listed in the **Customization** dialog and can be re-added to the view as explained above.

Table 16: Governed data view: Additional columns available

Column Title	Description
Description	The comments entered on the governed resource's **General** properties page.
Justification	The reason for assigning the ownership to the current owner as entered on the governed resource's **Business Owner** properties page or the **Set Business Ownership** page in the **Business Ownership** wizard.

Governed data view tasks

The **Governed data** view displays all of the resources (folders and shares) on the selected host that have been placed under governance. From this view you can manage the governed data, establish business ownership for the resource, remove resources from governance, publish and unpublish the resource to the IT Shop, and run resource access and activity reports.

When a resource is selected, you can perform the following tasks.

Table 17: Governed data view: Tasks

Task	Description	For more information
Calculate perceived owners	Calculates and provides a list of the perceived owners for the selected resource using the resource activity history or security information.	Calculating perceived owner
Change governed resource master data	Allows you to view or modify the master data for the selected governed resource, including assigning a business owner to the resource.	Managing resources under governance Managing business ownership for a resource
Publish to IT Shop	Publishes the selected resources to the IT Shop, making it available for employees and business owners to request and grant access to it. NOTE: Not available for resources on NFS managed hosts. NOTE: Not available for resources on Cloud managed hosts.	Publishing resources to the IT Shop
Refresh	Retrieves and displays the latest data about governed resources.	
Remove resources from governance	Removes a resource from governance and from the IT Shop.	Removing resources from governance
Resource access report	Generates a report that identifies the accounts that have access to specific resources within your environment. Selecting this task, displays the **Resource access** dialog allowing you to specify the report parameters.	Resource access report Viewing selected reports within the Manager
Resource activity report	Generates a report that provides a list of activities recorded over a period of time to verify proper resource usage and decide whether to remove access for particular accounts. Selecting this task, displays the **Resource activity** dialog allowing you to specify the report parameters. NOTE: Not available for resources on Cloud managed hosts.	Resource activity report Viewing selected reports within the Manager
Set business ownership	Assigns a business owner for the selected	Managing business ownership for a

ONE IDENTITY
by Quest

Task	Description	For more information
	resource. Selecting this task, displays the **Business Ownership** wizard where you can assign ownership to an individual employee or a group of employees belonging to an existing application role.	resource
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options
Unpublish from IT Shop	Removes a previously published resource from the IT Shop. NOTE: Not available for resources on NFS managed hosts. NOTE: Not available for resources on Cloud managed hosts.	Publishing resources to the IT Shop

In addition, when viewing governed data for a selected managed host (using the **Governed data** task or right-click command), you can open the following views.

Table 18: Governed data view: Views

View	Description	For more information
Accounts view	Displays the security index information returned by Data Governance agents for the selected managed host. NOTE: This task is only available when the **Governed data** view is opened for a selected managed host. That is, when you selected the **Governed data** task from the **Managed hosts** view, **Accounts** view or the **Resource browser**. NOTE: Not available for NFS managed hosts.	Accounts view
Resource browser	Launches the **Resource browser** which contains a live view of the data on the selected managed host. You can browse through the supported file systems and see all applied permissions and make changes where required. You can also see where the access on a resource differs from its parent and manage that access.	Browsing your environment Resource browser

View	Description	For more information
	NOTE: This task is only available when the **Governed data** view is opened for a selected managed host. That is, when you selected the **Governed data** task from the **Managed hosts** view, **Accounts** view or the **Resource browser**.	

Classification view

Selecting **Classification** in the Data Governance navigation view displays the **Classification** view in the right pane which lists all of classification levels defined. From this view, you can add, edit or remove classification levels. In addition, you can define the display order for the classification levels defined in your Data Governance Edition deployment.

Table 19: Classification view: Tasks

Task	Description	For more information
New	Adds a new classification level. Clicking the **New** task displays the **Classification Level** dialog allowing you to specify the following details: • **Name**: Name to be associated with the new classification level. • **Description**: Descriptive text to be associated with the new classification level.	Adding a classification level
Delete	Removes the selected classification level. Selecting **Yes** on the confirmation dialog will remove the classification assignment on any governed resource that is currently assigned to the classification level being deleted. TIP: Prior to removing a classification level, run the **Get-QGovernedDataByClassificationLevel** PowerShell cmdlet to retrieve a list of governed resources assigned to a specified classification level.	Removing a classification level

Task	Description	For more information
Edit	Launches the **Classification Level** dialog allowing you to modify the name or description associated with the selected classification level.	Editing a classification level
Move up	Moves the selected classification level up in the display list.	
Move down	Moves the selected classification level down in the display list.	
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options

Background operations view

Selecting **Background operations** in the Data Governance navigation view allows you to view the progress of various background operations, including:

- Log export operations
- Account access operations submitted from the **Manage access** view.

The following table describes the information displayed for current background operations.

Table 20: Background operations view: Default columns

Column title	Description
Description	A description of the background operation being processed by Data Governance Edition.
Status	The status of the background operation.
Resource	The resource involved in the operation.
Operation	The background operation being processed.
Start Time	The date and time (UTC) the operation began.
End Time	The date and time (UTC) the operation completed.

In addition to the default columns, you can add the following columns to the view using the **Column Chooser** command.

NOTE: Right-click the column header and select **Column Chooser** to add hidden columns to the display. In the **Customization** dialog, double-click the required column

or drag and drop it onto the column header bar.

To hide a column, right-click the column header and select **Remove This Column**. The column is now listed in the **Customization** dialog and can be re-added to the view as explained above.

Table 21: Background operations view: Hidden columns

Column title	Description
Enqueued Time	The date and time (UTC) the operation was added to the background queue.
Error	Any errors encountered during the background operation.

Resource browser

The **Resource browser** provides a live view of the data on the selected managed host. Using the **Resource browser**, you can browse through the supported files system to view and manage security information for folders and shares on the target managed host.

The **Resource browser** displays the following information:

- For a Windows computer, the shares and file system display.

- For a SharePoint farm, each farm is represented as a hierarchy, with the farm as the top level, followed by web applications, site collections, sites and then the contents of the site. The contents of a list are shown as "list item", regardless of the type of item in SharePoint. The **Resource browser** displays a list of the web applications on the selected farm.

- For a Distributed File System Root, links are displayed at the top level. Browsing into a link shows its target paths and browsing into a target path takes you to the appropriate backing folder. While browsing a backing folder, the Distributed File System path is shown in the **Location** field at the top of the page.

- For Cloud managed hosts, each site is represented by a folder hierarchy, with the Home top level site displayed as Site contents folder, followed by all other subsites. Each site contains a Site contents folder encompassing other nested folders. The contents of a site and document library are shown as "folder" type, whereas, files are shown as "file" type items. No other resource types are managed for Cloud managed hosts.

  NOTE: The **Resource browser** and resource access reports do not display the limited access users or "previewer" accounts.

You can display the **Resource browser** from the following views:

- **Managed hosts** view

- **Accounts** view

- **Governed data** view

Double-click through the resources to locate a resource. Depending on the resource type, you can perform the following tasks against the selected resource.

Table 22: Resource browser: Resource tasks

Task	Description	For more information
Calculate perceived owners	Calculates and provides a list of the perceived owners for the selected resource using the resource activity history or security information.	Calculating perceived owner
Copy resource path	Copies the full path of the selected resource to the clipboard.	
Copy Share Path	Copies the path of the selected Share to the clipboard.	
Edit host settings	Launches the **Managed Host Settings** dialog allowing you to view or edit the configuration settings for the selected managed host.	Editing managed host settings
Place resource under governance	Places the selected resource under governance, making it available for use in policies and attestations. NOTE: Only applies to folders and shares. That is, you cannot place a file under governance.	Placing a resource under governance
Publish to IT Shop	Publishes the selected resources to the IT Shop, making it available for employees and business owners to request and grant access to it. If applicable, also places the resources under governance. NOTE: Only applies to folders and shares. That is, you cannot publish a file to the IT Shop. NOTE: Not available for resources on NFS managed hosts. NOTE: Not available for resources on Cloud managed hosts.	Publishing resources to the IT Shop
Refresh	Retrieves and displays the latest details in the **Resource browser**.	
Remove resources from governance	Removes the selected resources from governance.	Removing resources from governance
Resource access	Generates a report that identifies the	Resource access

Task	Description	For more information
report	accounts that have access to specific resources within your environment.	report Viewing selected reports within the Manager
Resource activity report	Generates a report that provides a list of activities recorded over a period of time to verify proper resource usage and decide whether to remove access for particular accounts. NOTE: Not available for resources on Cloud managed hosts.	Resource activity report Viewing selected reports within the Manager
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options
Unpublish from IT Shop	Removes a previously published resource from the IT Shop. NOTE: Not available for resources on NFS managed hosts. NOTE: Not available for resources on Cloud managed hosts.	Publishing resources to the IT Shop
View deviations	Displays a tree view of all resources and all sub-resources below the root that have explicit security applied to them and any deviation warnings or errors encountered for the selected resource. As you select resources in the tree, you can view and manage their security. NOTE: Not available for resources on NFS managed hosts. NOTE: Not available for resources on Cloud managed hosts.	Managing security deviations
View governed data details	Displays a graphical representation of the details available for governed resources.	

When an account in the resource's permissions pane (lower pane) is selected, you can perform the following tasks against the selected account.

NOTE: These account tasks are not available for resources on NFS managed hosts.

Table 23: Resource browser: Account tasks

Task	Description	For more information
Account access report	Generates a report displaying the account's resource access across all managed hosts within the enterprise. Selecting this task displays the **Account Access** dialog allowing you to define the report parameters for running the Account access report.	Account access report Viewing selected reports within the Manager
Account comparison	Displays the **Account Comparison** view allowing you to compare the resource access of two accounts. NOTE: This feature is not available for Cloud accounts.	Comparing accounts
Account simulation	Displays the **Account Simulation** view allowing you to simulate changes to group membership to see the access that would be granted or revoked. NOTE: This feature is not available for Cloud accounts.	Simulating the effects of group membership modifications on an account
Add rights	Launches the **Add Permissions** dialog allowing you to manage a user or group's access to the selected resource. From this dialog, you can add or edit an account's access as required.	Modifying discretionary access control list (DACL) permissions for NTFS resources Modifying auditing system access control list (SACL) permissions for NTFS resources
Manage access	Displays the **Manage access** view that shows the managed hosts where the selected account has access. From here, you can also view detailed group membership information.	Manage access view Managing account access
Remove all explicit permissions	Removes all explicitly assigned permissions from the selected resource.	Managing security deviations
Remove selected permissions	Removes the selected permissions from the selected resource.	Modifying discretionary access control list (DACL) permissions for NTFS resources

Task	Description	For more information
		Modifying auditing system access control list (SACL) permissions for NTFS resources

In addition, you can access the following views from the **Resource browser**.

Table 24: Resource browser: Views

View	Description	For more information
Governed data	Displays the **Governed data** view to view all the resources within the selected host that have been placed under governance.	Governed data view Managing resources under governance
Accounts view	Displays the security index information returned by Data Governance agents for the selected managed host. NOTE: Not available for NFS managed hosts.	Accounts view

Manage access view

The **Manage access** view appears when **Manage access** is selected from the tasks view. From this view, you can see the access for the selected account on all managed hosts within your environment and detailed group membership information. This view consists of the following panes:

- **Access Points**: The main pane is the results of a database query that retrieves the hosts a trustee has access to.

  NOTE: By default, the **Filter builtin accounts (Administrators and Users)** check box is selected indicating that noisy accounts (that is, accounts with indirect access granted through the BUILTIN\Administrators or BUILTIN\Users accounts) are not included in the view. To include these accounts in the **Access Points** pane, clear the check box at the top of the view.

- **Detailed Access Information**: The lower pane is the result of an agent query that retrieves more information about the resource selected in the **Access Points** pane.

- **Group Memberships**: The left pane displays the group membership information resolved from Active Directory from the Data Governance server.

By default, the results in the **Access Points** pane are grouped by the host name of managed host. Expand a managed host and select an account in the **Access Points** pane to display all the resources where the selected user or group has access. Click the **Group Memberships** tab to view how the account has gained access through group membership. Selecting an account in the **Group Memberships** pane retrieves and displays the hosts where the selected trustee has access.

NOTE: This view is not available for NFS managed hosts.

When a resource is selected in the lower pane, you can perform the following tasks.

Table 25: Manage access view: Resource-related tasks

Task	Description	For more information
Calculate perceived owners	Calculates and provides a list of the perceived owners for the selected resource using the resource activity history or security information. NOTE: Task is not available for files.	Calculating perceived owner
Clone account access	Copies the access rights to grant the selected access to another user or group, while maintaining the existing rights on the selected account.	Cloning, replacing, and removing access for a group of accounts
Copy resource path	Copies the full path of the resource to the clipboard.	
Copy Share Path	Copies the path of the share to the clipboard. NOTE: Task is not available for files or folders.	
Edit security	Displays the **Edit Resource Security** dialog allowing you to manage the security settings for the selected resource. Right-clicking an account on this dialog allows you to perform the following tasks: • Add rights • Remove selected permissions • Remove all explicit permissions NOTE: This dialog is the same view displayed in the lower pane of the Resource browser and **Deviation** view when a resource is selected.	Working with security permissions
Place resource under governance	Places the selected resource under governance, making it available for use in	Placing a resource under governance

Task	Description	For more information
	policies and attestations.	
	NOTE: Task is not available for files.	
Publish to IT Shop	Publishes the select resources to the IT Shop, making it available for employees and business owners to request and grant access to it.	Publishing resources to the IT Shop
	NOTE: Task is not available for files.	
	NOTE: Not available for resources on Cloud managed hosts.	
Refresh	Retrieves and displays the latest details in the lower pane of the view.	
Remove account	Removes the selected account's access from the resource.	Cloning, replacing, and removing access for a group of accounts
	For direct access, remove the security setting from the resource ACL. For indirect access, remove the group that is on the ACL; the selected account (the one with the indirect access) remains a member of the group that had the access prior to the removal operation.	
Remove resource from governance	Removes the selected resource from governance.	Removing resources from governance
	NOTE: Task is not available for files.	
Replace account	Replaces access to grant the currently configured access to another user or group and remove the access from the original account.	Cloning, replacing, and removing access for a group of accounts
Resource access report	Generates a report that identifies the accounts that have access to specific resources within your environment.	Resource access report Viewing selected reports within the Manager
Resource activity report	Generates a report that provides a list of activities recorded over a period of time to verify proper resource usage and decide whether to remove access for particular accounts.	Resource activity report Viewing selected reports within the Manager

Task	Description	For more information
	NOTE: Not available for resources on Cloud managed hosts.	
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options
Unpublish from IT Shop	Removes a previously published resource from the IT Shop. NOTE: Not available for resources on Cloud managed hosts.	Publishing resources to the IT Shop
View deviations	Displays a tree view of all resources and all sub-resources below the root that have explicit security applied to them and any deviation warnings or errors encountered for the selected resource. As you select resources in the tree, you can view and manage their security. NOTE: Task is not available for files or shares. NOTE: Not available for resources on Cloud managed hosts.	Managing security deviations

In addition, you can open the following views.

Table 26: Manage access view: Views

View	Description	For more information
Account overview	Displays a graphical representation of the information returned by a Data Governance agent for the selected account.	Accounts view
Hosts view	Displays the managed hosts where the selected account has access.	
Account comparison	Displays the **Account Comparison** view allowing you to compare the resource access of two accounts. NOTE: This feature is not available for Cloud accounts.	Comparing accounts
Account simulation	Displays the **Account Simulation** view allowing you to simulate changes to group membership to see the access that would be	Simulating the effects of group membership modific-

View	Description	For more information
	granted or revoked. NOTE: This feature is not available for Cloud accounts.	

Accounts view

The **Accounts** view appears when **Accounts view** is selected from the tasks list or right-click menu. The **Accounts** view displays the security information returned by Data Governance agents for the selected managed host. All resource types where users or groups have some level of access are included.

You can display the **Accounts** view from the following views in the Manager:

- **Managed hosts** view
- **Resource browser**
- **Governed data** view

NOTE: This view is not available for NFS managed hosts.

The following table describes the default information displayed for each account.

Table 27: Accounts view: Default layout

Column title	Description
Resource Type	The type of resource: • File • Folder • Local User Rights • Operating System Administrative Rights • Share • Windows Service Identity NOTE: By default, the display is grouped by resource type. Click the expansion box to the left of a resource type to expand a resource type to display all of the accounts that have access.
Account Name	The name of the account that has access.
Account Type	The type of account: • Built-in Group • Group

Column title	Description
	• Special
	• Unknown
	• Machine Local User
	• Office 365 User
	• OneDrive for Business Group
	• SharePoint Online Group
	• User
	• Well known
Namespace	The logical group (namespace) to which the account belongs: • Cloud • NTFS • Windows Computer • Service Identities

In addition to the default columns, you can add the following columns to the view using the **Column Chooser** command.

> NOTE: Right-click the column header and select **Column Chooser** to add hidden columns to the display. In the **Customization** dialog, double-click the required column or drag and drop it onto the column header bar.
>
> To hide a column, right-click the column header and select **Remove This Column**. The column is now listed in the **Customization** dialog and can be re-added to the view as explained above.

Table 28: Accounts view: Hidden columns

Column title	Description
Security Identifier (SID)	The security identifier (SID) assigned to the account.

Accounts view tasks

When an account is selected in the **Accounts** view, you can perform the following tasks against the selected account.

Table 29: Accounts view: Tasks

Task	Description	For more information
Account access report	Generates a report displaying the account's resource access across all managed hosts within the enterprise. Selecting this task displays the **Account Access** dialog allowing you to define the report parameters for running the Account access report.	Account access report Viewing selected reports within the Manager
Account activity report	Generates a report displaying all the activity for the selected account against specific managed hosts. Selecting this task displays the **Account Activity** dialog allowing you to define the report parameters for generating the Account activity report. NOTE: This report is not available for groups. NOTE: This report is not available for Cloud/Office 365 accounts.	Account activity report Viewing selected reports within the Manager
Account comparison	Displays the **Account Comparison** view allowing you to compare the resource access of two accounts. NOTE: The selected account is pre-populated in the **Source** field. NOTE: This feature is not available for Cloud/Office 365 accounts.	Comparing accounts
Account simulation	Displays the **Account Simulation** view allowing you to simulate changes to group membership to see the access that would be granted or revoked. NOTE: This feature is not available for Cloud/Office 365 accounts.	Simulating the effects of group membership modifications on an account
Manage access	Displays the **Manage access** view that displays the managed hosts where the selected account has access. From here, you can also view detailed group membership information.	Manage access view Managing account access
Toggle layout options	Shows or hides the **Layout** controls at the top of the view, allowing you to change the layout displayed.	Toggle layout options

In addition, you can open the following views.

Table 30: Accounts view: Views

View	Description	For more information
Resource browser	Launches the **Resource browser** which contains a live view of the data on the selected managed host. You can browse through the supported file systems and see all applied permissions and make changes where required. You can also see where the access on a resource differs from its parent and manage that access.	Resource browser Browsing your environment
Governed data	Displays the **Governed data** view to view all the resources within the selected host that have been placed under governance.	Governed data view Managing resources under governance

Customizing your view

Any time you see a view with column headers, you can customize it to present the information to best suit your needs.

To change the sort criteria:

NOTE: An arrow in the column heading identifies the sort criteria and order, ascending or descending, being used to display information.

1. Click the column heading to be used for the sort criteria.
2. The sort order is in ascending order. To change it to descending order, click the heading a second time.
3. To specify a secondary sort order, press the SHIFT key and then click the heading of the column to be used for the secondary sort order.

To resize a column

1. Place your cursor on the boundary between column headings (your cursor changes to a double-arrow).
2. Click and hold the left mouse button dragging the column boundary to the desired size.

To change the order of the columns

1. Use the left mouse button to click the heading to be moved (the column heading pops off the grid).
2. Drag that column to the desired location (arrows indicate where you are placing the selected column).

ONE IDENTITY
by Quest

To add and remove columns

1. Right-click the column header, and select **Column Chooser**.

2. Select the column and drag it to the desired location in the column header.

3. Close the **Customization** dialog by clicking the X.

To group by columns

NOTE: Grouping data creates a collapsed view that can be expanded to view the detailed information that applies to that group.

1. Right-click the column header and select **Show Group By Box**.

2. Select the required column and drag it to the Group by box located above the header row.

    NOTE: You can also right-click an individual column header and select **Group By This Column**. Selecting this command moves the selected header to the Group by box above the header row.

    You can select to group by additional headings to create a hierarchy of groupings.

3. To remove a grouping, right-click the heading in the Group by box located above the header row and select **UnGroup** or drag the heading back into the column header row.

Toggle layout options

Use the **Toggle layout options** task to show or hide the Layout controls at the top of the displayed view. The **Layout** controls allow you to select a pre-defined layout for displaying data. All views have a "default" layout, and some views have additional views available to filter the content. If you customize a view, you can also save the custom layout for use at a later time. Once a layout is saved, it appears in the **Layout** drop-down menu.

To change the layout being displayed

1. To display a different layout, select the layout using the **Layout** drop-down menu.

    The new layout appears in the current view.

To save or remove a custom layout

1. To save the currently displayed layout (custom layout):

    a. Click the **Save Layout As** button.

    b. Enter a description name for the layout on the **Save Layout As** dialog and click **OK**.

        The new layout appears in the **Layout** drop-down menu.

2. To delete a previously saved layout:

    a. Select the layout using the **Layout** drop-down menu.

    b. Click the **Delete Layout** button.

    c. Select **Yes** on the **Delete Layout Confirmation** dialog.

       The layout is removed from the **Layout** drop-down menu.

    d. To redisplay the default layout or another layout, select the desired layout using the **Layout** drop-down menu.

Administering Data Governance Edition

Data Governance Edition overview

Control over your organization's data is vital to eliminating issues such as security breaches, loss of sensitive information, or non-compliance with external and internal guidelines. Data Governance Edition provides a systematic approach to managing data access, preserving data integrity, and providing content owners with the tools and workflows to manage their own data resources, removing reliance on IT administrators.

Ultimately, you need a process in place that allows you to:

- Ensure that your business runs efficiently with access to correct information on demand.
- Understand the access levels, patterns, and usage to build and maintain a governance strategy.
- Comply with organizational security and compliance policies.
- Bring accountability to contain damage.
- Review the usage patterns of sensitive information.
- Identify and assign business owners.
- Enable attestations from business owners to the validity of the data and its use.

The governance of unstructured data is accomplished through workflows that cross both the Manager and the web portal. The following diagram identifies the key processes in securing and controlling access to your organization's data.

Figure 1: Data Governance Edition key processes
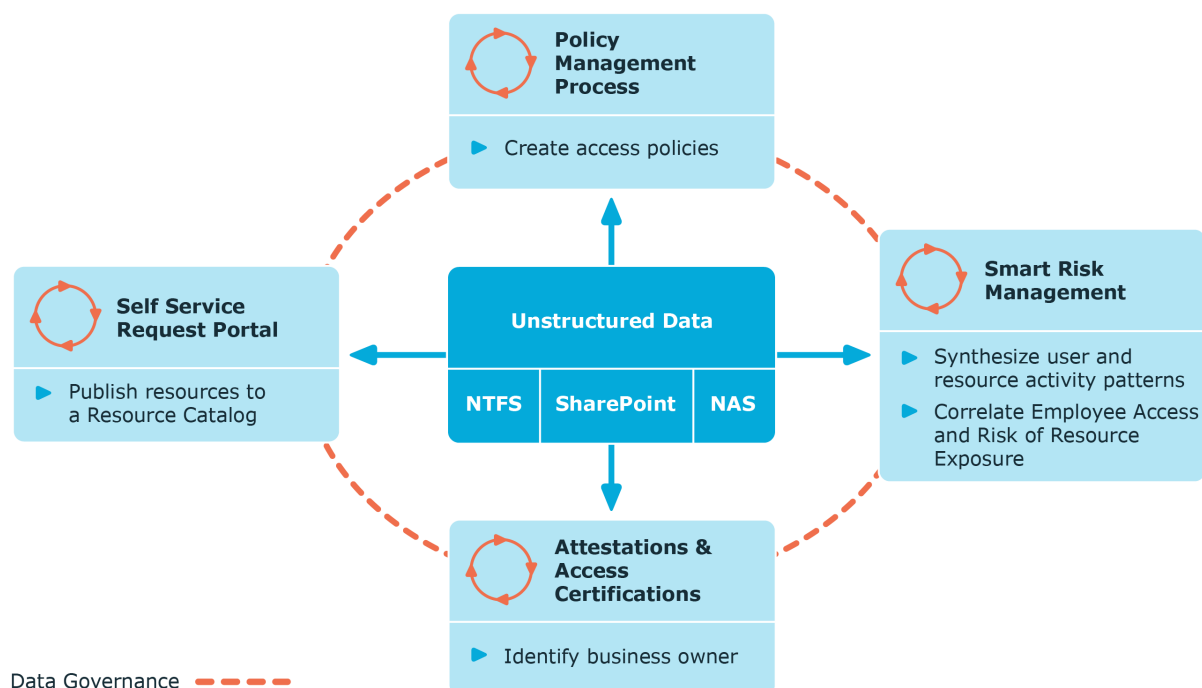
Data Governance Edition users

Data Governance Edition is designed to serve the needs of different users.

Table 31: Typical users and associated tasks

User	Tasks
Business Owner	• Resource owner.
	• Uses the web portal.
	• Reviews the resource security and usage; approves or denies requests for resource access; requests access on behalf of others, such as a new employee; and validates the security on resources.
	• Can view and assign a classification level to their owned resources.
	• Attests to the authorizations specified for the resources they own. A business owner who is also a department manager, performs access attestations for their department employees.

User	Tasks
	Business owners are automatically assigned to the **Data Governance | Direct Owners** application role when they are assigned as the business owner of a resource. They must also be assigned to the **Request & Fulfillment | IT Shop | Product Owners** application role or an application role under the Product Owners role to approve IT Shop requests. For more information on how to perform the business owner tasks, see Managing governed resources using the web portal on page 175
Compliance Officer\Security Officer	• Responsible for ensuring policies are created and are being enforced in the company. • Creates "Governance Programs", including all the required policies and workflows. • Verifies the state and progress of governance programs. • Oversees the activities of IT security personnel. This user must be assigned the **Identity & Access Governance | Compliance & Security Officer** application role. For more information, see Application roles on page 59.
Data Governance Administrator	• Maintains and edits resource security using the Manager. • Facilitates business owner and auditor requests. • Performs ad-hoc investigations of the rights of users and groups. • Configures and deploys Data Governance Edition. • Sets the resource owner and business owner. • Defines classification levels for use in classifying governed resources. • Maintains Data Governance Edition. • Delegates access to Data Governance Edition. • Implements the workflow defined by security officers, business owners, and others who need to consume the services of Data Governance Edition.

User	Tasks
	• Assigns the server and share root path to be used for creating file system shares requested through the IT Shop. Also, defines the group naming pattern to be used to create the Active Directory groups for the new share.
	This user must be assigned the **Data Governance | Administrators** application role. They must also be assigned to the **Request & Fulfillment | IT Shop | Product Owners** application role or an application role under the Product Owners role to approve IT Shop requests.
	For more information, see Application roles on page 59.
Employee\End-User\Resource Consumer\Knowledge Worker	• Uses the web portal. • Makes IT Shop requests to gain access to resources. • Makes IT Shop requests to create file system shares.
	All active employees are automatically members of the Identity & Access Lifecycle shop and can therefore make self-service requests.
Employee manager	• Uses the web portal. • Approves or denies requests for creating file system shares.
	Employee managers must be assigned the **Request & Fulfillment | IT Shop | Product Owners** application role or an application role under the Product Owners role to approve IT Shop requests.

Architecture

Data Governance Edition consists of the following components:

- Data Governance server: The server acts as an intermediary between the agents and the databases where information is stored. It coordinates all agent deployments and communication, and manages the security index for each managed host.

  The server is the central authority that receives and indexes information from agents deployed on target computers. It only maintains a subset of information for the computers that are being indexed (essentially access to specific resource types on managed computers). When you request detailed access information, the server attempts to contact the local agent and provide information stored in the local agent index.

- Data Governance agents: Agents collect security data from your managed hosts, and if configured, can also collect resource activity data. The agent cache stores all the detailed indexed information.

- Databases: The One Identity Manager database stores configuration and security information. The Data Governance Resource Activity database stores resource activity information.

- Managed hosts: A managed host is any network object that can host resources and can be assigned an agent to monitor security and resource activity. Managed hosts store the data on which users perform actions. Currently supported managed hosts include Windows computers, Windows clusters, certain network attached storage (NAS) devices, SharePoint farms and certain cloud providers, including SharePoint Online and OneDrive for Business. See the *One Identity Manager Data Governance Edition Deployment Guide* for a complete list of supported platforms.

For more information about component communications and how communication is encrypted, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Figure 2: Data Governance Edition architecture
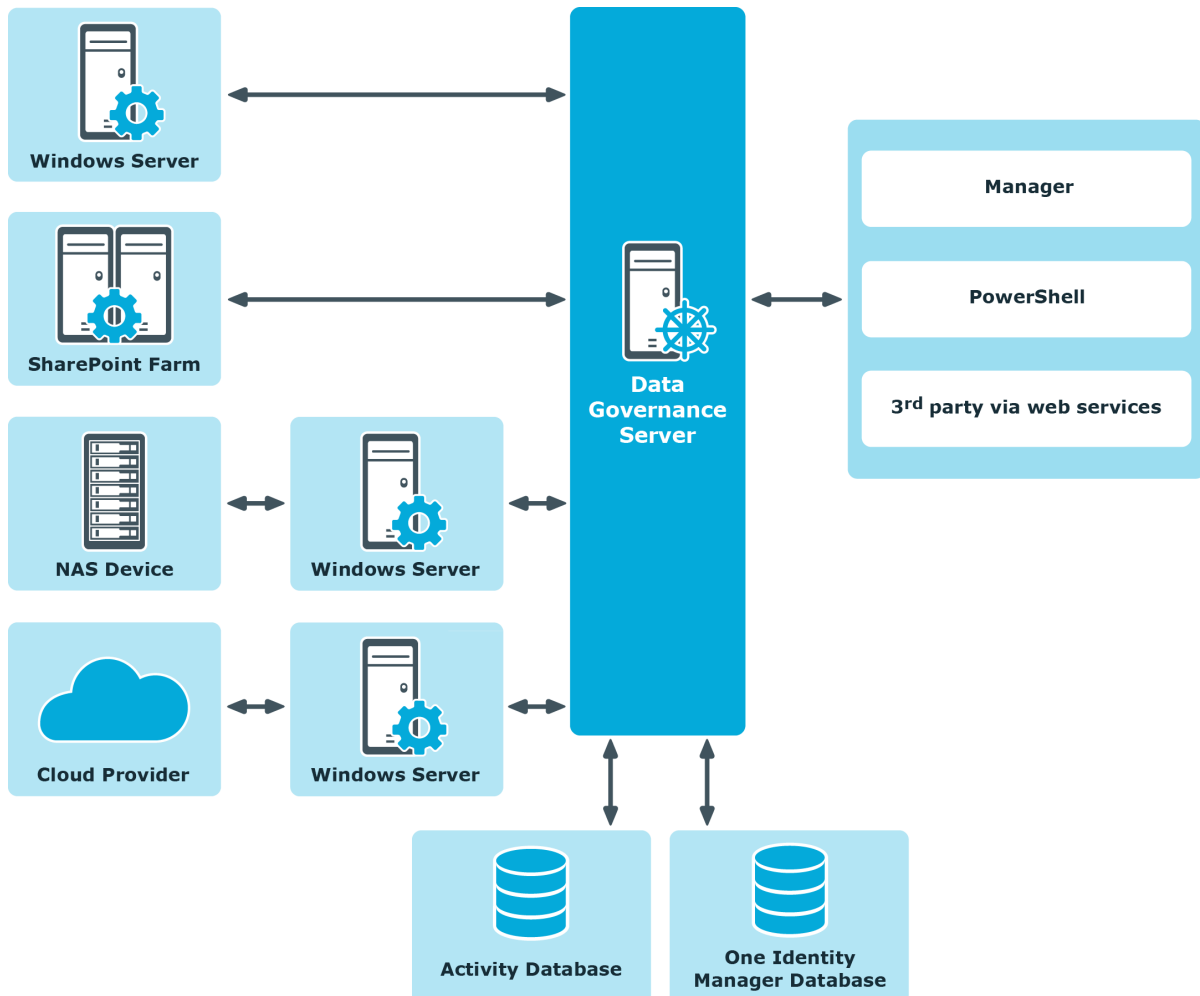
Setting up Data Governance Edition

You must perform the following activities to have a fully functional Data Governance Edition deployment:

- Install One Identity Manager Data Governance Edition.
- Create and configure the One Identity Manager database
- Install and configure the One Identity Manager service (Job server)
- Run the Data Governance Configuration wizard to:
    - Deploy the Data Governance server
    - Create the Data Governance Resource Activity database
- Configure the Data Governance service accounts for managed domains
- Add managed hosts and deploy agents
- Install the web portal

NOTE: **New in 7.0: Active Directory synchronization via the One Identity Manager service (job server) is not required for managed host deployment**.

In the absence of One Identity Manager target system synchronization, the Data Governance service automatically harvests the forest topology. It creates Employee records for all members found in each domain's Domain Admins group and for the current account running the Data Governance configuration wizard. It also links these accounts to the correct Data Governance application roles, which allows you to add managed hosts and deploy agents.

When additional One Identity Manager functionality is required, including generating complete Data Governance Edition reports, perform the following steps:

- Run the One Identity Manager Synchronization Editor to synchronize your target environments (Active Directory, and if applicable, SharePoint and Unix).

    IMPORTANT: Active Directory synchronization MUST be complete before starting the SharePoint synchronization.

- Assign Data Governance application roles to Employees.

For detailed installation and configuration procedures, see:

- Installing One Identity Manager in the *One Identity Manager Installation Guide*.
- Install One Identity Manager Data Governance Edition in the *One Identity Manager Data Governance Edition Deployment Guide*.
- Readying a service account and domains for deployment on page 61.
- Working with managed hosts and agents on page 62.
- Installing, Configuring and Maintaining the Web Portal in the *One Identity Manager Installation Guide* and the *One Identity Manager Web Portal User Guide*.
- Setting Up Synchronization with an Active Directory Environment in the *One Identity Manager Administration Guide for Connecting to Active Directory*.

- Setting Up Synchronization with a SharePoint Environment in the *One Identity Manager Administration Guide for Connecting to SharePoint*.

- One Identity Manager Application Roles in the *One Identity Manager Identity Management Base Module Administration Guide*.

Application roles

The following application roles are specifically for Data Governance Edition. They are to be used with One Identity Manager application roles. For details on applying application roles, see One Identity Manager Application Roles in the *One Identity Manager Identity Management Base Module Administration Guide*.

- **Data Governance** | **Access Managers**

  Members of this role can access all information related to Data Governance Edition, and can query information from Data Governance agents. Also, they can modify the security of objects contained on managed hosts.

- **Data Governance** | **Administrators**

  Members of this role can perform all administrative tasks necessary for the management of Data Governance Edition. This includes deploying and configuring managed hosts, managing data access, editing security, and placing data under governance.

- **Data Governance** | **Business Owner**

  Members of this role can view and edit information on resources they own. This role is used to control permissions in the web portal, and approvals and attestation workflows.

- **Data Governance** | **Direct Owners**

  This role is held by accounts and roles marked as the owners of resources within Data Governance Edition. It cannot be assigned manually; it is assigned programmatically when ownership is assigned.

- **Data Governance** | **Managed Resources**

  A default container used for roles automatically generated by Data Governance Edition managed resources. For more information on managed resources, see the *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide.*

- **Data Governance** | **Operators**

  Members of this role have read-only access to the **Managed hosts** view and **Agents** view in the Manager.

  NOTE: This role should not be used in conjunction with any of the other Data Governance application roles.

- **Identity & Access Governance** | **Compliance & Security Officer**

  Members of this role have a view into all security-related information collected by

Data Governance Edition. They are responsible for ensuring security-related compliance regulations are being followed correctly.

Authentication using service accounts and managed domains

Most organizations running a network of Windows computers have multiple Active Directory domains and forests to be managed. Users expect seamless integration and IT administrators need an all-encompassing view of their network security to make that happen.

Data Governance Edition consolidates security information across many domains and forests by accessing these network entities using stored credentials (service accounts). These service accounts are Active Directory users granted the appropriate permissions in their respective domains and registered with Data Governance Edition.

By elevating to the service accounts as necessary, the Data Governance server is able to deploy agents and retrieve security information across the organization. All communication is secure and all credential information is encrypted and protected.

Administrators responsible for the Data Governance Edition deployment must register service accounts with the system and link them with domains that have been previously synchronized with One Identity Manager. The link between a service account and an Active Directory domain makes it a "Managed Domain".

Administrators link a service account to an Active Directory domain through the Manager. For more information, see Readying a service account and domains for deployment on page 61.

How are the credentials stored securely?

Service account credentials are stored in the central One Identity Manager database. These credentials can be encrypted using the Crypto-Configuration tool. For more information, see Encrypt Data in a Database in the *One Identity Manager Installation Guide*.

What permissions do service accounts need and why?

For details on the required permissions, see the *One Identity Manager Data Governance Edition Deployment Guide*.

NOTES:

- Remote managed hosts (EMC, NetApp, Windows cluster, Cloud) require a service account with sufficient permissions to access target computers.

- SharePoint farms are similar to remote managed hosts in that they require a service account with sufficient permissions to access the data, even though they are installed locally.

- NetApp managed hosts require a service account with sufficient permissions to create and maintain FPolicy on a NetApp filer.

Readying a service account and domains for deployment

Before you can gather information on the data in your enterprise, you must:

- Add and assign the credentials (service account) used to access resources on the computers within the domain. For more information, see Adding and editing a service account on page 61.
- Select the domains that contain the computers and data that you want to manage. For more information, see Adding a managed domain on page 62.

You can specify these credentials on a per domain basis. Each domain can only have one associated service account at any time, but the same service account can be used for multiple domains. Service accounts are also used to run remote agent services on agent host computers and must be specified during remote agent deployment.

When a domain is managed, a Data Governance container is created in the domain's System container. This container holds a Service Connection Point object, which is used by the Data Governance Edition components to find one another. Agents use this information to determine where the Data Governance server they should connect to exists.

NOTE: Only domains that have had Active Directory synchronized with One Identity Manager can be managed. For details, see Setting up Synchronization with an Active Directory Environment in the *One Identity Manager Administration Guide for Connecting to Active Directory*.

Adding and editing a service account

To add a service account

1. In the Navigation view, select **Data Governance**.
2. Right-click **Service accounts** and select **New**.
3. In the **Change master data** form, select the Active Directory account, enter the password associated with the selected account and optionally enter comments.
4. Click the **Save** toolbar button to add the service account.

To edit a service account

1. In the Navigation view, select **Data Governance** | **Service accounts**.
2. In the **Service Accounts** result list, double-click the required service account.

   From the service account overview, you can view the domains associated with the selected service account.

3. From the Tasks view, select **Change master data**.

4. Select the Active Directory account, and enter the password and comment.

5. Click the **Save** toolbar button to save your changes.

Adding a managed domain

The rights needed to perform operations and scan computers are established by assigning a service account to the required domain.

The service account must already be created in Data Governance Edition to be assigned to a domain. For more information, see Adding and editing a service account on page 61.

To enable the Data Governance server to interact with computers in a domain

1. In the Navigation view, select **Data Governance** | **Service accounts**.

2. In the **Service Accounts** result list, right-click the service account, and select **Tasks | Assign domains**.

3. In the **Add assignments** pane (lower pane), double-click the required domain. You can also right-click the managed domain and select **Assign** or **Assign all objects**.

   The managed domain now appears in the top pane.

4. Click the **Save** toolbar button to save your selection.

NOTE: From the **Managed hosts** view, if you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Working with managed hosts and agents

A managed host is any network object that can host resources and can be assigned an agent to monitor security and resource activity. For more information, see Adding and configuring managed hosts on page 65.

NOTE: Any objects that you want to manage through Data Governance Edition must first be added to Active Directory.

Depending on the type of managed host, you may be deploying different agents. There are two types of agents — local and remote.

Table 32: Differences between local and remote agents

Agent	Description
Local agent	Local agents reside on the same computer as the managed host.
	When you deploy a local agent, it immediately scans all fixed volumes on the host computer by default. If you do not want everything scanned, you can define the paths to be scanned.
	You can only use a single agent on a local managed host; however local agents provide the best performance and the most functionality.
Remote agent	Remote agents reside on a remote computer other than the managed host, and require a service account with adequate credentials to read the security information.
	Remote agents scan only the configured managed paths on a defined schedule, in order to maximize performance. The default security scanning schedule is daily at 2:00 A.M.
	You can use remote agents on Windows computers, and you must use them on Windows clusters, NetApp devices (with CIFS or NFS file system protocols enabled), EMC devices (with CIFS or NFS file system protocols enabled), Generic host types, and Cloud host types.
	Remote agents cannot collect resource activity on remotely managed Windows, Windows clusters, Generic, or Cloud host types.

NOTE: SharePoint farm agents are remotely managed and require a service account for the agents. They must be installed on a SharePoint server. Ensure that the service account configured for the SharePoint managed host is a SharePoint Farm Account (same account that is used to run the SharePoint timer service).

NOTE: A DFS root managed host does not have an agent installed. Once a root is added as a managed host, the Data Governance server periodically synchronizes the DFS structure into the One Identity Manager database making the DFS path available within the Resource browser. You are able to quickly see where all the data has been replicated throughout your network.

You must have enough free space on the agent computer in the installation directory to store the data collected by the agent. Contact Software Support for details on estimating the disk space usage.

To optimize searches for access points, agents send security index information for resources under managed paths to the Data Governance server for storage in the One Identity Manager database. This allows clients to quickly determine the hosts where detailed access queries are to be directed.

NOTE: All detailed security information for resources placed under governance is sent to the Data Governance server and stored in the One Identity Manager database.

Detailed access information is maintained on the agent computer, only sending general access information to the server.

The server acts as an intermediary between the agents and the databases where information is stored. It coordinates all agent deployments and communication, and

manages the security index for each managed host. Only indexing direct-access points is done for several reasons:

- Security information that is not explicit is, by definition, inherited from a resource higher in the hierarchy. Unless the resource is the managed path, the agent has already indexed the explicit security on the parent resource that is causing the inherited security to be present.

- Not including inherited access points greatly reduces the total size of the index.

- Resources with only inherited access are not interesting from a security standpoint. Data Governance Edition is interested in the resources that have had security applied directly to them.

Deployment best practices

When deploying Data Governance agents, local agents are preferable to remote agents. Local agents reduce network bandwidth and increase responsiveness. When it is not possible to deploy local agents to a system (such as when using a network attached storage device, or a virtual cluster node), the following best practices should be considered:

- When deploying multiple remote agents to an agent host computer, the number of agents a host computer can handle is limited by several factors:

  - The total number of resources being scanned by all hosted agents.

  - The total number of resources with explicit security being indexed by all hosted agents.

  - All the queries that are serviced by agents hosted concurrently are executed on that local hardware.

- Overwhelming the host computer with too many agents can result in slow indexing performance and intermittent failures in agent queries or in indexing operations.

- When deploying remote agents, ensure that the agents are hosted on computers that have low latency, high-bandwidth connections to their targets. This ensures that agents that have real-time change watching enabled will not suffer from periodic watch failures.

- When possible, avoid deploying agents to the computer hosting the Data Governance service itself. The server requires significant network resources to perform its various operations. When agents are deployed to this system, they compete for these network resources. Leaving the server with as few agents as possible ensures that it will not suffer performance degradation due to resource scarcity.

- More than one remote agent may be used to scan remote Windows computers, Windows clusters, and NAS devices. This is useful if the managed host has a large set of managed paths. Multiple agents may not scan the same managed paths.

- Manually installing agents is not supported. You must use the Manager client to deploy and configure Data Governance agents because you need access to the Data Governance application roles within One Identity Manager.

- When adding a remote agent, ensure that a trust exists between:
    - the domains of the agent host and the agent service account
    - the domains of the agent service account and the computer being scanned
- When deploying multiple agents to manage a SharePoint farm, One Identity recommends that you manage the lowest resources in the SharePoint hierarchy that you plan on governing or reporting on. Also, divide these managed resources across as many agent services as your SharePoint server can handle. This will provide the fastest scanning and the least amount of downtime when running reports.

Once you have added a managed host, you can begin to manage the data contained within it. For more information, see Managing unstructured data access on page 123.

Agent leases

Data Governance Edition includes a mechanism that enables the server to determine what agents are functioning without needing each agent to maintain a persistent connection to the Data Governance server.

Every few minutes the agent contacts the server to renew its lease. If the server has not received a lease renewal from an agent in the expected time frame, the agent goes into the "No communication from agent" state. This state indicates that the server is unable to receive information from the agent.

If an agent is in this state, you can attempt to restart the agent. For more information, see Restarting agents on page 121. It is important to understand why the agent allowed its lease to expire. Leases may expire because the agent service stopped unexpectedly or the agent host computer lost its network connection so the agent could not contact the server to renew its lease.

NOTE: You can also review lease expiration information in the Data Governance server log (DataGovernanceEdition.Service.exe.dlog) in the Data Governance service installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\).

For a complete list of possible agent states, see Verifying managed host system status on page 115 or Checking the agent status on page 118.

Adding and configuring managed hosts

Different types of managed hosts behave differently. The following sections provide the steps to configure each type of managed host.

You can add the following host computers as a managed host to your Data Governance Edition deployment:

- Local Windows computer. For more information, see Adding a local managed host (Windows computer) on page 66.

- Windows Cluster/Remote Windows computer. For more information, see Adding a Windows cluster / Windows computer as a remote managed host on page 69.

- Generic resource (that is, a Server Message Block (SMB) share running on any Active Directory joined computer). For more information, see Adding a generic managed host on page 71.

- Distributed File System (DFS) root. For more information, see Adding a Distributed File System (DFS) root managed host on page 75.

- SharePoint farm. For more information, see Adding a SharePoint farm managed host on page 76.

- EMC storage device with CIFS file system protocol enabled. For more information, see Adding an EMC CIFS device as a managed host on page 84.

- NetApp 7-Mode filer with CIFS file system protocol enabled. For more information, see Adding a NetApp CIFS device as a managed host on page 80.

- NetApp Cluster-Mode filer with CIFS file system protocol enabled. For more information, see Adding a NetApp CIFS device as a managed host on page 80.

- EMC Isilon storage device with NFS system protocol enabled. For more information, see Adding an NFS managed host on page 87.

- NetApp 7-Mode filer with NFS file system protocol enabled. For more information, see Adding an NFS managed host on page 87.

- NetApp Cluster-Mode filer with NFS file system protocol enabled. For more information, see Adding an NFS managed host on page 87.

- SharePoint Online resources. For more information, see Adding a cloud managed host on page 91.

- OneDrive for Business resources. For more information, see Adding a cloud managed host on page 91.

Adding a local managed host (Windows computer)

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a local managed host to a Windows computer

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **Windows Computer**.

3. Select **Manage host** from the Tasks view or right-click menu.

   NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will

apply to all selected host computers.

The **Managed Host Settings** dialog appears.

> NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.
>
> Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This is a read-only field displaying the name of the host computer selected on the **Managed hosts** view.

   b. **Host Type**: Select **Local Windows Computer**.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

   > NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

   d. **Keywords**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. By default, local agents scan all local fixed volumes (NTFS devices) on the host computer. To limit the amount of security data being scanned, use the **Managed Paths** page to specify the root of an NTFS directory to be scanned. Once you configure one or more managed paths, only those paths are scanned.

   To add managed paths:

   a. Open the **Managed Paths** page.

   b. Click the **Add** button.

   c. In the **Managed Paths Picker** dialog, select the check box to the left of the directories to be scanned.

   > NOTE: For local managed hosts, the **Agent Selection** field at the bottom of this dialog is pre-populated with the name of the selected target machine.

   d. Click **OK**.

   For more information, see Managed paths page on page 104.

6. By default, local agents begin scanning immediately once deployed. Use the **Security Scanning** page to define a different scanning schedule for the agent.

   For example, to delay the scan to run during off peak hours:

a. Open the **Security Scanning** page.

b. Clear the **Immediately scan on agent restart or when managed paths change** check box.

c. Use the **Scan start time** control to specify the desired time to perform the full scan.

   | NOTE: The **Scan start time** is local agent time.

Review the options at the bottom of the page to determine if the default security scanning behavior needs to be modified:

- **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

- **Collect activity for real-time security updates**: Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

For more information, see Security Scanning page on page 105.

7. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

   IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

a. Open the **Resource Activity** page.

b. Select the **Collect and aggregate events** option.

c. Select the type of events to be collected:

   - Security change
   - Create
   - Delete
   - Rename
   - Write
   - Read (disabled by default)

d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:

   - 5 minutes
   - 1 hour
   - 8 hours (default)
   - 1 day

e. By default, certain well-known system accounts, file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts and objects to be excluded.

NOTE: By default, the Data Governance agent excludes the run as account (LOCAL SYSTEM) from activity collection and aggregation.

For more information, see Resource activity page on page 108.

8. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy a Data Governance Edition agent on the local computer.

By default, the security scan begins immediately upon agent deployment. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a Windows cluster / Windows computer as a remote managed host

You can add Windows servers and Windows clusters as managed hosts, with remote agents. However, you cannot collect resource activity for these types of remote managed hosts.

NOTE: Only Windows failover cluster configurations are supported.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a Windows cluster or Windows computer managed host with a remote agent

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **Windows Computer**.

3. Select **Manage host** from the Tasks view or right-click menu.

NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

The **Managed Host Settings** dialog appears.

NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to

the domain and adds it to the managed domains list.

Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This is a read-only field displaying the name of the host computer selected on the **Managed hosts** view.

   b. **Host Type**: Select **Windows Cluster / Remote Windows Computer**.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

      NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

   d. **Keywords**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

   To add a remote agent:

   a. Open the **Agents** page.

   b. **Select the agent**: Select the agent host computer to be used to scan the target computer.

   c. **Select the service account**: Select a service account with sufficient permissions to access the target computer and the agent host.

      An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.

   d. Click the **Add** button to add the agent to the agents list.

      TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

      For more information, see Agents page on page 103.

6. Use the **Managed Paths** page to specify the roots of the NTFS directory tree to be scanned by the agent.

   To add managed paths:

   a. Open the **Managed Paths** page.

   b. Click the **Add** button.

c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

> NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see .

7. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** tab to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

a. Open the **Security Scanning** page.

b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

c. Use the check boxes at the bottom of the page to modify the default security scanning behavior:

- **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.

- **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

- **Collect activity for real-time security updates**: Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

For more information, see .

8. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a generic managed host

You can remotely scan managed hosts (other than those on the supported list) by adding a "generic" managed host. This type of managed host supports scheduled scans only and does not support real-time security updates or resource activity collection.

NOTE: These hosts must be accessible through Windows shares. To determine if a host can be scanned for security information, you can use the Filesystem Statistics Utility (QAM.Server.FileSystemStatistics.exe) that is included with a Data Governance Edition installation. It scans a file system, enumerates its contents, and provides statistics on the files and folders contained on the specified data roots.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a generic managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.

   NOTE: If you do not see the host you want to manage listed, edit the Data Governance service configuration file (DataGovernanceEdition.Service.exe.config) as follows:

   - Locate the `customHostParameters` section.

     ```
     <customHostParameters>

         <additionalOperatingSystems>

             <!--<operatingSystem value="MyOperatingSystem"/>-->

         </additionalOperatingSystems>

     </customHostParameters>
     ```

   - Remove the commented `operatingSystem` line and replace it with a line that specifies the operating system value for the host you want to manage. That is, the string found in the ADSMachine.OperatingSystem field. For example, if the host you want to manage has the operating system field "MyOS", edit this setting as follows:

     ```
     <customHostParameters>

         <additionalOperatingSystems>

             <operatingSystem value="MyOS"/>

         </additionalOperatingSystems>

     </customHostParameters>
     ```

     This will include all machines that contain the string "MyOS" in its operating system field.

   - If you want to specify an exact match, include the `isExact` parameter as follows:

     ```
     <customHostParameters>

         <additionalOperatingSystems>

             <operatingSystem value="MyOS" isExact="true"/>

         </additionalOperatingSystems>

     </customHostParameters>
     ```

All of the hosts found using this filter will now appear in the Managed Host view as **Unknown** host type.

2. In the Managed hosts view (right pane), select a host with the status of **Not Managed** and a host type of **Unknown**.

3. Select **Manage host** from the Tasks view or right-click menu.

   NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

   The **Managed Host Settings** dialog appears.

   NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

   Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.

   b. **Host Type**: Select **Generic Host Type**.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example C:\Mypath) and cannot exceed 512 characters.

      NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance Server installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

      If there is an existing agent, you cannot install another agent with a different installation directory. All agents must be installed in the same directory.

   d. **Keywords**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

   To add a remote agent:

   a. Open the **Agents** page.

   b. **Select the agent**: Select the agent host computer to be used to scan the target computer.

   c. **Select the service account**: Select a service account with sufficient permissions to access the target computer and the agent host.

An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.

   d. Click the **Add** button to add the agent to the agents list.

   TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

   For more information, see Agents page on page 103.

6. Use the **Managed Paths** page to specify the roots of the NTFS directory tree to be scanned by the agent.

   To add managed paths:

   a. Open the **Managed Paths** page.

   b. Click the **Add** button.

   c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

   NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

   d. Click **OK** to save your selections and close the dialog.

   The selected paths, including those that are excluded, appear on the **Managed Paths** page.

   For more information, see Managed paths page on page 104.

7. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** page to change the time and frequency with which the agent scans the target computer.

   To modify the scanning schedule and settings:

   a. Open the **Security Scanning** page.

   b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

   c. Use the check boxes at the bottom of the page to modify the default security scanning behavior:

      • **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.

- **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

For more information, see .

8. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a Distributed File System (DFS) root managed host

Adding a DFS root enables you to view and manage the access on resources that are physically distributed throughout your network.

TIP: As of Data Governance Edition version 7.0.1, you can perform additional managed host tasks against DFS links, such as:

- Target existing reports, including the Resource Access and Resource Activity reports

- Calculate perceived owners

- Place a DFS link under governance; adding the DFS link to the **Governed data** view and making the usual menu options available

- Publish a DFS link to the IT Shop; making it available to others through a resource access request

Once added, the Data Governance server periodically synchronizes the DFS structure into the One Identity Manager database making the DFS path available within the **Resource browser**. You are able to quickly see where all the data has been replicated throughout your network.

This information is also available within the resource access, resource activity, and account activity reports if the underlying resource is being scanned on another activity enabled host.

NOTE: In order for a DFS link, target share path or folder to be placed under governance or published to the IT Shop, both the DFS server hosting the DFS namespace and the share server where the DFS link is pointing to must be added as managed hosts. If the required servers (those that contain DFS security details) are not already managed, a message box appears listing the servers that need to be added as managed hosts. Click the **Add managed hosts with default options** button to deploy a local agent to the servers listed in the message box and complete the selected operation. Click **Cancel** to cancel the selected operation and manually add the servers as managed hosts.

NOTE: By default, the Data Governance server synchronizes DFS every 24 hours, you can force an immediate synchronization using Windows PowerShell or you can alter the synchronization interval through a configuration file setting.

To force an immediate DFS synchronization, run the following PowerShell cmdlet:

```
Trigger-QDfsSync [-ManagedHostID] <String> [<CommonParameters>]
```

You must specify the ID (GUID format) of the DFS managed host to be synchronized. To synchronize all of your DFS managed hosts, set the -ManagedHostId to All.

To change the default synchronization interval, add or modify the following setting in DataGovernanceEdition.Service.exe.config file (which is located in the Data Governance server installation directory):

```
<add key="DFSDataSyncInterval" value="1440"/>
```

The value specified is interpreted as minutes. If this value is not present, the default is 24 hours.

To add a DFS root managed host

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. From the **Managed hosts** view (right pane), select **Manage DFS host** from the Tasks view or right-click menu.

3. In the **DFS Managed Host Settings** dialog, select the following information:

   - **DFS Domain**: Select the DFS domain.

   - **DFS Root**: Click the **Select Root** button to display a list of available DFS roots within the selected domain. Select a root from the list and click **OK**.

   Click **OK** to save your selections and close the dialog.

4. Back in the Manager, click the **Save** toolbar button to add the DFS root managed host.

Adding a SharePoint farm managed host

SharePoint farms are similar to remote managed hosts in that they require an associated service account, even though they are installed locally on a SharePoint server. You have the option of selectively including and excluding objects to be scanned by one or more agent services on the SharePoint server.

NOTE: Before adding a SharePoint managed host, ensure that the following configuration steps have been completed:

- Install a One Identity Manager service (job server) on a dedicated SharePoint Application Server in the SharePoint farms to be monitored. Ensure that the One Identity Manager service account is running as the SharePoint farm account (same account that is used to run the SharePoint timer service).

- On the Data Governance server, run the One Identity Manager Synchronization Editor to set up a synchronization project to load your Active Directory objects into the One Identity Manager database. For more information, see the *One Identity Manager Administration Guide for Connecting to Active Directory.*

- On the SharePoint farm server, run the One Identity Manager Synchronization Editor to set up a synchronization project to load your SharePoint objects into the One Identity Manager database. For more information, see the *One Identity Manager Administration Guide for Connecting to SharePoint*.

- Also, check/configure the master data (task in Manager) for the service account.

Once the SharePoint synchronization project has completed, the **Managed hosts** view is updated to include any SharePoint farms that are available for scanning.

To add a SharePoint farm as a managed host

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **SharePoint Farm**.

3. Select **Manage host** from the Tasks view or right-click menu.

   The **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.

   b. **Host Type**: This is a read-only field displaying the type of host computer selected in the **Managed hosts** view.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

      NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

   d. **Keywords**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the service account to be used to access the SharePoint farm and the agent services to be used to scan the SharePoint farm.

   To add an agent service:

   a. Open the **Agents** page.

   b. **Agent Service Account**: Select the service account that has the required rights for the selected SharePoint farm.

      The service account must be the SharePoint farm account (same account that is used to run the SharePoint timer service and the One Identity Manager

service (job server)). The SharePoint farm account also needs to be added to the local Administrators group on the SharePoint server.

   c. Click the **Add** button to add the agent service to the agents list.

     Repeat to add additional agent services to be used to scan the selected SharePoint farm.

     For more information, see Agents page on page 103.

6. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

7. Back on the **Managed hosts** view, select the newly deployed SharePoint managed host, and select the **Edit host settings** task or right-click command.

   The **Managed Host Settings** dialog appears allowing you to configure the additional settings required for a SharePoint managed host.

8. Use the **Managed Paths** page to specify the point within your SharePoint farm hierarchy to begin scanning.

   To add managed paths:

     a. Open the **Managed Paths** page.

     b. Click the **Add** button.

     c. In the **Managed Paths Picker** dialog, click the check box to the left of the component within your SharePoint farm hierarchy to be scanned.

> NOTE: When using multiple agent services to monitor a SharePoint managed host, select the managed path to be monitored and then select an agent service from the **Agent Selection** drop-down menu. Repeat this process for all of the paths to be monitored. An agent service can monitor multiple paths; however, multiple agent services cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the name of the agent service selected to scan the different paths.

     d. Click **OK** to save your selections and close the dialog.

   The selected paths and assigned agent service are displayed on the **Managed Paths** page.

   For more information, see Managed paths page on page 104.

9. By default, SharePoint agents scan daily at 2:00 A.M. Use the **Security Scanning** page to set the time and frequency with which the agent scans the target computer.

   To modify the scanning schedule and settings:

     a. Open the **Security Scanning** page.

     b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

     c. Use the options at the bottom of the page to modify the default security scanning behavior:

- **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
- **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

For more information, see Security Scanning page on page 105.

10. By default resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection and aggregation.

NOTE: To gather and report on resource activity in SharePoint, ensure that SharePoint native auditing is configured for any resources of interest. For more information, see Configure SharePoint to track resource activity on page 239.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

a. Open the **Resource Activity** page.

b. Select the **Collect and aggregate events** option.

c. Select the type of events to be collected:
  - Security change
  - Create
  - Delete
  - Rename
  - Write
  - Read (disabled by default)

d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
  - 5 minutes
  - 1 hour
  - 8 hours (default)
  - 1 day

e. By default, certain well-known accounts are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts to be excluded.

NOTE: The agent service account is not included in this exclusion list by default. You will need to add that manually for SharePoint managed hosts.

For more information, see Resource activity page on page 108.

11. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the SharePoint resources on the target managed host using the **Resource browser**. Double-click the managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a NetApp CIFS device as a managed host

You can add supported NetApp storage devices as managed hosts, with remote agents. This procedure covers NetApp 7-Mode devices and NetApp Cluster-Mode devices running OnTap with the CIFS file system protocol enabled. See Additional configuration for NetApp filers on page 234 before adding a NetApp managed host.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a NetApp CIFS device as a managed host

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **NetApp OnTap 7 Mode CIFS Device** or **NetApp OnTap Cluster Mode CIFS Device**.

3. Select **Manage host** from the Tasks view or right-click menu.

   NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

   The **Managed Host Settings** dialog appears.

   NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

   Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.

   b. **Host Type**: This is a read-only field displaying the type of host computer selected in the **Managed hosts** view.

c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

d. **Keyword**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. For NetApp OnTap Cluster Mode CIFS managed hosts, use the **Credentials** page to enter the credentials of a user with access to the target NAS host computer:

a. **User Name**: Enter the name of a user account with access to the target NAS host computer.

NOTE: The user must have the "ontapi" User Login Method application.

b. **Password**: Enter the password associated with the user account entered above.

c. **Port**: Enter the destination port to be used for communication between the agent and target NAS host computer. The default value is 443.

d. **Host EndPoint**: (Optional) Enter the API endpoint (FQDN, host name or IP address) for the NetApp Cluster Mode connection.

NOTE: The default is to use the FQDN of the targeted host. You would only use this setting if the API connection needs to be specified as something other than the FQDN of the targeted host.

e. Click the **Test API Credentials** button to verify valid credentials have been entered.

6. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

To add a remote agent:

a. Open the **Agents** page.

b. **Select the agent**: Select the agent host computer to be used to scan the target computer.

c. **Select the service account**: Select a service account with sufficient permissions to access the target computer and the agent host.

An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.

d. Click the **Add** button to add the agent to the agents list.

> **TIP:** For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.
>
> For more information, see Agents page on page 103.

7. Use the **Managed Paths** page to specify the roots of the NTFS directory tree to be scanned by the agent.

    To add managed paths:

    a. Open the **Managed Paths** page.

    b. Click the **Add** button.

    c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

    > **NOTE:** When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

    d. Click **OK** to save your selections and close the dialog.

    The selected paths appear on the **Managed Paths** page.

    For more information, see Managed paths page on page 104.

8. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** page to change the time and frequency with which the agent scans the target computer.

    To modify the scanning schedule and settings:

    a. Open the **Security Scanning** page.

    b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

    c. Use the options at the bottom of the page to modify the default security scanning behavior:

        • **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.

        • **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

        • **Collect activity for real-time security updates**: Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

    For more information, see Security Scanning page on page 105.

9. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

> IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

a. Open the **Resource Activity** page.

b. Select the **Collect and aggregate events** option.

c. Select the type of events to be collected:

- Security change
- Create
- Delete
- Rename
- Write
- Read (disabled by default)

d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:

- 5 minutes
- 1 hour
- 8 hours (default)
- 1 day

e. By default, certain well-known system accounts, file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts and objects to be excluded.

> NOTE: By default, the Data Governance agent excludes the domain service account from activity collection and aggregation.

For more information, see Resource activity page on page 108.

10. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding an EMC CIFS device as a managed host

You can add EMC storage devices as managed hosts, with remote agents. This procedure covers NAS devices running EMC Celerra/VNX or EMC Isilon operating systems with the CIFS file system protocol enabled. See Additional configuration for an EMC storage device on page 230 before adding an EMC managed host.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add an EMC CIFS device as a managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **EMC Celerra/VNX Device** or **EMC Isilon Device**.

3. Select **Manage host** from the Tasks view or right-click menu.

   NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

   The **Managed Host Settings** dialog appears.

   NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

   Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.

   b. **Host Type**: This is a read-only field displaying the type of host computer selected in the **Managed hosts** view.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

      NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

   d. **Keyword**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

   To add a remote agent:

   a. Open the **Agents** page.

   b. **Select the agent**: Select the agent host computer to be used to scan the target computer.

   c. **Select the service account**: Select a service account with sufficient permissions to access the target computer and the agent host.

      An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.

   d. Click the **Add** button to add the agent to the agents list.

      | TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

      | NOTE: If you are collecting resource activity (**Collect and aggregate events** on the **Resource Activity** page) or real-time security updates (**Collect activity for real-time security updates** on the **Security Scanning** page), you can only specify one agent to scan the EMC storage device.

      For more information, see Agents page on page 103.

6. Use the **Managed Paths** page to specify the roots of the NTFS directory trees to be scanned by the agent.

   To add managed paths:

   a. Open the **Managed Paths** page.

   b. Click the **Add** button.

   c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

      | NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

   d. Click **OK** to save your selections and close the dialog.

   The selected paths appear on the **Managed Paths** page.

   For more information, see Managed paths page on page 104.

7. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** page to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

   a. Open the **Security Scanning** page.

   b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

   c. Use the options at the bottom of the page to modify the default security scanning behavior:

   - **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.

   - **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

   - **Collect activity for real-time security updates**: Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

      NOTE: If you enable **Collect activity for real-time security updates**, ensure your EMC device is configured for auditing. For more information, see Additional configuration for an EMC storage device on page 230.

   For more information, see Security Scanning page on page 105.

8. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

   IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

   To configure resource activity collection and aggregation:

   a. Open the **Resource Activity** page.

   b. Select the **Collect and aggregate events** option.

   c. Select the type of events to be collected:

   - Security change

   - Create

   - Delete

   - Rename

   - Write

   - Read (disabled by default)

d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:

- 5 minutes
- 1 hour
- 8 hours (default)
- 1 day

e. By default, certain well-known system accounts, file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts and objects to be excluded.

   NOTE: By default, the Data Governance agent excludes the domain service account from activity collection and aggregation.

Click the **View/Update cepp.conf** button to check the status or modify the cepp.conf file. Selecting this button displays a **Logon Credentials** dialog allowing you to enter the IP address or hostname and credentials of the EMC Celerra/VNX control station and select the data mover that holds the managed paths to be scanned.

- Once the cepp.conf is retrieved and displayed, you can edit the Proposed cepp.conf file (lower pane). Select the **Update File** button to save your edits, which will be sent to the EMC device.

   NOTE: The cepp service will be stopped and restarted for the selected data mover to apply the new cepp.conf file.

- Use the **Check Status** button to check the status of the current cepp.conf file.

For more information, see Resource activity page on page 108.

9. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding an NFS managed host

Data Governance Edition supports the scanning of NAS devices with NFS file system protocol enabled, including NetApp 7-Mode, NetApp Cluster and EMC Isilon devices.

NOTE: Before adding an NFS managed host, ensure the following configuration steps have been completed:

- During the One Identity Manager installation process and Data Governance configuration process, add the optional Unix module.

- During the One Identity Manager Data Governance Edition installation process, ensure the One Identity Manager service (job server) is configured properly and that the UNIX connector server function is selected.

- Run the One Identity Manager Synchronization Editor to set up a synchronization project to load your UNIX objects into the One Identity Manager database.

For EMC Isilon NFS managed hosts:

- On the Data Governance server and all agent servers, you must have a Trusted Root Certificate Authority certificate to validate the Isilon server's HTTP certificate. See the EMC Isilon Web Administration Guide for details.

- The service account for an agent managing EMC Isilon storage devices, must have "run as root" permissions on the Isilon SMB share to be managed (that is, selected as a managed path).

For NetApp 7-Mode NFS managed hosts (does NOT apply to Cluster Mode devices):

- The service account for an agent managing NetApp 7-Mode filers must be a member of the local Administrators group on the NetApp filer in order to create FPolicy. This account must also have permissions to access folders being scanned.

- Monitoring real-time security updates and collecting resource activity requires FPolicy; and in order to use FPolicy, the CIFS file system protocol must be enabled for NetApp 7-Mode devices.

Adding a NFS managed host

1. In the **Navigation** view, select **Data Governance** | **Managed hosts**.

2. From the **Managed hosts** view, select **Manage NFS host** from the Tasks view or right-click menu.

   The **Managed Host Settings** dialog appears.

3. At the top of the dialog, specify the following information:

   a. **Managed Host**: Enter the IP address or the fully qualified domain name of the NFS host computer to be managed.

   b. **Host Type**: Select **NetApp Cluster NFS Device**, **NetApp 7-Mode NFS Device**, or **EMC Isilon NFS Device**.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

      NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

   d. **Keywords**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

4. Open the **NIS Host** page to specify the NIS server whose users and groups have been synchronized with One Identity Manager.

5. Open the **Credentials** page and enter the credentials of a user with access to the target NAS host computer:

   a. **User Name**: Enter the name of a user account with access to the target NAS host computer.

   b. **Password**: Enter the password associated with the user account entered above.

   c. **Port**: Enter the destination port to be used for communication between the agent and target NAS host computer.

      - NetApp filers: The default value is 443.

      - EMC devices: The default value is 8080.

   Click the **Test API Credentials** button to verify valid credentials have been entered.

   For more information, see Credentials page on page 101.

6. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

   To add a remote agent:

   a. Open the **Agents** page.

   b. **Select the agent**: Select the agent host computer to be used to scan the target computer.

   c. **Select the service account**: Select a service account with sufficient permissions on the selected agent host.

      Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.

   d. Click **Add** to add the agent to the agents list.

      > TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

   For more information, see Agents page on page 103.

7. Use the **Managed Paths** page to specify the directories to be scanned by the agent to create and maintain the security index.

   To add managed paths:

   a. Open the **Managed Paths** page.

   b. Click the **Add** button.

   c. In the **Managed Paths Picker** dialog, select the check box to the left of the directories to be scanned.

NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

    d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see .

8. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** tab to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

    a. Open the **Security Scanning** page.

    b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

    c. Review the options at the bottom of the page to modify the default security scanning behavior:

- **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.

- **Collect activity for real-time security updates**: Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

    NOTE: Collecting real-time security updates is not available for EMC Isilon NFS devices.

    NOTE: For NetApp 7-Mode managed hosts, real-time security updates and resource activity collection requires FPolicy. In order to use FPolicy, CIFS file system protocol must be enabled.

For more information, see .

9. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

NOTE: Collecting resource activity is not available for EMC Isilon NFS devices.

To enable and configure resource activity collection and aggregation:

a. Open the **Resource Activity** page.

b. Select the **Collect and aggregate events** option.

c. Select the type of events to be collected:
   - Security change
   - Create
   - Delete
   - Rename
   - Write
   - Read (disabled by default)

d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
   - 5 minutes
   - 1 hour
   - 8 hours (default)
   - 1 day

e. By default, certain file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the objects to be excluded.

   For more information, see Resource activity page on page 108.

10. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a cloud managed host

Data Governance Edition supports the scanning of folders hosted on SharePoint Online and OneDrive for Business.

NOTE: Before adding a cloud managed host, One Identity Manager must be configured to use Azure Active Directory and SharePoint Online. See the following One Identity Manager documents for instructions on configuring and synchronizing the data from these target systems with the One Identity Manager Service:

- *One Identity Manager Administration Guide for Connecting to Azure Active Directory*
- *One Identity Manager Administration Guide for Connecting to SharePoint Online*

These One Identity Manager documents can be found on the One Identity support site: https://support.oneidentity.com/identity-manager/technical-documents

To add a cloud managed host

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. In the **Managed hosts** view, select **Manage Cloud host** from the Tasks view or right-click menu.

   You are redirected to Microsoft to sign in to your account and grant access to Office 365 data.

3. On Microsoft's **Sign in to your account** dialog, enter the administrator account login credentials to be used to authenticate with the Data Governance Edition API cloud proxy.

   NOTE:Data Governance Edition only supports one Office 365 domain per cloud provider at this time. That is, you can deploy only one managed host for the SharePoint Online administrator account and one managed host for the OneDrive for Business administrator account. Data Governance Edition does not currently block you from deploying a second SharePoint Online or OneDrive for Business managed host; however, it will not work.

   NOTE: You must use a separate administrator account for this purpose. This administrator account must be, or have equal access as, a SharePoint Online Administrator. Each site will be modified to list this account as a Site Collection Administrator for the site. This provides the account with access to the site's contents.

   a. **Email, phone, or Skype**: Enter the email address of the administrator account to be used to grant access to your Office 365 domain. For example: Administrator@MyDomain.onmicrosoft.com.

      Click **Next**.

   b. **Password**: Enter the password associated with the specified email.

      Click **Sign In**.

   After successfully signing in, the **Managed Host Settings** dialog appears allowing you to configure your cloud managed host.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

   a. **Managed Host**: This field will remain blank.

   b. **Host Type**: Select the type of cloud provider: **SharePoint Online** or **OneDrive for Business**.

   c. **Agent Install Path**: (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

      NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

d. **Keywords**: (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. The **Cloud Provider** page displays a green check mark and message indicating you are authenticated with your Office 365 domain. If you do not see this green check mark and authentication message, use the **Re-authenticate** button to authenticate with the cloud API proxy.

6. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

   | NOTE: You can only specify one agent to scan a cloud host.

   To add a remote agent:

   a. Open the **Agents** page.

   b. **Select the agent**: Select the agent host computer to be used to scan the target managed host.

   c. **Select the service account**: Select a service account with sufficient permissions on the selected agent host.

      Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.

   d. Click **Add** to add the agent to the agents list.

   For more information, see Agents page on page 103.

7. Use the **Managed Paths** page to specify the folders under the Documents site to be to be scanned by the agent to create and maintain the security index.

   NOTE: OneDrive for Business support is limited to the Documents folder for the Administrator account. Therefore, all managed paths are selected within the scope of the Administrator's Documents folder.

   For SharePoint Online, a site is available for managing, only if it can be navigated on the SharePoint Online website.

   To add managed paths:

   a. Open the **Managed Paths** page.

   b. Click the **Add** button.

   c. In the **Managed Paths Picker** dialog, click the check box to the left of the folders to be scanned.

      TIP: A check box appears to the left of the folders that can be selected. Click the expansion box to the left of a container to expand it and navigate to the folders available for scanning.

   d. Click **OK** to save your selections and close the dialog.

   The selected paths appear on the **Managed Paths** page.

   For more information, see Managed paths page on page 104.

8. By default, remote agents scan cloud-based managed hosts daily at 2:00 A.M. Use the **Security Scanning** page to set the time and frequency with which the agent scans the target computer.

   To modify the scanning schedule and settings:

   a. Open the **Security Scanning** page.

   b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.

   c. Use the options at the bottom of the page to modify the default security scanning behavior:

      - **Immediately scan on agent restart or when managed paths change**: Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.

      - **Ignore all files and only store folder security data**: Clear this check box if you want to include file security data in the security index.

   For more information, see Security Scanning page on page 105.

9. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the resources on the target managed host using the **Resource browser**. Double-click the managed host in the **Managed hosts** view to display the **Resource browser**.

Managed host configuration settings

Managed hosts must be properly configured for security scanning (and resource activity collection, if applicable) to begin. An agent must be configured to communicate with the server and gather resource information. Until this is completed, no security information will be stored or indexed for this computer. Agents are configured when you add or edit a managed host.

- Real-time security updates in the context of Data Governance Edition refers to the monitoring of changes to the file system caused by create, delete, and rename operations, as well as DACL, SACL and Owner changes, in order to maintain the security index. These real-time security updates are not monitored by default, but can be configured on the **Security Scanning** page of the **Managed Host Settings** dialog.

  NOTE: Enabling real-time security updates for NAS devices requires additional configuration on the NAS device itself. For more information, see Additional configuration for an EMC storage device on page 230 and Additional configuration for NetApp filers on page 234.

- When enabled, resource activity is collected in real time, compressed, and then stored in the Data Governance Resource Activity database. Historical activity data

can then be used to calculate a resource's perceived owner and to generate activity-related reports. Use the **Resource Activity** page of the **Managed Host Settings** dialog to enable and configure resource activity collection and aggregation.

- Managed paths will be scanned for security access information and if enabled, for collecting resource activity.

The available configuration settings vary depending on the type of managed host, as shown in the following table. Yes indicates that the settings can be configured.

Table 33: Configurable managed host settings

Managed host type	Resource activity	Real-time security updates	Security scanning	Managed paths	Service accounts
Local Windows Computer	Yes Not collected by default.	Yes Not monitored by default.	Yes By default, scanning starts immediately once an agent is deployed.	Yes By default, all NTFS drives are scanned if no managed paths are specified.	No service account is required as the agent runs as the Local System.
Windows Cluster / Remote Windows Computer	N/A	Yes Not monitored by default.	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account with Local Administrator rights on the managed host. The agent scanning the host runs under the service account.
NetApp 7-Mode and Cluster-Mode CIFS Devices NetApp 7-Mode and Cluster Mode NFS Devices	Yes Not collected by default. Requires FPolicy	Yes Not monitored by default.	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account; must be a member of the local Administrators group on the NetApp 7-Mode filer in order to create FPolicy. This account must also have permissions to

Managed host type	Resource activity	Real-time security updates	Security scanning	Managed paths	Service accounts
					access folders being scanned.
EMC CIFS Devices	Yes Not collected by default.	Yes Not monitored by default.	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account with required permissions. The agent scanning the host runs under the service account. The service account for an agent managing EMC Isilon storage devices, must have "run as root" permissions on the Isilon SMB share to be managed (that is, selected as a managed path).
EMC Isilon NFS Devices	N/A	N/A	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account; must have "run as root" permissions on the Isilon SMB share to be managed (that is, selected as a managed path).
SharePoint Farm	Yes Not collected by default.	N/A	Yes Scanning starts on a configured schedule. By default, every day of	Yes Managed paths must be defined for scanning to occur.	Requires a service account; must be the SharePoint farm account (same account that is used to run the

Managed host type	Resource activity	Real-time security updates	Security scanning	Managed paths	Service accounts
			the week at 2:00 A.M.		SharePoint timer service and the One Identity Manager service (job server)); must be a member of the administrators group on SharePoint server. The agent scanning the host runs under the service account.
Cloud (for example, SharePoint Online)	N/A	N/A	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account which becomes the agent run as account. This account is not used to connect to the Cloud provider.
Generic	N/A	N/A	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account with required permissions. The agent scanning the host runs under the service account.
Distributed File System	Yes Not collected by default.	N/A	N/A	N/A	N/A

Managed host settings dialog

The **Managed Host Settings** dialog allows you to define the configuration settings for new managed hosts. This dialog appears when you select one of the following tasks from the **Managed hosts** view:

- Manage host
- Manage multiple hosts
- Manage NFS host
- Manage Cloud host
- Edit host settings

This dialog contains the following controls.

Table 34: Managed Host Settings dialog: Controls

Control	Description
Managed Host	Specifies the managed host to be added.
	• For local managed hosts, this is a read-only field that displays the name of the host computer selected in the **Managed hosts** view.
	• For remote managed hosts, including supported EMC and NetApp storage devices with CIFS file system protocol enabled, this is a read-only field that displays the name of the host computer selected in the **Managed hosts** view.
	• For cloud managed hosts, this field is blank when using the **Manage Cloud host** task. However, it displays the *<DomainName>*.onmicrosoft.com host name when using the **Edit host settings** task.
	• If multiple hosts are selected, **<Multiple Managed Hosts>** appears in this field.
	• For NFS managed hosts, enter the IP address or fully qualified domain name of the NFS host computer to be managed.
Host Type	Select the type of managed host to be added to the Data Governance Edition deployment.
	When using the **Manage host** or **Manage multiple hosts** task, the options available depend on the host computer selected in the **Managed hosts** view. Valid managed host types include:
	• EMC Celerra/VNX Device
	• EMC Isilon Device
	• Generic Host Type
	• Local Windows Computer

Control	Description
	• NetApp OnTap Cluster Mode CIFS Device
	• NetApp OnTap 7-Mode CIFS Device
	• SharePoint Farm
	• Windows Cluster/Remote Windows Computer
	When using the **Manage NFS host** task, you must select one of the following host types:
	• EMC Isilon NFS Device
	• NetApp Cluster NFS Device
	• NetApp 7-Mode NFS Device
	When using the **Manage Cloud host** task, you must select one of the following host types:
	• SharePoint Online
	• OneDrive for Business
	When using the **Edit host settings** task, this is a read-only field that specifies the type of host.
Agent Install Path	By default, the agent will be installed in the Data Governance Server installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).
	When you deploy an individual agent, you can use this field to specify an alternate agent installation. To specify an alternate installation directory, enter a local path (for example C:\Mypath) that does not exceed 512 characters.
	NOTE: If there is an existing agent on the machine, you cannot install another agent with a different installation directory. All agents must be installed in the same directory.
	NOTE: If required, use the **Customize default host settings** task to define an alternate default installation directory for deploying new agents. When you opt to set the installation directory for an individual agent using the **Agent Install Path** field on the **Managed Host Settings** dialog, it will take precedence over the default agent installation location defined on the **Customize default host settings** dialog.
Keywords	(Optional) Enter a keyword which can then be displayed and used to group your managed hosts on the **Managed hosts** view.
NIS Host	Use the **NIS Host** page to select the Network Information Systems (NIS) server whose users and groups have been synchronized with One Identity Manager.

Control	Description
	NOTE: This page only applies to NFS managed hosts.
	For more information, see NIS Host page on page 101.
Credentials page	Use the **Credentials** page to provide user credentials that can establish a connection with the NAS device.
	• For NetApp hosts, the user must have the "ontapi" User Login Method application.
	• For EMC hosts, this account must have the "Platform API" privileges applied.
	NOTE: This page only applies to NFS managed hosts and NetApp OnTap Cluster Mode CIFS managed hosts.
	For more information, see Credentials page on page 101.
Cloud Provider	The **Cloud Provider** page indicates if you are successfully authenticated with the Data Governance Edition API cloud proxy and can also be used to re-authenticate to the cloud proxy.
	NOTE: This page only applies to Cloud managed hosts.
	For more information, see Cloud Provider page on page 102.
Agents page	Use the **Agents** page to configure the agents to be used to monitor a remote managed host or SharePoint managed host.
	NOTE: This page only applies to remote managed hosts and SharePoint managed hosts.
	For more information, see Agents page on page 103.
Managed Paths page	Use the **Managed Paths** page to define the paths to be managed by Data Governance Edition. These managed paths will be scanned for security access information and if enabled, for collecting resource activity.
	Click the **Add** button to display the **Managed Paths Picker dialog**, where you can then navigate to and select the paths to be scanned.
	For more information, see Managed paths page on page 104.
Security Scanning page	Use the **Security Scanning** page to set the schedule and settings for scanning agents for changes to the structure and security of the file system.
	For more information, see Security Scanning page on page 105.
Resource activity page	Use the **Resource Activity** page to configure the collection and aggregation of resource activity for the target managed host.
	NOTE: Not available for Windows Cluster/Remote Windows Computer, Generic, or Cloud managed hosts.

Control	Description
	For more information, see Resource activity page on page 108.
OK	Click the **OK** button to save your selections and close the dialog.
Cancel	Click the **Cancel** button to close the dialog without saving your selections.

NIS Host page

Select a Network Information Service (NIS) server whose users and groups have been synchronized with One Identity Manager.

NOTE: This page only applies to NFS managed hosts.

Table 35: NIS Host page: Controls and settings

Control/setting	Description
NIS Host	Select the NIS server to be managed.
	The NIS servers previously synchronized with One Identity Manager (UNIX synchronization project) are listed in the drop-down menu.

Credentials page

Provide the credentials of a user which can establish a connection to the NAS storage device.

- For NetApp devices, this user account must have the 'ontapi' User Login Method application.
- For EMC Isilon devices, this user account must be assigned the 'Platform API' privilege.

NOTE: This page only applies to NFS managed hosts and NetApp OnTap Cluster Mode CIFS managed hosts.

Table 36: Credentials page: Controls and settings

Control/setting	Description
User Name	Enter the name of a user account with access to the target NAS storage device.
Password	Enter the password associated with the specified user account.
Port	Enter the destination port to be used for communication between the agent and target NAS storage device. • NetApp filers: The default value is 443.

ONE IDENTITY
by Quest

Control/setting	Description
	• EMC devices: The default value is 8080.
Host EndPoint	Optionally, enter the API endpoint for the NetApp Cluster Mode connection. This could be an FQDN, host name or IP address.
	The default is to use the FQDN of the targeted host. You would only use this setting if the API connection needs to be specified as something other than the FQDN of the targeted host.
	NOTE: Only applies to NetApp Cluster Mode devices.
Test API Credentials	Click this button to verify that the credentials entered are valid.

Cloud Provider page

The **Cloud Provider** page appears when managing a cloud resource. This page indicates if you are successfully authenticated with the Data Governance Edition API cloud proxy. You can also use this page to re-authenticate to the API cloud proxy. This API cloud proxy provides a consistent method for Data Governance Edition to interface with different cloud providers. When valid login credentials are provided, the system issues an access token which is used during the current and subsequent sessions to access resources hosted by the specified cloud provider.

NOTE: This page only applies to Cloud managed hosts.

Clicking the **Re-authenticate** button redirects you to Microsoft to sign in to your account and grant access to Office 365 data.

On Microsoft's **Sign in to your account** dialog, enter the following information:

1. **Email, phone, or Skype**: Enter the email address of the administrator account to be used to authenticate with the cloud proxy.

   For example: Administrator@MyDomain.onmicrosoft.com

   NOTE: You must create a separate administrator account for this purpose. This administrator account must be, or have equal access as, a SharePoint Online Administrator. Each site will be modified to list this account as a Site Collection Administrator for the site. This provides the account with access to the site's contents.

   For SharePoint Online, create a separate Global Administrator account.

   Click **Next**.

2. **Password**: Enter the password associated with the specified email account.

   Click **Sign in**.

Once signed in, Data Governance Edition will have access to the specified resources for all users in your organization; no other user will be prompted to enter credentials.

Agents page

Use the **Agents** page of the **Managed Hosts Settings** dialog to configure the agents to be used to monitor remote managed hosts and SharePoint farms. Once an agent is deployed, use the Agents view to check its status and performance metrics.

NOTE: For EMC managed hosts, if you are collecting resource activity (**Collect and aggregate events** on the **Resource Activity** page) or real-time security updates (**Collect activity for real-time security updates** on the **Security Scanning** page), you can only specify one agent to scan the EMC storage device.

NOTE: You can only specify one agent to scan a cloud host.

Table 37: Agents page: Remote managed hosts

Control/setting	Description
Select the agent	Select the agent host computer to be used to monitor the target computer.
Select the service account	Select the service account with sufficient permissions to access both the target computer and the agent host.
	An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.
Add	After selecting the agent and service account, click the **Add** button to add it to the Agent list.
Remove	Select an agent from the Agents list and click the **Remove** button to remove it from the Agent list.
	Removing the selected agent also removes the configured managed paths for the agent.
Agent list	Displays the agents selected to monitor the target computer.
	For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

Table 38: Agents page: SharePoint farm managed hosts

Control/setting	Description
Agent Service Account	Select the service account with sufficient permissions to access the SharePoint farm.
	The service account must be the SharePoint farm account (same account that is used to run the SharePoint timer service and the One

Control/setting	Description
	Identity Manager service (job server)). The SharePoint farm account also needs to be added to the local Administrators group on the SharePoint server.
	Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 61.
Add	After selecting the service account, click the **Add** button to add an agent service to the Agent list.
	Repeat to add additional agent services to be used to scan the target SharePoint farm.
Remove	Select an agent service from the Agent list and click the **Remove** button to remove it from the Agent list.
	Removing the selected agent service also removes the configured managed paths for the agent service.
Agent list	Displays the agent services selected to monitor the target SharePoint farm.

Managed paths page

Managed paths determine the unstructured data for which a security index is maintained. A managed path is the root of an NTFS directory tree to be scanned by an agent, or a point in your SharePoint farm hierarchy below which everything is scanned. The agent monitors the specified managed paths for changes to security settings to maintain the security index. In addition, if resource activity collection is enabled, the agent collects resource activity for resources within these same managed paths.

Use the **Managed Paths** page on the **Managed Host Settings** dialog to specify the paths to be monitored and scanned for the target managed host.

NOTE: For all managed host types, when placing a resource under governance, the resource must be a managed path or a folder or share under a managed path.

- For remote managed hosts and SharePoint managed hosts, if you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. If the managed host has more than one agent assigned, you are prompted to select the agent to which the managed path is added.

- For local managed hosts, if you are scanning managed paths (that is, there are paths in the managed paths list), and you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. However, if you are scanning the entire server (that is, the managed paths list is empty) and you place a resource under

ONE IDENTITY
by Quest

> governance, no changes are made to the managed paths list and you continue to scan the entire server.

Table 39: Managed paths page: Controls and settings

Control/setting	Description
Managed paths list	Displays the managed paths to be monitored by the agent. • For local managed hosts, when this list is empty, all NTFS drives are scanned and monitored (default scan behavior). When paths are added to this list, only the specified paths are scanned and monitored. • For remote managed hosts and SharePoint managed hosts, you must specify the paths to be managed in order for scanning to occur. So if this list is empty, no scanning will occur for the target managed host.
Add	Use the **Add** button to define the paths to be monitored. Clicking the **Add** button displays the **Managed Paths Picker** dialog allowing you to select the paths to be managed and the agent to be used to scan the selected managed paths. In the **Managed Paths Picker** dialog, click the check box to the left of a path to add it to the managed paths list and use the **Agent Selection** drop-down menu to specify the agent to be used to scan the different managed paths. Multiple agents cannot scan the same managed paths on a remote managed host or SharePoint managed host.
Remove	Use the **Remove** button to remove a path from the managed paths list. Select the path to be removed and click the **Remove** button.

Security Scanning page

Use the **Security Scanning** page on the **Managed Host Settings** dialog to define when an agent is to perform the initial security scan and when to watch for changes to the structure and security of the file system. Where possible, schedule the scan to low peak hours to avoid heavy network traffic.

The default behavior for security scanning is different depending on the type of agent deployed:

• Local agents: By default, local agents begin scanning immediately when the agent is deployed. Subsequent scans occur on the configured schedule, which is daily at 2:00 A.M. by default.

• Remote agents: Remote agents scan the target computer on a configured schedule. By default, scans are daily starting at 2:00 A.M.

• SharePoint farm agents: SharePoint farm agents scan the target computer on a configured schedule. By default, scans are daily starting at 2:00 A.M.

You can modify the scan schedule and define the time and frequency with which the agent scans the target computer using the options available on the **Security Scanning** page. In addition to defining the security scan schedule, you can specify whether to ignore files and only store folder security data, as well as continuously monitor the file system and apply real-time updates to scanned security data.

| NOTE: The schedule times for security scanning are based on the agent's local time.

Table 40: Security scanning page: Controls and settings

Control/setting	Description
Scanning Schedule	Use the options in the **Scanning Schedule** pane to define the frequency at which the agent performs a full security scan on the target managed host.
	For remote managed hosts and SharePoint managed hosts, managed paths must be defined for scanning to occur. For more information, see Managed paths page on page 104.
Scan start time	Specifies the local time of day, with respect to the machine on which the agent is running, when the security scan is to start. The default start time is 2:00:00 AM. To change this time, use the arrow controls to specify a new time.
	When the **Immediately scan on agent restart or when managed paths change** option is selected, the scan start time is ignore for the initial scan.
Run Daily	Select this option to scan the target computer on a daily schedule. Use the days of the week check boxes to define when the scan will occur during the week and the **Scan start time** field to specify the time the daily scan is to begin.
	• **Days of the week**: Specifies the days of the week to be included/excluded from the daily run. All days of the week are selected by default. Click the corresponding day check box to clear the check box and exclude that day from the daily schedule.
	For all agents, this option is selected by default along with a scan start time of 2:00 A.M. However, since local agents also have the **Immediately scan on agent restart or when managed paths change** option selected by default, the initial scan starts immediately when a local agent is deployed. This daily schedule is then used for subsequent scans by the agent. For remote and SharePoint agents, this daily schedule is used for the initial and subsequent scans.
Run on an interval	Select this option to scan the target computer on an hourly interval instead of a daily schedule. Selecting this option enables the **Every** control to specify the interval to be used.
	• **Every**: Specifies the hour interval to be used. Every 4 hours

Control/setting	Description
	is specified by default. Click the arrow controls to select a different hour interval.
	When using the **Run on an interval** option, it is possible to select a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time is skipped and the next scan starts as normal.
Run once	Select this option to schedule a single security scan of the agent.
	When the **Run once** option is selected, the **Collect activity for real-time security updates** option is automatically selected. This is to ensure that changes to the structure and security of the file system on the target managed host are applied to the scanned data.
Immediately scan on agent restart or when managed paths change	Select the **Immediately scan on agent restart or when managed paths change** option if you want the agent to scan immediately when it is added, when the agent is restarted and when any managed paths are changed.
	For local agents, this option is selected by default. To delay the initial scan and use a configured scan time, clear this check box and use the options in the **Scanning Schedule** pane to define when to start the agent scan.
Ignore all files and only store folder security data	The **Ignore all files and only store folder security data** indicates whether the agent is to capture file security data for the target managed host during an agent scan. When this option is cleared, the agent will include file security data in the agent scan.
	For all supported managed host types, this option is selected by default, indicating that only folder security data is to be scanned.
	NOTE: This option is not available for NFS host types.
Collect activity for real-time security updates	Select the **Collect activity for real-time security updates** option to have the agent watch for changes to the structure and security of the file system on the target managed host (that is, monitor create, delete, and rename operations, as well as DACL, SACL, and Owner changes). This results in a more up-to-date security index.
	When the **Run once** option is selected, this option is automatically selected to ensure that change to the structure and security of the files system on the target host are applied to the scanned data.
	NOTE: When using Change Auditor to collect resource activity, it is not recommended to enable the **Collect activity for real-time security updates** on EMC or NetApp managed hosts. The

Control/setting	Description
	agents managing these host types should be configured to scan on a schedule and not run once. The performance gain in using Change Auditor's event collection will be lost if the Data Governance agent is also collecting activity from these storage devices for security updates.
	NOTE: This option is not available for Generic, SharePoint Farm, SharePoint Online or OneDrive for Business host types.
	NOTE: When changing this setting, the agent starts watching for changes during and following the next scheduled full scan.

Resource activity page

You can collect resource activity on local managed Windows servers, SharePoint farms, and supported NetApp and EMC managed hosts. Resource activity collection is not supported for Windows Cluster/Remote Windows Computer, Generic, or Cloud managed hosts.

NOTE: Limitations with collecting resource activity on EMC storage devices:

- EMC activity collection requires that EMC CEE 7.1 is installed on the same server as the Data Governance agent.

- EMC VNX activity collection by Data Governance agents is not supported for storage devices with multiple CIFS exposed virtual data movers.

- Resource activity collection and real-time security updates are not supported for EMC Isilon NFS managed hosts.

- If Change Auditor is configured to collect activity from your EMC device via the Quest Shared EMC Connector, and you would like activity collection/aggregation in Data Governance Edition, you MUST configure Data Governance Edition to collect activity directly from Change Auditor. You will not be able to collect activity from your EMC device with both Change Auditor and Data Governance Edition.

When enabled, you can configure to collect data on identities, reads, writes, creates, deletes, renames, and security changes on securable objects. Resource activity summary information is used to calculate ownership and for generating activity-related reports, including:

- Resource activity report
- Account activity report
- Interesting resources without an owner report
- Data owner vs. perceived owner report
- Perceived owners for data under governance report

IMPORTANT: By default, the collection of resource activity is disabled. You can enable it when you configure your managed hosts. However, collecting resource activity on your managed hosts impacts network usage and increases load on the Resource Activity

database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation is important to limit some of this load. You should carefully plan out which servers you want to collect activity on and enable it only on those machines.

If you are collecting resource activity, it is recommended that you set up a scheduled execution of the activity database compression utility. This utility compresses the activity in your database that is older than a certain age and optionally purges entries that are even older. This is essential in ensuring your database remains manageable. For more information on the activity database compression utility, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

NOTE: Data Governance Edition may report certain operations in unexpected ways. For example, in some instances a file rename operation may be represented as a delete and a create. This is normal behavior and depends on the system, or in some cases, the applications being used to interact with the resources.

NOTE: The time stamps for resource activity are based on the agent local time.

The **Resource Activity** page on the **Managed Host Settings** dialog contains the following information and options to configure the collection and aggregation of resource activity.

Table 41: Managed host settings: Resource Activity page

Field	Description
No activity (scheduled security scans only)	Use this option if you do not want to collect resource activity for the target managed host. NOTE: For all types of managed hosts, this option is selected by default indicating that resource activity in not being collected for the target managed host.
Collect and aggregate events	Select this option to collect resource activity for the target managed host. When this option is selected, you can configure the events to be collected and the aggregation interval to be used to compress the activity data. NOTE: For SharePoint farm managed hosts, native SharePoint auditing must be enabled in order to collect resource activity. NOTE: For NetApp managed hosts, the FPolicy settings control the activity sent to the agent, unless resource activity is being collected directly from Change Auditor. For more information, see FPolicy deployment on page 235. NOTE: For EMC Celerra/VNX devices, you must configure the cepp.conf. For more information, see Creating the cepp.conf file (Celerra or VNX devices) on page 231. NOTE: For EMC Isilon CIFS devices, you must enable auditing. For more information, see Enabling system configuration auditing (Isilon devices) on page 233. NOTE: When using Change Auditor to collect resource activity,

Field	Description
	this option is selected by default. For more information, see the *Post installation configuration* chapter in the *One Identity Manager Data Governance Edition Deployment Guide*.
Events	Select or clear the check boxes to specify the type of events to be included in the resource activity collection process: • Security change • Create • Delete • Rename • Write • Read (Disabled by default) NOTE: When resource activity collection is enabled, read operations are not collected by default. Care should be taken when enabling read operations because they may cause performance issues.
Aggregation	Select how often you would like to aggregate the data. Valid aggregation intervals are: • 5 minutes • 1 hours • 8 hours (default) • 1 day All activity is aggregated within the set time frame, which is 8 hours by default. For example, if a user reads a file ten times within the time frame, it appears as a single line item with a count of 10. The aggregation interval should be chosen carefully. A shorter interval gives more granular information about activities but can cause the size of the database to use up all the disk space on the server. NOTE: When using Change Auditor to collect resource activity, the aggregation setting is not available. Change Auditor is configured to collect events every 15 minutes on all managed hosts. For more information, see the *Post installation configuration* chapter in the *One Identity Manager Data Governance Edition Deployment Guide*
Resource Activity Exclusions	Click this button to specify the accounts, file extensions, and folders to be excluded from the resource activity collection process. By focusing on the objects in whose activity you are interested, you can

Field	Description
	reduce network traffic.
	Certain well known system accounts, file extensions, and folders are excluded by default, such as:
	- Accounts: Local Service, Network Service, Null SID, System The Accounts tab is not available for NFS managed hosts. - File Extensions: Database files, Disc Image files, Email files, Executable files, Explorer Metadata files, Log files, Shortcut files, Temporary files, and Virtual machine files - Folders: %SystemRoot%, %ProgramFiles%, %ProgramFiles (x86)%
	By default, the Data Governance agent excludes the run as account (local managed hosts) and the domain service account (remote managed hosts) from activity collection and aggregation regardless if the service account is specified in the Resource Activity Exclusions list. The service account for SharePoint farm managed hosts are not excluded by default; you will need to add the SharePoint service account manually for SharePoint farm managed hosts.
	To see the full list, click the **Resource Activity Exclusions** button.
	- If the list is empty on the **Resource activity exclusions** dialog, click **Default** to populate the exclusions list with default values. - To add an object to the exclusion list, click **Add** and specify the account, file extension or folder.
	NOTE: When using Change Auditor to collect resource activity, the Resource Activity Exclusions feature is not available. For more information, see the *Post installation configuration* chapter in the *One Identity Manager Data Governance Edition Deployment Guide*.
View/Update cepp.conf	For EMC Celerra/VNX hosts, this button allows you to view or update the cepp.conf file for the selected data mover.
	Clicking this button displays a **Logon Credentials** dialog allowing you to enter the EMC Celerra/VNX control station credentials and to select the data mover to be scanned.
	- Control Station: Enter the IP address or host name of the EMC Celerra/VNX control station. - User: Enter the user name of an account with administrative rights on the specified control station. - Password: Enter the password associated with the user

Field	Description
	account entered.
	The client attempts to connect and loads the list of available data movers on the specified device.
	• Data Mover: Select the data mover that holds the managed paths you wish to monitor and will also be associated with resource activity collection.
	The client then retrieves and displays the cepp.conf file from the selected data mover. You can edit the Proposed cepp.conf file (lower pane) as needed. To save your edits, select **Update File**. The client then sends the Proposed cepp.conf file to the EMC device. It will stop and start the cepp service for the selected data mover to apply the new cepp.conf file.
	Click the **Check Status** button to retrieve the same information you wold get if you ran "server_cepp server_2-pool-info" on the EMC device.

Editing managed host settings

You can edit the managed host settings for one or more managed hosts of the same host type. For more information on the configuration options available, see Managed host configuration settings on page 94. You can also use the **Edit host settings** task to add, remove or change the agents used to scan a remote managed host. For more information, see Removing agents on page 122.

To edit a managed host's configuration settings

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. In the **Managed hosts** view (right pane), select the required managed host with a status of **Managed**.

3. Select **Edit host settings** in the Tasks view or right-click menu.

   The **Managed Host Settings** dialog appears, displaying the pages that contain settings that can be edited based on the type of host selected in the Managed hosts view.

   • Use the **Managed Paths** page to change the paths to be scanned and monitored.

   • Use the **Security Scanning** page to change the scanning schedule and scan settings.

   • Use the **Resource Activity** page to change the resource activity collection and aggregation settings.

4. After making the required changes, click **OK** to save your selections and close the dialog.

The agent will scan using the new settings at the next scheduled scan time. However, if you modified the managed paths being scanned and the **Immediately scan on agent restart or when managed paths change** option is selected on the **Security Scanning** page, the agent initiates a scan immediately.

To edit multiple managed hosts

NOTE: When multiple managed hosts are selected, keep in mind that the settings are overwritten for all selected managed hosts and only the settings that are appropriate for the selected managed host type are applied. Because of this, you may notice that not all the same pages are displayed when multiple managed hosts are selected for editing (for example, the **Managed Paths** page is not displayed).

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. Select multiple managed hosts with the same host type in the **Managed hosts** view

3. Select **Edit host properties** in the Tasks view or right-click menu.

   The **Managed Host Settings** dialog appears, displaying the pages that contain settings that can be edited based on the type of host selected in the Managed hosts view.

   - Use the **Security Scanning** page to change the scanning schedule and scan settings.

   - Use the **Resource Activity** page to change the resource activity collection and aggregation settings.

   The options displayed are the factory default values regardless of the current values of the selected managed hosts.

4. Select the **Apply these settings to all selected managed hosts** check box and make the required changes, which will be applied to all selected managed hosts.

5. Click **OK** to save your selections and close the dialog.

The agent will scan using the new settings at the next scheduled scan time.

Customizing default host settings

Defining default host settings for each type of managed host is now available through the Manager. Using the **Customize default host settings** task in the Manager, you can define the default scanning schedule and settings and the default resource activity collection and aggregation settings for the selected managed host type. Once customized default settings are defined, they are used when adding new managed hosts to the Data Governance Edition deployment.

NOTE: Currently managed hosts are not affected by the default host setting changes made on this dialog; only those added in the future use the settings defined here.

To customize default host settings

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Select the **Customize default host settings** from the Tasks view or right-click menu.

    The **Customize default host settings** dialog appears.

3. At the top of the dialog, specify the following information:

    a. **Host Type**: Select the host type from the drop-down menu:

    - Local Windows Computer
    - Windows Cluster/Remote Windows Computer
    - Generic Host Type
    - SharePoint Farm
    - EMC Celerra/VNX Device
    - EMC Isilon Device
    - NetApp OnTap 7-Mode CIFS Device
    - NetApp OnTap Cluster Mode CIFS Device
    - NetApp Cluster NFS Device
    - EMC Isilon NFS Device
    - NetApp 7-Mode NFS Device
    - SharePoint Online
    - OneDrive for Business

    b. **Agent Install Path**: Use this field if you want to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

    c. **Keywords**: Use this field if you want to specify a keyword to be assigned to newly managed hosts, which can be used for sorting and grouping on the **Managed hosts** view.

4. Use the **Security Scanning** page to define the default scanning schedule and settings. For more information, see Security Scanning page on page 105.

5. Use the **Resource Activity** page to define the resource activity collection and aggregation settings. For more information, see Resource activity page on page 108.

    NOTE: Resource activity collection is not available for the following host types:

    - Windows Cluster/Remote Windows Computer
    - Generic Host Type
    - EMC Isilon NFS Device
    - SharePoint Online
    - OneDrive for Business

6. Repeat steps 3 - 5 for any additional host types that require custom default settings.

7. If necessary, click the **Restore Factory Defaults** button to reset all changed settings back to the factory defaults.

   NOTE: Clicking the **Restore Factory Defaults** button resets all custom default settings back to the factory default settings for all managed host types.

8. Click **OK** to save your selections and close the dialog.

All managed hosts of the selected host type that are added in the future will use these customized default settings.

Deployment management

You should regularly check the status of your managed hosts to ensure that the system is working properly. You can see the state of your deployment through the **Managed hosts** view and **Agents** view.

- Verifying managed host system status
- Determining the state of the data
- Checking the agent status
- Viewing agent errors
- Restarting agents
- Removing managed hosts (and associated agents)
- Removing agents

Verifying managed host system status

When you first deploy a managed host it takes a few minutes for the agent to start collecting data. As the status changes, a regular refresh allows you to see the changes. You can also use this status to track the progress whenever you add or remove an agent.

A managed host's status is displayed on the **Managed hosts** view.

Table 42: Managed host status

Status	Description
Agent Issue	One or more agents for this managed host are in an error state. The **Status Detail** column on the **Agents** view may contain additional information to identify the problem.
	NOTE: For remote managed hosts, if there is an issue with any of its agents, you see a status of "Agent Issue."
Agent Out of Disk Space	An agent for this managed host is out of free disk space. For

Status	Description
	more information, see Checking the agent status on page 118.
Agent Registration Failed	An error occurred while an agent was attempting to register with the server.
Agent Unregistered	An agent for this managed host has unregistered. Ensure that the agent service is running, and that the computer hosting the agent is online.
Agent Update Required	An unsupported agent version has attempted to register with the server. The agents on the managed host must be upgraded.
Deleting	The managed host is being deleted.
Deleting And Uninstalling	The managed host is being deleted and all agents associated with this managed host are being removed.
Deploying Agent	An agent for this managed host is being installed.
Install Failed	An automatic agent install has failed. The **Status Detail** column on the **Agents** view may contain additional information regarding the failure.
Installing agents failed	You are attempting to install an agent on a server that already has an agent on it, and that agent belongs to another Data Governance Edition deployment. The **Status Detail** column on the **Agents** view may contain additional information, including the name of the deployment that is already using this agent.
Managed	All agents associated with this managed host are working properly.
No communication from agent	The lease for an agent on this managed host has expired. A communications issue has occurred between the agent and the server, or the agent is no longer running. Ensure that the agent can communicate with the server.
No agents for host	There are no agents associated with this managed host. Deploy an agent for this host in order to maintain a security index and track resource activity.
Not Managed	The host computer is not being managed by Data Governance Edition. That is, no managed host has been configured for the host computer.
Resolved	The managed host's information has been resolved, but it has not yet been configured for management. This is a

Status	Description
	temporary state.
Resolving Agents	The server is resolving an agent computer for this managed host.
Un-deploying Agents	An agent for this managed host is being uninstalled.
Uninstalling agents failed	An automatic uninstall of an agent failed. The **Status Detail** column on the Agents view may contain more information regarding the failure.
Unknown	An error occurred while retrieving this managed host's agent status.
Unknown host type	A host computer with an unknown host type was found.
Unresolvable	The managed host computer has failed to be resolved.
Unresolved	The managed host computer has not yet been resolved.
Upgrading agent	The agent is being upgraded to the latest version.
Waiting for Agent Connection	The managed host has been configured and is waiting for an agent to register. If a managed host stays in this state for a long time, it could indicate a communications issue between the agent and the server.

Determining the state of the data

For each managed host, use the **Managed hosts** view to determine the state of the data. Errors should be addressed immediately, in order to ensure accurate data from the managed host being scanned. The following table outlines the different states your data can have.

Table 43: Data states

State	Description
A scanning error has occurred	There has been an error with one of the scanners. Data is incomplete, so you should determine what the issue is. Ensure that the managed host is available on the network, and confirm that the agent's service account has adequate access to the managed host.
Data available	The agent has successfully completed scanning security information for the managed host.
Please use Agents View to see status	On multi-agent hosts, this message indicates that the status of the data is not available for all of the agents. Open the **Agents** view to

State	Description
data for multiple agents	see the status of the data for each individual agent assigned to the selected managed host.
Scanning	The agent is performing a full scan of security information. Queries for information at this time may be incomplete.
No managed paths configured	There are no managed paths specified and therefore scanning cannot be performed on the managed host.
Waiting for scanning to start	The agent is ready to scan when the next scheduled scan is triggered.
Waiting for scanning status	The agent is not yet ready to start scanning.

Checking the agent status

For security indexing and resource activity tracking to function as expected, the agent must have a status of **Managed**. You can see the status of an agent in the Agents view. Also, if the status of a managed host is anything other than **Managed**, check the host's agents' status to determine where the issue lies.

NOTE: During deployment, the state changes quickly, and a regular refresh allows you to see the changes.

Table 44: Agent states

Agent states	Description
Agent host belongs to another deployment	An agent already resides on this server that belongs to another Data Governance Edition deployment. See the **Status Detail** column for additional information, including the name of the deployment that is already using this agent.
Agent Out Of Disk Space	The hard disk of the agent's working directory dropped below 2GB.
	NOTE: This condition causes the agent to shutdown with an error. This is a safeguard to prevent disruption of other services hosted on the computer, allowing you time to add a volume or reallocate space. See Agent Shutdown Because of Error.
Agent Shutdown Because of Error	The agent may shut down with error for the following reasons:
	• Agent scanning does not progress after two hours.
	• There is not enough free disk space on the agent (minimum 2GB). See Agent Out Of Disk Space.

Agent states	Description
	NOTE: To determine if low space on the host volume was the cause, check the **Agent Events** view or agent logs.
	• An error occurred while the agent attempted to open an NTFS security database to perform a sync.
Agent Update Required	An unsupported agent version has attempted to register with the server.
Agent Unregistered	The agent has unregistered.
Configuration Failed	An error has occurred while creating the agent service on the agent host computer.
Configuration in Progress	The agent service is being configured.
Deleting	The agent is being deleted.
Deleting and Uninstalling	The agent software is being uninstalled.
Host Configuration Failed	While preparing for an agent installation, one of the conditions were encountered: • The host's data root is invalid. • The host has a NetApp FPolicy configuration error.
Host Domain Not Managed	The host domain is not yet managed in Data Governance Edition.
Install Failed	An error occurred while installing the agent.
Install in Progress	The agent installation is in progress.
No Communication from Agent	The agent has failed to renew its lease. This state is often an indication of an error on the agent computer. Ensure that the agent can communicate with the server.
OK	The agent is working properly. The agent is deployed and has contacted the Data Governance service.
Registration Failed	An error occurred while the agent was attempting to register with the server.
Removal of config-uration failed	An error occurred while removing the agent from the agent host computer.
Removal of config-uration in progress	The agent service is being removed.
Resolved	The managed host's information has been resolved, but it has

ONE IDENTITY
by Quest

Agent states	Description
	not yet been confirmed for management. This is a temporary state.
Uninstall Failed	An error occurred while uninstalling the agent service from the agent host computer.
Uninstall in Progress	The agent is being uninstalled.
Uninstalled	The uninstall has finished. This is a temporary state.
Unknown	The current state of the agent is unknown.
Unresolvable	The agent computer cannot be resolved.
Unresolved	The agent computer has not yet been resolved.
Waiting for agent connection	The management server is waiting for the agent to register with the server. NOTE: If an agent remains in this state for a long time, it could indicate a communication issue between the agent and the server.

Viewing agent errors

You can quickly assess your agents for any potential critical issues by reviewing logged error messages using the **Agents** view in the Manager.

NOTE: The **Agent Errors** column in the **Managed hosts** view indicates when an agent associated with a managed host has encountered any errors. However, you can only view an agent's error messages using the Agents view.

To view agent errors

1. In the Navigation view, select **Data Governance** | **Agents**.

   The **Agents** view appears.

2. The **Critical Error** column indicates if there are any error messages logged for an agent.

3. Select the agent from the **Agents** view, and select **View agent errors** in the Task view or right-click menu.

   NOTE: The **View agent errors** task is only available for agents that have error messages logged.

4. The event viewer appears.

   Click the 🗑**Clear Events** button in the upper left corner to clear the agent errors. Click **Yes** on the confirmation dialog.

   Click the close button in the upper right corner to close the event viewer.

NOTE: You can also clear error messages for a specific agent using the **Clear agent errors** task from the Agents view.

Restarting agents

You must restart an agent when a new storage volume is added to the managed host being scanned by the agent.

To restart an agent

1. In the Navigation view, select **Data Governance** | **Agents**.
2. Select the required agents in the **Agents** view, and select **Restart agent** in the Tasks view or right-click menu.
3. Click **Yes** to confirm.

NOTE: When a Data Governance agent is restarted, it re-creates all information within its local index. The server index is updated when the full scan completes. An agent will immediately start scanning when the service is restarted if the **Immediately scan on agent restart or when managed paths change** option is selected. This option is available at the bottom of the **Security Scanning** page on the **Managed Host Settings** dialog.

To determine whether data in the client is the most current from the agent, ensure that the data state of the managed host being examined is marked as "Data available."

Removing managed hosts (and associated agents)

NOTE: All agents associated with a managed host are uninstalled when you remove a managed host. You can, however, remove a remote agent without removing the managed host using the **Edit host settings** task. For more information, see Removing agents on page 122.

Before removing a managed host ensure that the impact of its removal is considered. Any governed data records or activity information associated with resources on that host is removed from the database as well. Use caution when removing the governance on an item, as there may be business reasons for this setting. For more information on removing governance, see Managing resources under governance on page 153.

It can take a considerable amount of time to remove a managed host with governed resources (for example, one to two hours per million governed resources). The Manager lists the managed host in the "Deleting" state until this process finishes.

To remove a managed host (and its agents)

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. Select a managed host from the **Managed hosts** view, and select **Remove** in the Tasks view or right-click menu.

   NOTE: You can select multiple managed hosts for removal.

   The **Remove** task is not available for host computers with a status of **Not Managed**.

3. Click **Remove** to confirm the removal.

   If you remove a managed host with governed data, the data is no longer governed. All associated security information and resource activity is also deleted.

Removing agents

All agents associated with a managed host are uninstalled when you remove a managed host. You can, however, remove a remote agent without removing the managed host using the **Edit host settings** task.

NOTE: You must have at least one agent assigned to the managed host in order to complete the edit operation.

To remove a remote agent from a managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. In the **Managed hosts** view (right pane), select the required managed host with a status of **Managed**.

3. Select **Edit host settings** in the Tasks view or right-click menu.

   The **Managed Host Settings** dialog appears.

4. Open the **Agent** page, select the agent to be removed and click **Remove**.

   NOTE: Removing the agent will also remove the managed paths associated with that agent. If that is the desired result, select **Yes** on the confirmation dialog.

5. Click **OK** to remove the selected agent.

   NOTE: If you remove the last agent in the list, the **OK** button will not be available. You will need to specify at least one agent for the managed host before you can save your changes.

Managing unstructured data access

- Managing resource access
- Managing account access
- Working with security permissions
- Working with SharePoint security permissions
- Account access modeling
- Bringing data under governance

Managing resource access

One of the key security measures in an organization is to ensure that the access control policies are deployed effectively. Data Governance Edition provides you with several ways of managing access to data and measuring your progress to meet your security and compliance needs.

This section deals with looking at access management from a resource perspective. Managing account access on page 127 provides details on managing access from an identity perspective.

Data Governance Edition enables you to:

- Determine what is in your environment and who has access to it.

    Data Governance Edition provides a real-time view of data access, allowing for a centralized view and control of permission assignments throughout the managed domain.

- Minimize IT's role as gatekeeper.

    While IT is responsible for implementing access controls, the governing of data should be carried out by the people within the organization who actually own it. Data Governance Edition, along with the web portal, provides the workflow to accomplish this.

- Improve access control consistency.

  Inconsistent application of permissions contributes to downtime, lost productivity, security breaches and more. Organizations seek to create a governed environment that provides users with access to exactly the resources they need — no more and no less.

Using Data Governance Edition, you can browse through the resources on the hosts in your managed domains to:

- Examine a file system or SharePoint farm to see what users and groups have access to it, and modify the access if necessary. For details on the Resource browser, see Browsing your environment on page 124.

- Examine a user or group to ensure that they have the correct data access. For details, see Managing account access on page 127.

- Investigate access for a user in a particular role within your organization to help grant the same access to a new hire. For details, see Cloning, replacing, and removing access for a group of accounts on page 130.

- Evaluate a group's access before deleting it. For details, see Viewing group membership on page 129.

- Compare account access for selected users or groups and simulate the addition and removal of users or groups from selected groups. For details, see Comparing accounts on page 143 and Simulating the effects of group membership modifications on an account on page 147.

- Calculate perceived owners to identify potential business owners for data within your environment. For details, see Calculating perceived owner on page 163.

- Place data under governance and leverage the self-service requests attestations, policies, and reports that help to ensure that your data is in compliance. For details see, Bringing data under governance on page 149.

Browsing your environment

A key challenge in improving data governance is keeping track of permissions within your environment. To ensure that data is secured in a manner that meets your business needs, you must be able to easily identify who has been given access and manage that access appropriately.

Once you have added a managed host, you can view access to its data through the:

- Resource browser: This is a live view of data on the managed host. You can browse through the supported file systems and see all applied permissions and make changes where required. For more information, see Working with security permissions on page 132.

  Through the **Resource browser** you can also identify, in an easy to browse tree view, where the access on a resource differs from its parent and manage that access.For more information, see Managing security deviations on page 135.

- Accounts view: This view displays the security index returned by Data Governance agents, which is controlled by the schedule and settings for each agent. You can browse to an account, and see all the data to which they have access on the managed host. For more information, see Managing account access on page 127.

- Manage access view: This view summarizes the type of data to which an account has access and the specific data of that type. From here, you can also view detailed group membership information. For more information, see Managing account access on page 127 and Viewing group membership on page 129. (You can only manage directly applied access from the **Accounts** view and the **Security Index** node. Accounts with indirect access, through group membership, can be managed from the Active Directory view.)

  NOTE: You can also view governed data access by selecting a user or group's Account Overview.

  NOTE: You can also select to manage access from Active Directory users and groups. Select **Active Directory** in the Navigation view, select the required user or group, and select **Manage access** from the Tasks view.

Once you have located the data, you can edit the security as required or place it under governance to control access to it. For more information, see Bringing data under governance on page 149.

To view the access on a specific resource

1. In the Navigation view, select **Data Governance | Managed hosts**.

   NOTE: To group this view by host type, right-click on the **Host Type** column header and select **Group By This Column**. If the **Host Type** column is not displayed, right-click on the column headers, select **Column Chooser** and drag **Host Type** into the column header.

2. Open the Resource browser using one of the following methods:

   - Double-click the required managed host in the **Managed hosts** view.

   - Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. In the **Resource browser**, double-click through the resources to locate the required resource.

   The **Resource browser** displays the following information:

   - For a Windows computer, the shares and file system display.

   - For a SharePoint farm, each farm is represented as a hierarchy, with the farm as the top level, followed by web applications, site collections, sites and then the contents of the site. The contents of a list are shown as "list item", regardless of the type of item in SharePoint. The **Resource browser** displays a list of the web applications on the selected farm.

   - For a Distributed File System Root, links are displayed at the top level. Browsing into a link shows its target paths and browsing into a target path takes you to the appropriate backing folder. While browsing a backing folder,

the Distributed File System path is shown in the **Location** field at the top of the page.

- For Cloud managed hosts, each site is represented by a folder hierarchy, with the Home top level site displayed as Site contents folder, followed by all other subsites. Each site contains a Site contents folder encompassing other nested folders. The contents of a site and document library are shown as "folder" type, whereas, files are shown as "file" type items. No other resource types are managed for Cloud managed hosts.

  NOTE: The **Resource browser** and resource access reports do not display the limited access users or "previewer" accounts.

You can use the **Location** field, at the top of the page, to view your current location. If you have navigated too far, you can move back by clicking the 🔼**Up One Level** button.

4. Select a resource in the top pane to display the permissions applied to that resource.

To view a selected user or group's access on all managed hosts in your environment

1. In the Navigation view, select **Data Governance | Security Index**.
2. In the **Accounts** result list, double-click the required user or group.
3. In the Tasks view, select **Manage access**.

   All the access points for the selected user or group are displayed. By default, the results are listed by managed host.

4. Expand a managed host to display all the resources where the selected user or group has access.

   You are able to see if the access has been granted explicitly (Directly held — the account is in the ACL) or through group membership (Indirectly held — the account belongs to a group that is in the ACL).

5. Browse through the managed hosts and their resources to view and manage the security on the object.

   Once you have located the resource, you can select to manage its access and create reports that detail account access and group membership information.

To view all the users and groups that have access on a specific managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. Select the required managed host from the **Managed hosts** view.
3. In the Tasks view, select **Accounts view**.

   All resource types where users and groups have some level of access displays. By default, the results are grouped by resource type.

4. Expand a resource type to display all the accounts that have access.

   For more information, see Managing account access on page 127.

Searching for resources

You can quickly and easily locate specific resources to manage through the search option.

| NOTE: The search feature is not available for SharePoint and DFS managed hosts.

Once you have located the resource, you can place the resource under governance so that it is available to use in policies and attestations, publish it to the IT Shop so that it is available for employees and business owners to request and grant access to it, assign a business owner, or edit the security as required.

To search for a resource

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

   - Double-click the required managed host in the **Managed hosts** view.

   - Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. Select a share or a local path to enable the search controls in the top right corner.

4. In the search field, enter the search criteria.

   You can use the * character to search for resources. For example, enter Finance* to return all resources that begin with Finance, *.txt returns all resources that end with .txt, and *Fin* returns all resources that contain Fin in their name.

5. By default all items that match your query are returned. To limit the search results, click the arrow control to the right of the search button and select how many items you would like to return.

   You have the option of returning the top 100, 200, or 500 results, or all the items that match your query.

6. Click the 🔍 **Search** button.

Managing account access

As people join, depart, and move through your organization, you need to change their data access. With Data Governance Edition, you can validate that users and groups have been granted access to all the resources they need, ensure that they do not have access to excess resources, and manage their access when problems arise.

Whether you select to manage a particular user or group through the **Security Index** node in the Navigation view or through the Accounts view for a selected managed host, you have access to all the detailed security index information that has been returned by the agents within your environment.

You are able to:

- View the group membership information for the selected account
- Clone, replace, or remove the account access on a resource
- Place a resource under governance and publish it to the IT Shop
- Edit resource security for selected resources

Before altering access for users or groups, you may want to compare accounts or view the potential effects of group membership changes. For more information, see Comparing accounts on page 143.

NOTE: To identify where accounts have access, for SharePoint web apps that use Windows claims, the claim is associated with the relevant Active Directory account for all governed data.

To view access for a specific managed host

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Select the required managed host from the **Managed hosts** view.

3. Select **Accounts view** from the Tasks view or right-click menu.

    All resource types where users and groups have some level of access displays. By default, the results are grouped by resource type. Expand a resource type to display all the accounts that have access.

4. Browse through the resources, select the required user or group, and select **Manage access** from the Tasks view or right-click menu.

    The **Manage Access** view appears displaying the managed hosts where the selected user or group has access.

5. Select the **Group Memberships** tab to see how the account has gained access through group membership.

    NOTE: This tab is not available for SharePoint account types.

    The first level beneath the root is all the groups for which the account is a direct member. The groups contained beneath each of those groups the account has gained access indirectly from the first-level groups, and so on.

6. Click the pin icon to dock the window and select a group to see their access on all managed hosts within your environment.

7. Drill down through the managed hosts and the resource types to locate the required resource.

    You are able to see if the access has been granted explicitly (Directly held — the account is in the ACL) or through group membership (Indirectly held — the account belongs to a group that is in the ACL).

8. Select a resource in the lower pane.

    Once you have located the resource, you can place the resource under governance to secure it; publish it to the IT Shop so that it is available for users and business owners to request and grant access to it; copy, remove, or replace access on the

resource; edit the security as required; and create reports that detail account access and group membership information.

To manage access for a specific user or group

1. In the Navigation view, select **Data Governance | Security Index**.

   All the users and groups that have been returned by the agent's scan is available in the **Accounts** result list.

2. Select the required user or group from the **Security Index** view and select **Manage access** from the Tasks view or right-click menu.

   From here, you can see the access for a selected user or group on all managed hosts within your environment. You can quickly see whether this access has been granted explicitly (Directly held — the account is in the ACL) or through group membership (Indirectly held — the account belongs to a group that is in the ACL) and select to manage their access.

3. Select the **Group Memberships** tab to see how the account has gained access through group membership.

   The first level beneath the root is all the groups for which the account is a direct member. The groups contained beneath each of those groups the account has gained access indirectly from the first-level groups, and so on.

4. Click the pin icon to dock the window and select a group to see their access on all managed hosts within your environment.

5. Drill down through the managed hosts and select the required resource.

   Once you have located the resource, you can place the resource under governance to secure it; publish it to the IT Shop so that it is available for users and business owners to request and grant access to it; copy, remove, or replace access on the resource; edit the security as required; and create reports that detail account access and group membership information.

Viewing group membership

Because user and group access may be the result of several layers of nested groups, it may be difficult to assess how a specific account has gained access to a resource. Using the **Group Memberships** view, you can easily see group membership, computers, and resource types where the user or group has both direct access and indirect access by group membership and ensure that group access is properly assigned.

To view group membership information

1. In the Navigation view, select **Data Governance | Security Index**.

2. Select a user or group in the **Security Index** view and select **Manage access** from the Tasks view or right-click menu.

3. On the **Manage Access** view, click the **Group Memberships** tab to view all group members for the selected user or group — both direct and indirect.

   NOTE: The **Group Membership** tab is only available for Active Directory users and groups.

   This opens a tree view with the selected account at the root. The first level beneath the root is all the groups for which the account is a direct member. The groups contained beneath each of those groups the account has gained access indirectly from the first-level groups, and so on. This view allows you to select any group to see the resource access granted by being a member of that particular group.

4. Click the pin icon to dock the window and select a group to see their access on all managed hosts within your environment.

Cloning, replacing, and removing access for a group of accounts

When you select **Manage access** for a user or group, you will see all the resources they have access to on the managed hosts within your organization. This access may be both applied directly and indirectly (gained through group membership).

From here, you can select to clone, replace, or remove access for a single account or for multiple users and groups at once. It is important to note that all actions are made on the actual security settings for the resource; actions will not alter group membership.

- Cloning access grants the selected access to another user or group, while maintaining the existing rights on the selected account.

- Removing direct access removes the security setting from the resource ACL. For indirect access, the group that is on the ACL is removed - the selected account (the one with the indirect access) remains a member of the group that had the access prior to the removal operation.

- Replacing access grants the currently configured access to another user or group and removes the access from the original account.

You can view the progress of these changes by selecting **Data Governance | Background Operations** in the Navigation view.

To clone, replace, or remove access for a group of accounts

1. In the Navigation view, select **Data Governance | Security Index**.

2. In the **Accounts** result list, double-click a user or group, and select **Manage access** in the Tasks view.

3. Browse through the managed hosts and resource types.

4. In the bottom pane, select the resource and select one of the following tasks from the Tasks view:

- **Clone account access** to copy the account access for a new user or group. Select the user or group that you want to have this access, and click **OK**.

- **Replace account** to grant the currently configured access to another user or group. Select the user or group that you want to replace the existing user or group with, and click **OK**.

- **Remove account** to remove the selected account's access from the resource. Click **Yes** on the confirmation dialog to confirm the operation.

NOTE: If you see a message in the list of issues that the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

Adding an account to a resource with no associated access information

Through Windows Active Directory, it is possible to have a resource without associated access information, whether through a null security descriptor (SD) or a null discretionary access control list (DACL). This resource is accessible by all groups and users.

Data Governance Edition enables you to put in place a security measure to eliminate this possibility by adding a user or group to ensure that all resources have access information.

To add an account to a null SD or null DACL

1. In the Navigation view, select **Data Governance | Security Index**.

2. In the **Accounts** result list, double-click the **Null Security Descriptor Alias** or the **Null Discretionary Access Control List Alias** account.

   NOTE: If you do not see a **Null Security Description Alias** or **Null Discretionary Access Control List Alias** in the view, then you have no orphan SDs or DACLs.

3. In the Tasks view, select **Manage access**.

   A list of managed hosts and the resources without assigned access display.

4. Double-click a managed host and select a resource type to see a list of resources with the **Null Security Descriptor Alias** or **Null Discretionary Access Control List Alias**.

5. In the bottom pane, select the resource that you want to secure, and select **Edit security** in the Tasks view.

6. In the **Edit Resource Security** dialog, specify the required permissions and control. Click **Save** to save your selections.

Working with security permissions

Access to data affects how employees can ultimately perform their day to day tasks. Through the Manager, administrators can manage and set permissions for network objects. For more information, see Viewing the security on objects on page 132.

> NOTE: Access can also be granted through the web portal's IT Shop. Employees access requests follow a defined approval process where authorized persons, the business owner and group owner, can approve or deny requests.
>
> For more information, see Publishing resources to the IT Shop on page 155.

Before you can edit permissions, you must be granted the **Data Governance | Access Managers** application role.

Viewing the security on objects

You can see and manage the security for a selected resource or a selected account. Once you have located an object, you can see:

- The users and groups that have access to the object. These can be Active Directory users or groups or SharePoint groups.
- The level of access, both DACL and SACL, for NTFS objects.
- The permission level assigned to each user or group.

  For SharePoint, you can see the permissions associated with a particular permission level, and a summary of all the permissions granted by the combination of assigned permission levels.

- Whether the object has inherited or unique permissions. You cannot edit inherited permissions; however, you can view the details of the assigned permissions.

  For SharePoint, you can switch between inherited and unique, and then configure the unique permissions.

- The resource and business owner.

For details on managing security on objects, see:

- Modifying discretionary access control list (DACL) permissions for NTFS resources
- Modifying auditing system access control list (SACL) permissions for NTFS resources
- Working with SharePoint security permissions
- Managing security deviations
- Managing account access

Modifying discretionary access control list (DACL) permissions for NTFS resources

As the administrator, ensure that users and groups have the access they require to perform their day to day tasks. Using Data Governance Edition, you can determine the existing data access, add users and groups to the resource ACL, edit any existing access, and remove access as required.

NOTE: You can only modify access that has been explicitly granted, but you can change inheritance from the Control tab when you select to **Edit Security** for a resource.

NOTE: If you see a message in the list of issues that the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

To add, edit or remove access DACL permissions

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

    - Double-click the required managed host in the **Managed hosts** view.

    - Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. In the **Resource browser**, use the top pane to locate and select the resource. Double-click through the resources to locate the required resource.

4. Select the required resource to display the security for the resource in the lower pane.

    You can use the **Location** field, at the top of the tab, to view your current location.

    If you have navigated too far, you can move back by clicking the ⬆ **Up One Level** button.

5. Select the **Folder Permissions** tab or **File Permissions** tab.

6. To give a user or group access to the selected resource, click in the lower pane and select **Add rights** in the Tasks view.

    a. Select the account to add and click **Next**.

    b. Select where to apply the permissions.

    c. Select the permissions to add.

    d. If applicable, select to limit the permissions to only objects and containers within the selected container.

    e. Click **Finish**.

    Back on the **Folder Permissions** or **File Permissions** tab, unsaved changes appear bold.

7. To remove access, right-click the required account and select **Remove selected permissions**. Click **OK** on the confirmation dialog to confirm the remove operation.

8. To alter the access, select the required user or group, and click in the **Rights** column.

   a. Alter the permissions as required.

   b. Click the **Applies To** column to select how you want the permissions applied.

9. Click the **Save** toolbar button located above the Folder Permissions or File Permissions tab to save your selections. Click **Yes** on the confirmation dialog.

   You can now browse through the network to ensure that the proper access has been granted or removed.

To configure DACL inheritance settings

1. In the Resource browser, select the **Control** tab.

2. Select whether you want the settings to be inherited. The **Inheritance from Parent** options available include:

   - Allow inheritable permissions from the parent to propagate to this object and all child object.

   - Allow inheritable audit settings from the parent to propagate to this object and all child objects.

   NOTE: Clearing either of these check boxes cause inheritance to be blocked. Select the appropriate option on the **Block Access Inheritance** dialog before clicking **OK** to confirm this change:

   - Copy all permissions inherited from parent and make explicit (default)

   - Remove all permissions inherited from parent

3. Click the **Save** toolbar button to save your selection.

Modifying auditing system access control list (SACL) permissions for NTFS resources

Adding, editing or removing these rights enables you to manage the auditing of data access success and failures.

To add, edit or remove SACL permissions

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

   - Double-click the required managed host in the **Managed hosts** view.

   - Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. In the **Resource browser**, use the top pane to locate and select the resource. Double-click through the resources to locate the required resource.

4. Select the required resource to display the security for the resource in the lower pane.

You can use the **Location** field to view your current location. If you have navigated too far, you can move back by clicking the ⬆ **Up One Level** button.

5. Select the **Auditing** tab.

6. To add a SACL right to a user or group, click in the lower pane and select **Add rights** in the Tasks view.

    a. Select the account to add and click **Next**.

    b. Select where to apply the rights.

    c. Select the rights to monitor.

    d. If applicable, select to limit the auditing to only objects and containers within the selected container.

    e. Click **Finish**.

    Back on the Auditing tab, unsaved changes appear bold.

7. To remove a SACL right, right-click the user or group, and select **Remove selected permissions**. Click **OK** on the confirmation dialog to confirm the remove operation.

8. To edit the rights, select the required user or group, and click in the **Rights** column.

    a. Alter the permissions as required.

    b. Click the **Applies to** column to select how you want the permissions applied.

9. Click the **Save** toolbar button to save your selections.

Managing security deviations

Through the **Resource browser** you can see how security has been applied on selected resources and implement changes as required. The **Deviations** view enables you to browse through a tree view and identify where subfolders and files of the identified resources have security that differs from the parent (for example, if inheritance is overridden or blocked).

NOTE: The Deviations view is not available for NFS managed hosts.

From this view you can also quickly address access issues and edit security where required. This helps you meet your compliance and audit goals by ensuring only authorized users can access the specific resources.

To manage security deviations

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

    • Double-click the required managed host in the **Managed hosts** view.

    • Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. In the **Resource browser**, double-click through the resources to locate and select the required resource.

4. In the Tasks view, select **View Deviations**.

    A tree view displays all resources and all the sub-resources below the root that have explicit security applied to them. As you select resources in the tree, their security displays in the lower pane. To see the deviation warnings or errors encountered for the selected resource, click the **Click here to see warnings and errors** link.

5. Select the **Folder Permissions** tab or **File Permissions** tab.

6. To give a user or group access to the selected resource, click in the lower pane and click **Add rights** in the Tasks view.

    a. Select the account to add and click **Next**.

    b. Select where to apply the permissions.

    c. Select the permissions to add.

    d. If applicable, select to limit the permissions to only objects and containers within the selected container.

    e. Click **Finish**.

    Back on the **Folder Permissions** or **File Permissions** tab, unsaved changes appear bold.

7. To remove access, right-click the required account and select **Remove all explicit permissions**. Click **OK** to confirm the remove operation.

8. To alter the access, select the required user or group, and click in the **Rights** column.

    a. Alter the permissions as required.

    b. Click the **Applies To** column to select how you want the permissions applied.

9. Click the **Save** toolbar button to save your selections.

    You can now browse through the network to ensure that the proper access has been granted or removed.

Assigning an owner to a resource

| NOTE: This functionality is not available for NFS managed hosts.

The resource owner is an important security principle, as the owner can alter the permissions (both DACL and SACL) on any of their resources. This should not be confused with the business owner, which is not a security principle, but rather a concept where ownership is based on use and activity.

Data Governance Edition provides reports that suggest an appropriate resource owner for the data so that the IT department knows who to contact with questions regarding securing the associated resource. You can also access this information through the Resource browser. This information can help your organization clearly identify who owns resources within your organization to meet security and privacy compliance requirements.

For details, see Data owner vs. perceived owner report on page 204 and Calculating perceived owner on page 163.

NOTE: If you see a message in the list of issues that the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

To change the owner for a resource

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

    • Double-click the required managed host in the **Managed hosts** view.

    • Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. In the **Resource browser**, double-click the folder or container to locate the required resource.

4. Select the required resource to display the security for the resource in the lower pane. The security for the resource displays in the lower pane.

    You can use the **Location** field to view your current location. If you have navigated too far, you can move back by clicking the ▣ **Up One Level** button.

5. Select the **Control** tab.

6. The **Current Owner of this item** field displays the resource's current owner. Click **Change Owner** to select a new owner for the resource.

7. Use the **Inheritance From Parent** options to select whether you would like the permissions and auditing settings to be inherited from the selected object.

    • Allow inheritance permissions from the parent to propagate to this object and all child objects.

    • Allow inheritable audit settings from the parent to propagate to this object and all child objects.

8. Click the **Save** toolbar button to save your selections.

NOTE: This is for the NTFS resource owner only. It does not reference the One Identity Manager's concept of Business Owner.

Working with SharePoint security permissions

As with NTFS resources, SharePoint resources must be properly secured to ensure that users have the appropriate access. For information on the configuration necessary to ensure you can properly manage access, see, Working with security permissions on page 132.

Using Data Governance Edition, you can determine who has access to a SharePoint resource, what permissions make up the permission levels that have been assigned, and then manage that access, including the inheritance setting of a resource. If the right permission level does not exist, you can also use Data Governance Edition to create one.

When you change security settings using Data Governance Edition, you are using the One Identity Manager delegation model. This model bypasses native SharePoint to apply the permission changes but the security changes that result use the SharePoint security for enforcement.

Changing the security inheritance on a resource

SharePoint security can either be inherited or unique. If it is inherited, you cannot modify any security settings, as they are defined by a parent resource. A well-structured site can reduce the number of inheritance breakages required to effectively secure your SharePoint resources. When you need to change the setting at a particular point in the hierarchy, you create new unique permissions at that point. By default, all items below the uniquely-permissioned object inherit the settings of its parent.

When you break inheritance, all current permission levels and security settings are copied, and you can then modify them as needed. Although it is easy to change to unique permissions using Data Governance Edition, care should be taken when doing this, as it requires more administration to manage unique permissions.

To change the inheritance on a SharePoint resource

1. In the Navigation view, select **Data Governance** | **Managed hosts**.
2. Open the Resource browser using one of the following methods:
   - Double-click the required SharePoint farm in the Managed hosts view.
   - Select the required SharePoint farm in the Managed hosts view and select **Resource browser** from the Tasks view or right-click menu.

   The web applications for the selected farm display. From here you can browse the SharePoint hierarchy.
3. Double-click through to browse to the required resource.

   When a resource is selected, the security settings for the resource display in the Permissions pane (lower pane).

   One of the following messages appear across the top of the tab indicating whether permissions are inherited or unique:
   - Permissions are unique. Click here to restore inheritance.
   - Permissions are inherited. Click here to break inheritance and edit permissions.
4. To toggle the inheritance setting, click the message.
5. Click **Yes** on the confirmation dialog.

Modifying the permissions on a SharePoint resource

You can add and remove accounts from a SharePoint resource, including sites, libraries, lists, documents, and so on. You can assign Active Directory users and groups, and SharePoint groups. You can also modify the permission levels assigned to each account, if the resource has unique permissions. For more information, see Working with SharePoint permission levels on page 140.

NOTE: If you see a message in the list of issues that the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

To add or remove accounts from a SharePoint resource

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

    - Double-click the required SharePoint farm in the **Managed hosts** view.

    - Select the required SharePoint farm in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

    The web applications for the selected farm display. From here, you can browse the SharePoint hierarchy.

3. Double-click to browse to the required resource.

    When a resource is selected, the security settings for the resource display in the **Permissions** pane (lower pane).

4. To add an account, click **Add Account**, then browse to the required account.

    NOTE: To add SharePoint groups, ensure that you set the Location to SharePoint. Only groups from the current site are shown.

5. In the **Permissions** pane, click in the **Permission Levels** column that corresponds to the newly added account.

    A pop-up appears displaying all the permission levels available. Select the permissions levels to assign to the new account and press **Enter**.

6. To remove an account, select the account in the **Permissions** pane, click **Remove Account** and then click **Yes**.

7. Click the **Save** toolbar button to save your selections.

To modify the permission levels assigned to an account

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

ONE IDENTITY
by Quest

- Double-click the required SharePoint farm in the **Managed hosts** view.
- Select the required SharePoint farm in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

The web applications for the selected farm display in the lower pane.

3. For the account that you want to manage, click in the corresponding **Permission Levels** column to display the permission levels list.

4. Select the required permission levels.

    You can see the permissions included in a permission level by hovering your cursor over the level, and you can hover over an individual permission to see its description.

5. Press **Enter** to save your selections and close the permission levels list.

6. Click the **Save** toolbar button to save your changes.

Working with SharePoint permission levels

SharePoint permissions are a collection of list, site, and personal permissions designed to provide the appropriate level of access for a given group of users. Permission levels are unique for each site collection. Although permission levels are created and managed at the site collection level, Data Governance Edition allows you to manage permissions regardless of your context, and resolves your permission level changes to the appropriate site collection. You can create a permission level at anytime, as long as you have the Manage Permissions permission on the site collection. You can also edit existing permission levels, and delete those you no longer need.

You may want to view the details of existing permission levels before creating new ones. The fewer well-designed permission levels you have, the easier your site permissions are to manage.

NOTE: If you see a message in the list of issues that the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

To view the permissions contained in a permission level by viewing a resource

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. Open the **Resource browser** using one of the following methods:
    - Double-click the required SharePoint farm in the **Managed hosts** view.
    - Select the required SharePoint farm in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. In the **Resource browser**, double-click through the farm to locate the required resource.

    The security for the resource displays in the **Permissions** pane (lower pane).

    A message across the top of the pane indicates whether permissions are inherited or unique.

4. In the **Permissions** pane, click in the corresponding **Permission Levels** column for one of the accounts listed.

   A pop-up appears displaying all the permission levels available. The permission levels assigned to the selected account are marked with a check mark. To see the permissions included in a permission level, hover your cursor over the permission level. You can also hover your cursor over an individual permission to see its description.

5. Press **Enter** to save your selection and close the permission levels list.

To view the permissions contained in a permission level using the Permission Levels dialog

1. In the **Resource browser**, double-click through to a resource within the site you want to examine.

2. In the lower pane, click the **Permission Levels** toolbar button.

3. In the left pane of the **Permission Levels** dialog, select a permission level.

   The permissions included in the level are shown on the right side of the dialog.

4. Click **OK** to close the **Permission Levels** dialog.

Creating a SharePoint permission level

If you need a new combination of permissions to achieve your security goals, you can create it through the **Resource browser**. Regardless of the object you have selected, the permission level is associated with the site collection, and is available for use with any object in the site collection.

To create a SharePoint permission level

1. In the **Resource browser**, double-click through the farm to locate the required resource.

   The security for the resource displays in the lower pane.

2. In the lower pane, click the **Permission Levels** toolbar button.

3. In the **Permission Levels** dialog, click **New**.

4. Provide a unique name and a description for the permission level.

5. Select the required permissions.

   Some permissions are actually collections of permissions. For example, when you select Manage Lists, additional permissions required to perform this task, such as View Pages and Open, are also selected.

6. Click **OK**.

Deleting a SharePoint permission level

If you no longer need a permission level, you can delete it.

NOTE: When you delete a permission level, you may be leaving users or groups without their accustomed access to SharePoint. Ensure that you have assigned appropriate permission levels to all affected accounts before deleting a permission level.

To delete a SharePoint permission level

1. In the **Resource browser**, double-click through the farm to locate the required resource.

   The security for the resource displays in the lower pane.

2. In the lower pane, click the **Permission Levels** toolbar button.

3. In the **Permission Levels** dialog, select the permission level to be removed.

4. Click **Delete**.

5. Click **Yes** on the confirmation dialog.

6. Click **OK** to exit the **Permission Levels** dialog.

Modifying an existing SharePoint permission level

You can change the permissions in a permission level, and the name or description.

To modify an existing SharePoint permission level

1. In the **Resource browser**, double-click through the farm to locate the required resource.

   The security for the resource displays in the lower pane.

2. In the lower pane, click the **Permission Levels** toolbar button.

3. In the **Permission Levels** dialog, in the **Permission Levels** pane (left pane) select the permission level to be modified and click **Modify**.

4. Modify the name, description and included permissions as needed.

5. Click **OK** to save your selections and close the **Permissions** dialog.

Account access modeling

NOTE: This functionality is not available for NFS or Cloud managed hosts.

Before managing user or group access to data (for details, see Managing account access on page 127), you may want to compare the access for two accounts, or model what would happen if you modified an account's group membership.

This enables you to model access including:

- identify common or different access between two users or two groups
- identify why two employees in the same department have different access rights
- identify the access permissions granted or lost by adding/removing users to/from groups

The results of an account comparison shows where there are deviations between the two account's access (different access); and where the accounts hold identical access or have the same access but it was obtained differently (similar access).

You can save the results in customized layouts that will help you to see where and if changes are required to your current account access. For ease of use, Data Governance Edition includes predefined layouts that allow you to see the types of access (differences only, similar only), rights held by the source account only, and rights held by the target account only.

The results of an account simulation shows the rights that would be granted or revoked based on the change made to an account's group membership.

Comparing accounts

Comparing accounts can help you understand the group deployment within your organization. You can easily investigate two groups with similar or identical permissions to determine groups that could be consolidated into one.

Comparing accounts can also be helpful as a troubleshooting tool. If two accounts should have the same access to a resource but one account is being denied access, you can compare their access to see where the differences are found and make the necessary adjustments.

NOTE: If you see a message in the list of issues that the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

To compare accounts

1. Navigate to and select an account (through the **Security Index** node, **Accounts** view, **Security editor**, and so on)
2. Select **Account comparison** in the Tasks view or right-click menu.
3. Select one of the following options to define the type of access to be compared:
   - **Compare explicit and indirect**: Select this option to compare all access, including access granted through group membership. This option is selected by default.
   - **Compare explicit**: Select this option to compare access that has been granted explicitly.

   NOTE: For machine local trustees, well-known group accounts and built-in group accounts, the account comparison will compare only explicit rights, regardless of the option selected.

4. The **Source** field defines the source account to be compared. By default, the selected account appears. Click the ⋯ browse button to locate and select a different source account.

5. The **Target** field defines the target account to be compared. Click the ⋯ browse button to locate and select the target account.

6. The **Resource Types** field defines the types of resources and the managed hosts to be included in the comparison. By default, all resource types and all managed hosts are included.

   Click the **Change** button to limit your comparison to selected resource types or managed hosts. Clicking the **Change** button displays additional fields allowing you to make your selections:

   - **Host**: Click the arrow control to select one or more managed hosts from a list of available managed hosts. To exclude a managed host, click the selected check box to clear it.

   - **Type**: Click the arrow control to select one or more types from a list of available resource types. To exclude a resource type, click the selected check box to clear it.

   NOTE: Running an account comparison against all hosts and resource types could take a significant amount of time to process. It is recommended that you select the hosts and resource types you are interested in to speed up the comparison process.

7. Click **Compare** to run the account comparison for the selected accounts.

   For each resource path to which either account has access, the rights of both accounts are returned. If a column has no entry, that account has no access to the resource. See Account comparison results for more details on how to interpret the results.

8. By default, the Default layout is used to display the results, which shows all resource access available. Other predefined layouts available include:

   - Rights Held by Source Only

   - Rights Held by Target Only

   - Show Differences

   - Show Similar Access

   NOTE: You can use the Layout controls to select a predefined layout for displaying data. If you do not see the **Layout** field or buttons, use the **Toggle layout options** task to display these controls.

   For more information, see Toggle layout options on page 51.

9. (Optional) Click the **Export to CSV** button to export the results to a file. The **Save As** dialog appears allowing you to select the location where the report is to be saved and to specify a file name.

   NOTE: The exported .CSV file contains more information about the account comparison. For example, it contains the managed host ID which can be used to run scripts or commands against a particular managed host.

Account comparison results

The Account comparison feature in the Manager allows you to compare the access for two accounts. The results are grouped by:

- **Different**: Shows account access that is different between the two accounts. That is, where only one account has access or where both accounts have different access to the resource.

- **Similar**: Shows account access that is similar for both of the accounts. This can include access rights that are granted indirectly through the same or different group membership or explicitly through different user accounts.

The account comparison results contain the following details.

Different results

Table 45: Account comparison results: Different

Column	Description
Resource Name	The name of the resource to which one or both of the selected accounts has access.

<Source Account>	Indicates whether the Source account has access to the resource.
	
	• A blank means that the Source account does not have access to the resource. (Only the Target account has access to the resource.)
	
	• A green check mark means that the Source account has access to the resource. See the **Right** and **Via Group** columns to view the rights granted and whether it was granted directly or indirectly through group membership.
	
	   • When the Source account is the only account with access, the type of access is displayed in the **Right** column.
	
	   • When both accounts have access to the resource, but the type of access is different, the type of access is shown in parenthesis after the check mark.

<Target Account>	Indicates whether the Target account has access to the resource.
	
	• A blank means that the Target account does not have access to the resource. (Only the Source account has access to the resource.)
	
	• A green check mark means that the Target account has access to the resource. See the **Right** and **Via Group** columns to view the rights granted and whether it was granted directly or indirectly through group membership.
	
	   • When the Target account is the only account with access, the type of access is displayed in the **Right** column.
	
	   • When both accounts have access to the resource, but the type

Column	Description
	of access is different, the type of access is shown in the parenthesis after the check mark.
Right	The type of access granted to the resource.
Via Group	Displays the name of the account through which the displayed access (**Right** column) was granted. • When a group name appears, this means that the account has indirect rights granted through group membership. • When the user name appears, this means that the account has explicit rights to the resource.
Governed Resource	Indicates whether the resource is governed: • **True**: Resource is governed. • Blank: Resource is not governed.

Similar results

Table 46: Account comparison results: Similar

Column	Description
Resource Name	The name of the resource to which both of the selected accounts have similar access.
<Source Account>	A green check mark indicates that the Source account has access to the resource. • When the same explicit rights are granted through different user accounts, the user account appears in parenthesis (Via *<User Name>*). • When the same indirect rights are granted through different group membership, the group appears in parenthesis (Via *<Group Name>*). • When the same indirect rights are granted through the same group membership, the group appears in the **Via Group** column.
<Target Account>	A green check mark indicates that the Target account has access to the resource. • When the same explicit rights are granted through different user accounts, the user account appears in parenthesis (Via *<User Name>*). • When the same indirect rights are granted through different group membership, the group appears in parenthesis (Via *<Group Name>*). • When the same indirect rights are granted through the same group membership, the group appears in the **Via Group** column.

Column	Description
Right	The type of access granted to the resources.
Via Group	When rights are granted through the same group membership, the name of the group through which the access was granted.
Governed Resource	Indicates whether the resource is governed: • **True**: Resource is governed. • Blank: Resource is not governed.

Simulating the effects of group membership modifications on an account

Simulating changes to group membership enables you to see the access that would be gained or removed if a user or group had a change to their existing group membership.

NOTE: Account membership simulation is not supported for machine local trustees, well-known group accounts or built-in group accounts.

Once you have reviewed the results of the simulation, and before making any changes to the group membership, investigate the group membership on all managed hosts for the selected user or group. For details, see Viewing group membership on page 129 and Managing account access on page 127.

To simulate changes to group membership

1. Navigate to and select an account (through the **Security Index** node, **Accounts** view, **Security editor**, etc.)

2. Select **Account simulation** in the Tasks view or right-click menu.

3. The **Account** field displays the selected account. Click the ⋯ browse button to locate and select a different account.

4. Select the type of modification to be simulated:

    • **Remove from Group(s)**

    • **Add to Group(s)**

5. The **Resource Types** field defines the types of resources and the managed hosts to be included in the simulation. By default, all resource types and all managed hosts are included.

    Click the **Change** button to limit your simulation to selected resource types or managed hosts. Clicking the **Change** button displays additional fields allowing you to make your selections:

    • **Type**: Click the arrow control to select one or more types from a list of available resource types. To exclude a resource type, click the selected check

box to clear it.

- **Host**: Click the arrow control to select one or more managed hosts from a list of available managed hosts. To exclude a managed host, click the selected check box to clear it.

NOTE: Running an account simulation for all hosts and resource types could take a significant amount of time to process. It is recommended that you select the hosts and resource types you are interested in to speed up the simulation process.

6. Click the **Select Groups** button to select the groups to be used in the simulation.

7. In the **Remove Groups or Add Groups** dialog, click the **Browse Groups** button to display the **Select User or Group** dialog. Locate and select the groups to be included in the simulation and click **OK**.

The selected groups appear on the **Remove Groups or Add Groups** dialog.

Click the **Simulate** button.

8. The results of the simulation appears, showing:

- For an **Add to groups** simulation, the resources the selected account will have access to if added to the specified groups.

- For a **Remove from groups** simulation, the resources the selected account would no longer have access to if removed from the specified groups.

See Account simulation results on page 148 for a more detailed description of the simulation results.

9. (Optional) Click the **Export to CSV** button to export the results to a file. The **Save As** dialog appears allowing you to select the location where the report is to be saved and to specify a file name.

NOTE: The exported CSV file contains more information about the account simulation. For example, it contains the managed host ID which can be used to run scripts/commands against a particular managed host.

NOTE: You can use the Layout controls to select a predefined layout for displaying data. If you do not see the **Layout** field or buttons, use the **Toggle layout options** task to display these controls.

For more information, see Toggle layout options on page 51.

Account simulation results

The account simulation feature allows you to simulate changes to group membership before making any changes to the group membership.

- For a "Add to Groups" simulation, you can see the resources the selected account will have access to if added to the specified groups.

- For a "Remove from Groups" simulation, you can see the resources the selected account would no longer have access to if removed from the specified groups.

The results generated by an account simulation contain the following details:

Table 47: Account simulation results

Column	Description
Simulation Type	The type of simulation performed: • Right Granted • Right Revoked
Resource Name	The name of the resource, to which the account would be granted access or revoked access.
Resource Type	The type of resource.
Right	The access rights that would be granted or revoked. • For a "Add to groups" simulation, the right to be granted is prefaced with a plus sign symbol. • For a "Remove from groups" simulation, the right to be revoked is prefaced with a minus sign symbol.
Via Group	The name of the group through which access would be granted or revoked.
Governed Resource	Indicates whether the resource is governed. • True: Resource is governed. • Blank: Resource is not governed.

Bringing data under governance

Controlling access to data is vital to eliminating issues such as security breaches, loss of sensitive information, or non-compliance with external and internal guidelines. You need a process that enables you to:

- Assign business owners.

  Assigning the business owner for a resource to establish the custodian for data should be done with care. This employee can be identified through various reports. For more information, see Managing business ownership for a resource on page 160.

  > NOTE: The assignment of a business owner is an essential component of data governance as this role is inherently part of the compliance workflows. You do not need to assign an owner when you place a resource under governance; however, you cannot assign an owner unless the resource is governed.

- Publish resources to the IT Shop.

  Resource access requests are performed within the web portal for resources located in the IT Shop. For more information, see Publishing resources to the IT Shop on page 155. Requests follow a predefined approval process where the control over

whether the request is approved or denied is made by the assigned business owner and group owners.

- Create policies that allow you to set rules and guidelines surrounding data to ensure its safety, reliability, and accountability.

  Policies and violations can help to identify resources that need to be placed under governance.

  For a list of the governed data company policies provided with Data Governance Edition, see Governed data company policies on page 257

- Establish a data access approval and attestation process to ensure the data stays in a managed state.

  Attestation reviews ensure that the business has a clear statement of an employee's data access and ensure that access to NTFS and SharePoint data is correct.

  The attestation process places responsibility for the attestation review with the data or business owner as they have the best knowledge of the data and its intended use.

  For a list of the governed data attestation policies provided with Data Governance Edition, see Governed data attestation policies on page 255

What is "Governed Data"?

Governing unstructured data allows you to manage data access, preserve data integrity, and provide content owners with the tools and workflows to manage their own data. The workflows cross the Manager and the web portal.

Through the Manager, you can:

- Place resources (folders or shares) under governance.
- Publish resources (folders or shares) to the IT Shop, thereby enabling self-service requests that provide compliance checks.

  NOTE: Publishing resources to the IT Shop is not available for resources on NFS or Cloud managed hosts.

- Identify and assign the business owner for data.
- Create access policies to ensure a system of least privileges

Through the web portal, users have access to:

- IT Shop self-service access requests.
- Access certification processes that ensure proper allocations of resources.
- Policy enforcement systems.
- Views, dashboards, and reports that enable business owners to see the access employees have to all the resources they own and the resource activity on those resources.

Data is considered "governed" when one of the following actions has occurred:

- Resource (folder or share) has been explicitly placed under governance. For more information, see Placing a resource under governance on page 151.
- Resource (folder or share) has been published to the IT Shop. For more information, see Publishing resources to the IT Shop on page 155.

Once data is "governed", the Data Governance server periodically queries the agent responsible for scanning that data and retrieves detailed security information concerning it and any child data. The data is then placed in the central database to be used by policies and attestations.

The Data Governance server also periodically retrieves resource activity summary and security information which is used to calculate perceived ownership suggestions for data under governance. The activity summary information is used for populating various dashboards and views in the web portal and the perceived ownership data is used for reports.

Placing a resource under governance

Identifying data to be governed is continuously adaptive in nature. Those responsible for identifying the data may include the business owner, the administrator, the compliance officer, and managers.

Consider the following when making your selection:

- Monitor "Top Active Content" and "Top Active Users" reports and views in the web portal to locate content that is potentially valuable to the organization.
- Identify enterprise applications that provide the ability to export sensitive information in an unencrypted format.
- Identify content with several access points. For example, if content is available to "Everyone", "All Sales", or "All Employees" you would assume that it is meant for public consumption. However, there is the chance that a sensitive file may be placed in the public area either in error or through malicious intent. It is important to assign a "high risk" index to content with wide access points and bring them under control.
- Identify groups with many members and investigate their data access. Sensitive information could be inadvertently available to people through their group memberships.
- Talk to business owners. They are stakeholders in making the data governance process successful. Understand how they create content and the repositories they use — SharePoint or file servers. They can provide information about the importance of content that is created by the different "roles" in their department or organization. This can identify shares and folders that must be governed and important groups or roles from their perspective.
- Identify trends in "Resource Access Requests" in the web portal IT Shop. If there is an increase in requesting access to a share or a specific SharePoint folder — maybe the resource is a candidate to be watched for activity.

NOTE: For all managed host types, when placing a resource under governance, the resource must be a managed path or a folder or share under a managed path.

- For remote managed hosts and SharePoint managed hosts, if you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. If the managed host has more than one agent assigned, you are prompted to select the agent to which the managed path is added.

- For local managed hosts, if you are scanning managed paths (that is, there are paths in the managed paths list), and you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. However, if you are scanning the entire server (that is, the managed paths list is empty) and you place a resource under governance, no changes are made to the managed paths list and you continue to scan the entire server.

NOTE: On a per host basis, ensure to complete all tasks (such as adding managed paths and placing resources under governance) in the same manner — either at the share or folder level.

NOTE: In order for a DFS link, target share path or folder to be placed under governance or published to the IT Shop, both the DFS server hosting the DFS namespace and the share server where the DFS link is pointing to must be added as managed hosts. If the required servers (those that contain DFS security details) are not already managed, a message box appears listing the servers that need to be added as managed hosts. Click the **Add managed hosts with default options** button to deploy a local agent to the servers listed in the message box and complete the selected operation. Click **Cancel** to cancel the selected operation and manually add the servers as managed hosts.

To place a resource under governance

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

   - Double-click the required managed host in the **Managed hosts** view.

   - Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. Double-click through the resources to locate the required resource (folder or share).

4. Select the required resource (folder or share) and select **Place resource under governance** from the Tasks view or right-click menu.

5. In the **Place resource under governance** dialog, confirm the display name and click **Govern Resources**.

   When placing a share under governance, you can use the backing folder security or share permissions for self-service resource access requests in the web portal. The **Use backing folder security for self-service** option is selected by default and uses the backing folder security for the share. Clear this option to use the share permissions for the share.

   When placing a DFS link under governance, select the type of security to be used:

- **Use Folder Security**: This option is selected by default and uses the backing folder security for self-service resource access requests to this governed resource. The backing folder should be accessible to the Data Governance service and the Data Governance agent service.
- **Use Share Security**: Select this option to use the share permissions for self-service resource access requests to this governed resource.
- **Use DFS Security**: Select this option to use the DFS access-based enumeration security for self-service resource access requests to this governed resource.

Back in the **Resource browser**, "True" now appears in the **Governed Resource** column. The governed resource is also added to the Governed data view.

Managing resources under governance

Once a resource has been placed under governance, you can view details, assign a business owner, and publish the resource to the IT Shop.

NOTE: If you rename or move a resource, the data governance system considers this a new resource that needs to be governed. The original governed resource is marked as "stale". To rectify this, you need to search for the resource in question and place it under governance again.

Also, any associated business ownership that existed needs to be recreated on the new resource.

Managing governed data details

From the Governed data view you can modify the properties assigned to a governed resource, assign a business owner to a governed resource, and publish a governed resource to the IT Shop.

To manage governed resources

1. In the Manager, open the **Governed data** view.
   - From the Data Governance navigation view, select **Governed data**.
   - From the **Managed hosts** view, navigate to the required managed host, select **Governed data** from the Tasks view or right-click menu.
2. Select the required resource, and select **Change governed resource master data** in the Tasks view or right-click menu.

   The General tab displays the resource information, including:
   - Display Name: Displays the display name of the governed resource.
   - Governed Data: Displays the network path and name of the governed data.
   - Resource Type: Displays the type of resource.

- Last collected: Displays the last time the resource security information (and that of its children) was synchronized and included in the One Identity Manager database.

- Available in IT Shop: A check in this check box indicates that the resource is available through the IT Shop.

  NOTE: Select this check box to publish the resource to the IT Shop. For details, see the *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide* or Publishing resources to the IT Shop on page 155.

- Publishing date: Displays the date (UTC) when the resource was published to the IT Shop.

- Date Governed: Displays the date the data was placed under governance.

- No longer found: A check in this check box indicates that the resource was renamed or deleted.

  NOTE: A resource is deemed stale if it has not been scanned by any of your agents or if the resource has been moved or renamed.

- Comments: Displays comments entered about the governed data.

- Risk Index (calculated): Displays the calculated risk of all assignments to this data.

  For a list of the governed data risk index functions provided with Data Governance Edition, see Governed data risk index functions on page 259

  NOTE: Before risk calculations can be performed on governed data, the required schedule must be enabled. In the Designer, select **Base Data | General | Schedules** and enable **Calculate risk indexes of governed data**. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.

3. Select the **Business Owner** tab to assign an owner for the resource or modify the current owner.

   - Owner (Application role): If ownership is assigned to an application role, this displays the name of the role.

   - Owner (Employee): If ownership is assigned to an employee, this displays the name of the employee.

   - Justification: Displays descriptive text entered as justification for assigning the owner to the resource.

   - Date ownership set: Displays the date the owner was last set.

   - Ownership set by: Displays the user who set the ownership to its current owner.

   - Requires ownership: Indicates whether the resource must be assigned a business owner.

   For more information, see Managing business ownership for a resource on page 160.

4. Click the **Save** toolbar button to save your changes.

Removing resources from governance

Removing a resource from governance, also removes it from the IT Shop.

To remove a resource from governance

1. In the Manager, navigate to the required managed host. For example, select the required managed host from the Managed hosts view.

2. Open the Resource browser or the Governed data view.

3. Locate and select the required resource and select the **Remove resources from governance** task or right-click command.

4. Click **Yes** on the confirmation dialog.

Publishing resources to the IT Shop

Publishing a resource to the IT Shop makes it available for users to request access to it. It also places the resource under governance if it is not already governed.

NOTE: In order for a DFS link, target share path or folder to be placed under governance or published to the IT Shop, both the DFS server hosting the DFS namespace and the share server where the DFS link is pointing to must be added as managed hosts. If the required servers (those that contain DFS security details) are not already managed, a message box appears listing the servers that need to be added as managed hosts. Click the **Add managed hosts with default options** button to deploy a local agent to the servers listed in the message box and complete the selected operation. Click **Cancel** to cancel the selected operation and manually add the servers as managed hosts.

Each request is processed by a policy-based approval process, which determines whether access to the data can be assigned or not. Authorized persons, in this case the business owner and group owner, can approve or deny IT Shop requests. The request history also makes it possible to follow who requested what resource and when it was requested, renewed or canceled. For more information on how to make and manage resource access requests, see the *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide*.

You can quickly see all the resources that have been placed under governance and manage (add and remove) resources in the IT Shop from the Resource browser or **Governed data** view in the Manager.

You can publish NTFS shares and folders, and SharePoint objects from the site level and below.

NOTE: This functionality is not available for NFS managed hosts.

NOTE: This functionality is not available for Cloud managed hosts.

To place a resource under governance and publish it to the IT Shop

1. In the Manager, navigate to the required resource.

   For example, to use the **Resource browser**:

   a. Select the required managed host from the **Managed hosts** view.

   b. Double-click to display the **Resource browser**.

   c. Double-click through the resources to locate the required resource.

2. Select the required resource and then select the **Publish to IT Shop** task or right-click command.

3. In the **Publish to IT Shop** confirmation dialog, confirm the display name of the selected resource and click **Publish Resources**.

   When placing a share under governance, you can use the backing folder security or share permissions for self-service resource access requests in the web portal. The **Use backing folder security for self-service** option is selected by default and uses the backing folder security for the share. Clear this option to use the share permissions for the share.

   When placing a DFS namespace under governance, select the type of security to be used:

   - **Use Folder Security**: This option is selected by default and uses the backing folder security for self-service resource access requests to this governed resource. The backing folder should be accessible to the Data Governance service and the Data Governance agent service.

   - **Use Share Security**: Select this option to use the share permissions for self-service resource access requests to this governed resource.

   - **Use DFS Security**: Select this option to use the DFS access-based enumeration security for self-service resource access requests to this governed resource.

4. If the resource has not been assigned a business owner, the **Business Owner** wizard appears allowing you to assign ownership.

   a. On the **Set Business Owner** page, select to assign an application role or employee as the owner, optionally enter a justification for the ownership, and click **Next**.

   b. Click **Finish** to close the wizard.

Back in the **Resource browser**, "True" appears in both the **Governed Resource** and **Published to IT Shop** columns. The assigned business owner is also added to the **Business Owner** column. The governed resource is also added to the Governed data view.

Users are now able to request access to the resource from within the web portal and set in motion the request workflow.

To publish a governed resource to the IT Shop

1. In the Manager, navigate to the governed resource.

   For example, to use the **Resource browser**:

a. Select the required managed host from the **Managed hosts** view.

b. Double-click to display the **Resource browser**.

c. Double-click through the resources to locate the required resource.

For example, to use the **Governed data** view.

a. In the Data Governance navigation view, select **Governed data**.

b. Locate the required resource.

2. Locate and select the governed resource and select the **Publish to IT Shop** task or right-click command.

3. In the **Publish to IT Shop** confirmation dialog, click **Yes**.

4. If the resource has not been assigned a business owner, the **Business Owner** wizard appears allowing you to assign ownership.

a. On the **Set Business Owner** page, select to assign an application role or employee as the owner, optionally enter a justification for the ownership, and click **Next**.

b. Click **Finish** to close the wizard.

Back in the **Resource browser** and **Governed data** view, "True" appears in **Published to IT Shop** column. The assigned business owner is also added to the **Business Owner** column.

To remove a resource from the IT Shop

Removing a resource from the IT Shop, does not remove the item from governance. However, removing a resource from governance removes it from the IT Shop. For information on removing resources from governance, see Removing resources from governance on page 155.

1. Open the **Resource browser** or **Governed data** view.

2. Locate and select the required resource and then select the **Unpublish from IT Shop** task or right-click command.

3. Click **Yes** on the confirmation dialog.

Restricting access to self-service resource access requests

There are various ways of restricting who can see (and consequentially request access to) governed data that has been published to the IT Shop. These include:

- Defining a restriction list based on organizational structure (department, location or cost center).

- Explicitly marking groups for exclusion.

- If the Business Roles module is purchased and installed, defining a restriction list based on business roles.

NOTE: Ask your Data Governance Administrator to set up a restriction list or mark groups to restrict access to your governed data.

Restriction list based on organizational structure

By defining a restriction list, only those employees who are in the specified departments, cost centers or geographical locations are able to see (and request access to) a governed resource.

NOTE: Organizational inheritance is not supported. Each required level of an organizational structure must be added to the restriction list.

To restrict access to a resource in the IT Shop (Data Governance Administrator)

1. In the Manager, open the **Governed data** view.

   - From the Data Governance navigation view, select **Governed data**.

   - From the **Managed hosts** view, navigate to the required managed host, select **Governed data** from the Tasks view or right-click menu.

2. Select the required resource and select **Change governed resource master data** in the Tasks view or right-click menu.

3. Select **Assign organizations** in the Tasks view or right-click menu.

   The **Organizations assignment** page appears, which consists of three tabbed pages (Departments, Locations, and Cost centers) allowing you to select from a list of previously defined organizational assignments.

4. Use the different tabs to define who can see (and request access to) the selected resource. In the lower pane of the tabbed pages, double-click the departments, locations or cost centers to be assigned to the resource. The employees not assigned through the assignment page are restricted from seeing or accessing the resource through the IT Shop.

5. When finished with the assignments, click the **Save** toolbar button.

To restrict access to an owned resource in the IT Shop (Only for Business Owners who also have Data Governance Administrator role)

NOTE: Business owners who have both the **Data Governance** | **Administrators** and **Data Governance** | **Direct Owners** application roles assigned, can use the web portal to define who can see and access owned resources.

1. Log on to the One Identity Manager web portal.

2. From the menu bar, select **Responsibilities** | **My Responsibilities**.

3. On the **My Responsibilities** view, select the **Governed Data** tile.

4. On the **Governed data** view, select a governed resource.

5. Click the **Master data** tab.

6. At the bottom of the properties page, click the **Assign** button to the right of Departments, Locations, or Cost centers.

NOTE: You can also restrict access based on Business Roles or One Identity Manager application roles.

7. In the **Assign** dialog, use the left pane to select the organizational assignment to be assigned to the selected resource.

   Once selected, the assignment appears in the **Assigned** pane (right pane) and the icon to the left of the assignment changes to a check mark. To remove an assignment, select the assignment in the **Assigned** pane. The icon to the left of the assignment changes back to an X and is removed from the **Assigned** pane.

   Click **OK** to save your selections and close the **Assign** dialog.

8. When finished with the assignments, click the **Save** button.

Explicit exclusion of groups

You may want to mark certain groups as being ineligible for self-service requests, especially when Data Governance Edition is configured to allow for non-published groups to be presented. In this case, it is possible to mark either specific groups, or all groups within a particular Active Directory container as being ineligible for access requests.

To explicitly exclude groups

NOTE: Modifying the registry can cause serious issues. Ensure that when making these changes, only the described keys are modified.

1. On the Data Governance server, navigate to the following registry key using regedit.exe:

   HKEY_LOCAL_MACHINE\Software\One Identity\Broadway\Server\DeploymentData\SelfService\ExclusionByDN

   NOTE: The "DeploymentData" and "SelfService" subkeys may not exist. If these keys are not present, they should be created.

2. Beneath the ExclusionByDN key, create string values whose names match the distinguished name of the groups that are to be excluded.

   To exclude an entire container of groups, specify the distinguished name of the container, with an asterisk ("*") prefix. For example to exclude all groups in the Users container of example.com, use the following syntax: "*CN=Users,DC=example,DC=com".

Restriction list based on business role

The Business Role module is an optional module that can be purchased with One Identity Manager. If this module is installed (selected on the **Module selection** page of the Setup wizard), you can restrict employees from seeing (and consequentially requesting access to) governed data that has been published to the IT Shop based on their business role assignments.

By defining a business role restriction list, only those employees who are assigned the selected business roles are able to see and request access to a governed resource.

To restrict access to a resource in the IT Shop (Data Governance Administrator)

1. In the Manager, open the **Governed data** view.

   - From the Data Governance navigation view, select **Governed data**.

   - From the **Managed hosts** view, navigate to the required managed host, select **Governed data** from the Tasks view or right-click menu.

2. Select the required resource and then select **Change governed resource master data** in the Tasks view or right-click menu.

3. Select **Assign business roles** in the Tasks view or right-click menu.

   The **Business Roles assignment** page appears allowing you to select from a list of business roles.

4. In the lower pane, double-click the business roles to be assigned to the resource.

5. When finished with the assignments, click the **Save** toolbar button.

To restrict access to an owned resource in the IT Shop (Only for Business Owners who also have Data Governance Administrator role)

NOTE: Business owners who have both the **Data Governance** | **Administrators** and **Data Governance** | **Direct Owners** application roles assigned, can use the web portal to define who can see and access owned resources.

1. Log on to the One Identity Manager web portal.

2. From the menu bar, select **Responsibilities** | **My Responsibilities**.

3. On the **My Responsibilities** view, select the **Governed Data** tile.

4. On the **Governed data** view, select a governed resource.

5. Click the **Master data** tab.

6. Click the **Assign** button to the right of **Business Roles**.

7. In the **Assign** dialog, use the left pane to select the business roles to be assigned to the selected resource.

   Once selected, the business role appears in the **Assigned** pane (right pane) and the icon to the left of the business role changes to a check mark. To remove a business role, select the business role from the **Assigned** pane. The icon to the left of the business role changes back to an X and is removed from the **Assigned** pane.

   Click **OK** to save your selections and close the **Assign** dialog.

8. When finished with the assignments, click the **Save** button.

Managing business ownership for a resource

Assigning a business owner for a resource enables you to establish the custodian for data. The business owner should be an employee who understands the nature of the data and the list of authorized users. The owner can be an individual employee or all employees in an application role. They should be able to answer important questions such as whether

people who have access to it should, whether it is still relevant, and whether it should be deleted or archived.

The business owner is also the first in line to approve or deny IT Shop requests for resource access.

NOTE: You do not need to assign an owner when you place a resource under governance; however, you cannot assign an owner unless the resource is governed. For more information, see Placing a resource under governance on page 151.

NOTE: Business ownership is not the same as resource ownership, which is a property of the security configuration of the resource.For more information, see Working with security permissions on page 132.

The goal of establishing and assigning ownership is to prevent unauthorized access to data and to be secure in the knowledge of who has access to what within your organization. Once assigned, the business owner grants access, not IT.

Because the business owner is an integral component in the securing of data through access requests and attestations, it is important to schedule a "business owner attestation" to periodically confirm the governed data ownership.

Data Governance Edition can suggest appropriate owners for the data based on usage and access through both reports and through a calculation performed in the Manager. For more information, see Perceived owners for data under governance report on page 205 and Calculating perceived owner on page 163.

Using the web portal, the Data Governance Administrator can view a list of resources without an owner assigned and assign ownership. In addition, as a business owner, you can reject ownership of a governed resource. For more information, see Managing governed resources using the web portal on page 175.

To assign ownership for previously governed resources

1. In the Manager, open the **Governed data** view.

    - From the Data Governance navigation view, select **Governed data**.

    - From the **Managed hosts** view, navigate to the required managed host, select **Governed data** from the Tasks view or right-click menu.

2. Select the governed resource and select **Change governed resource master data** in the Tasks view or right-click menu.

3. Select the **Business Owner** tab to apply an owner for the resource.

    From here, you can select to apply an owner based on an existing application role or to a specific user, enter the reason why the resource requires an owner, and view when the ownership was set and by whom.

    - Owner (Application role): Use this field to assign an owner for the resource based on their application role. If you assign an application role, any holder of this role can be responsible for attestations or access requests. If the application role is not listed in the drop-down menu, click the add button to the right of this field to add a One Identity Manager application role.

- Owner (Employee): Use this field to assign an owner for the resource based on an employee name. If you assign an employee as the owner, they are solely responsible for attestations or access requests.
- Justification: (Optional) Enter the reason for assigning this owner to the resource.
- Date ownership set: Read-only field that displays the date the owner was last set.
- Ownership set by: Read-only field that displays the user who set the ownership to its current owner.
- Requires ownership: (Optional) Select this option to indicate that a resource must be assigned a business owner.

4. Click the **Save** toolbar button to save your selections.

To set a business owner on multiple resources

NOTE: This procedure can also be used as an alternate method of assigning a business owner to a single governed resource.

1. In the Manager, open the **Governed data** view.
    - From the Data Governance navigation view, select **Governed data**.
    - From the **Managed hosts** view, navigate to the required managed host, select **Governed data** from the Tasks view or right-click menu.
2. Select the required resources and select **Set business ownership** in the Tasks view or right-click menu.
3. On the **Set Business Owner** page, select to assign either an application role or an employee as the owner, and enter a justification for the ownership.

    NOTE: If all of the selected resources already have the same business owner set, the employee or application role field will display the current owner assignment.
4. If one or more of the selected resources already have a business owner set, click **Yes** to confirm that you want to override existing settings.
5. Click **Next**.
6. Click **Finish** to exit the wizard.

To revoke ownership

1. In the Manager, open the **Governed data** view.
    - From the Data Governance navigation view, select **Governed data**.
    - From the **Managed hosts** view, navigate to the required managed host, select **Governed data** from the Tasks view or right-click menu.
2. Select the required resource and select **Change governed resource master data** in the Tasks view or right-click menu.
3. Select the **Business Owner** tab and clear the owner field for the resource.
4. Click the **Save** toolbar button to save your selection.

    The account is removed as the owner for that resource.

Calculating perceived owner

The perceived owners for data is calculated from resource activity history and security information collected by Data Governance Edition.

By default, Data Governance Edition uses resource activity history as the primary source and only uses the security information to provide additional perceived ownership suggestions for the resource if the resource activity calculation returns less than two results. By default, the calculation is based on activity recorded for the last 30 days to determine perceived owners. You can, however, change the primary source, maximum number of results to be returned, and activity period used to determine perceived owners using the following server configuration settings:

- PerceivedOwnershipByResourceActivity: Indicates the primary source for calculating perceived owners: resource activity history or security information.

- PerceivedOwnershipByResourceOwner: Indicates whether the access control list owner of the target system should be considered as a perceived owner suggestion.

- PerceviedOwnershipMaxReturnValue: Defines the maximum number of perceived ownership suggestions returned as a result of calculating perceived owners for a resource.

- PerceivedOwnershipActivityPeriod: Defines the time period (in days) to look for past resource activity to determine perceived owners.

For more information on these configuration settings, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Using resource activity history to calculate perceived owners

When resource activity history is available for a resource, the following is considered in the perceived owner calculation:

- The account that performed the activity

- The scope of the data on which activity was performed

- The type and frequency of activity (read, write, create, delete, rename, or security change)

- The time span in which the activity took place

Activity is collected based on the aggregation time span settings and recorded in the Data Governance Resource Activity database. Once all the activity records for the time span in question are gathered, a weight is assigned to each different type of activity. The default calculation assumes that it is more likely that the data owner would create, edit, delete, and change security rather than just read the data, so a heavier weight has been assigned to these change operations. By default, the heaviest weight has been given to change security and a lighter weight to read.

The total weight for all operations is summed for each account, and the accounts with the highest total weight are presented as the calculated perceived owner for the data. If the selected resource is a folder, the activity on all child objects is collated for the resultant weights.

When the perceived owner calculations are based on activity data, the following resource activity collection settings can affect the calculation:

- If an account is excluded from activity collection, that account is never perceived as an owner.
- If a particular resource is excluded through a file extension or a folder exclusion setting, it never has any activity data from which to perceive an owner.
- If the aggregation window is large, changes in perceived owner may take more time to become visible.

The biggest group of settings to affect the perceived owner calculation are the weight multipliers for the different types of actions of resource activity collected by Data Governance Edition. They are responsible for weighting the various activities so that (for example) a user performing a security change operation is more likely to be an owner of a particular resource than another user who has just read that resource. For information on modifying these weight multipliers, see *Activity weight multipliers* in the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Using security to calculate perceived owners

When using security information to calculate perceived ownership, Data Governance Edition considers the following:

- Trustee access
    - Data Governance Edition looks for trustees with access. The following weight priority (highest to lowest) is used for the calculation:

    Cloud managed hosts:
        - owner
        - writer
        - reader

    For information on how Data Governance Edition maps permission levels to these roles, see the *One Identity Data Governance Edition Technical Insight Guide*.

    NFS managed hosts:
        - Full Control
        - Write
        - Manager
        - Read
        - Execute

    NTFS managed hosts:
        - Owner
        - Modify

- Write

- Manager

- Read and Execute

- Read

- List Folder Contents

- Full Control

SharePoint managed hosts:

- Design

- Edit

- Contribute

- Manager

- Read

- View Only

- Limited Access

- Full Control

- Common managers amongst trustees with access to resource

    - Data Governance Edition then tries to find common managers within the One Identity Manager organizational structure.

- Remaining trustee rights

    - Lastly, Data Governance Edition weighs the remaining rights that trustees have (for example, read, limited access, etc.).

- Built-in accounts

    - Data Governance Edition filters out built-in accounts from the perceived owner calculation.

        NOTE: For Cloud manage hosts, Data Governance Edition does not filter out Cloud built-in accounts.

During any of these steps, when Data Governance Edition finds the top perceived ownership suggestions, the process stops looking and returns the results.

To determine perceived owners through the Manager

1. In the Navigation view, select **Data Governance | Managed hosts**.

2. Open the **Resource browser** using one of the following methods:

    - Double-click the required managed host in the **Managed hosts** view.

    - Select the required managed host in the **Managed hosts** view and select **Resource browser** from the Tasks view or right-click menu.

3. Double-click through the resources to locate the required resource.

4. Select the required resource and select **Calculate perceived owners** from the Tasks view or right-click menu.

The calculation is performed to determine the perceived owners.

5. The **Perceived Business Owners** dialog appears showing the results of the calculation.

   - The Governed Data Information appears when the selected resource is under governance. This section indicates whether the resource is published to the IT Shop and whether it has an assigned business owner.

   - The Account grid displays the perceived ownership suggestions (and the associated Employee) with percentage points based on their level of activity or security.

6. To assign an owner based on the perceived owner calculation, select the account from the list and click the **Set Owner** button.

   NOTE: An account is only eligible to be set as an owner if they have an associated One Identity Manager Employee.

   - In order to assign ownership to an NFS Export resource, ensure that an Active Directory employee is assigned to the UNIX account.

     To assign a One Identity Manager Employee to a UNIX account:

     - In the Manager, select **Employees** | **Employees**.

     - Locate and select the employee, right-click and select **Tasks** | **Assign Unix user accounts**.

     - In the lower pane, locate and double-click the account to be assigned to the selected employee.

   - In order to assign ownership to a cloud resource, ensure that an Active Directory employee is assigned to the SHAREPOINTONLINE or ONEDRIVEBUSINESS account.

     To assign a One Identity Manager Employee to a cloud account:

     - In the Manager, select **Employees** | **Employees**.

     - Locate and select the employee, right-click and select **Tasks** | **Assign user accounts**.

     - In the lower pane, locate and double-click the account to be assigned to the selected employee.

   The **Perceived Business Owner** dialog re-appears where the **Current Business Owner** field is now showing the newly selected owner.

7. Click **Close** to save your selection and close the dialog.

Establishing compliance policies

Maintaining consistent access policies to data ensures that a system of least privileges is in place. Through the Manager you can manage company policies and assess the risk involved. Policies can be assigned to compliance frameworks and groups for categorization; they can have accountable and exception approvers, a risk index, and assigned mitigating controls for risk reduction.

Policies can be customized to meet your specific requirements. For example, you can create a company policy such as "Users should not have direct access to NTFS resources" to ensure that access has been granted only through group membership; or you can enable a predefined policy such as "Full access not granted on governed data for the predefined group "Everyone" to ensure that the built-in Active Directory group "Everyone" does not have "Full Control" to data under governance.

Assuming the appropriate data is stored in the database, One Identity Manager determines all the company resources that violate these company policies. Adherence to company policies is checked regularly using scheduled tasks and notification of policy violations are displayed in the web portal.

Regular testing of company policies is managed through schedules. A "default schedule" is assigned to every new company policy. You can customize the supplied schedule to meet your requirements or set up your own schedules and assign them to the company policies.

Processing tasks are created for the DB-Scheduler to test the validity of a company policy. The DB-Scheduler identifies the employees who satisfy company policy and the employees who are in violation of company policy. The specified company policy approvers can test policy violations and if necessary grant exception approval.

For details on managing policies, see Company Policies in the *One Identity Manager Company Policies Administration Guide*.

NOTE: Before a resource can be used in the creation of policies, it must be placed under governance. For more information, see Placing a resource under governance on page 151.

To create a policy

1. In the Navigation view, select **Company Policies** | **Policies**.

2. In the Result list, click the ⊞ **Create** toolbar button or right-click command and select **New** to create a new working copy of the policy.

3. On the policy's **General** properties page, enter all the required information for the policy.

   - **Policy**: Enter the name for the company policy.

   - **Base table**: Select the base table for which the company policy is defined.

   - **Edit condition**: Click the **Edit condition** button to display the WHERE clause wizard to define the policy conditions.

   All other fields and options are optional.

4. Click the **Save** toolbar button to save your policy.

5. In the Tasks view, select **Enable working copy**.

   The company policy is not added to the database until the working copy is enabled. The working copy remains and can be used for making changes to the company policy later.

Classifying governed resources

Classification helps you and the security professionals in your organization understand the contents of your unstructured data, thereby ensuring that sensitive assets are properly secured.

More specifically, the Classification feature in Data Governance Edition provides:

- The ability to classify governed resources. For more information, see Classifying governed resources on page 173.

- The ability to apply company policies based on classification. For details on managing policies, see Company Policies in the *One Identity Manager Company Policies Administration Guide*.

Classification is included in Data Governance Edition, however you should first define the classification levels in Data Governance Edition to match those defined by your company. For more information, see Defining classification levels on page 169.

The following application roles are used for Classification functionality. They are to be used in conjunction with other One Identity Manager roles. For more information, see Application roles on page 59.

Table 48: Classification: Typical users and associated tasks

User	Tasks
Data Governance Administrator	Employees assigned this role are responsible for the management and maintenance of the Data Governance Edition deployment including Classification. Members of this role can: • Define the classification levels for use in the Data Governance Edition deployment. • Assign a classification level to a governed resource. This user must be assigned the **Data Governance** | **Administrators** application role.
Business Owner	Employees assigned this role are responsible, through the web portal, for managing and attesting to the classification of resources that they own. Members of this role can:

User	Tasks
	• View the classification level that is assigned to governed data.
	• Assign a classification level to an owned resource.
	Business owners must be assigned to the **Data Governance** | **Direct Owner** application role, which is automatically assigned when the business ownership is set.

Defining classification levels

Data Governance Edition ships with predefined classification levels; however, you may need to modify these predefined classification levels to match the classification levels defined for your organization. You can use the Manager or Windows PowerShell to add, edit or delete the classification levels in your Data Governance Edition deployment.

By default, the following Classification levels are defined for you:

- **No Restriction**: Information created, received or distributed with the intention of being shared publicly. This includes personal information. Examples: Whitepapers, Approved Technical Documents, Marketing and Sales Brochures, Product launches.

- **Internal Use Only**: Information intended for internal use by the organization and its stakeholders. This includes distribution to associates such as consultants, outside counsel, OEMs, and other team members. Examples: Internal Procedures, Policy Documents, Corporate Directory Information, Facility Information, Organizational Chart.

- **Restricted**: Information intended for internal use by the organization and its stakeholders that requires a heightened level of control. This may include third-party disclosures such as contract agreements. Examples: Personally Identifiable Information (PII), Customer Data, HR Data, Financial Data, IP Formulas/Algorithms, Product Development Concepts.

- **Critical Handling**: Handling requirements are driven by external parties such as customers and regulatory organizations. Examples: U.S. Federal regulatory bodies, Export-Controlled Intellectual Property (IP), Payment Card Industry.

NOTE: When the Data Governance service first starts up, it writes the default classification level data into the One Identity Manager database. This behavior is controlled by a registry key, HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Broadway\Server\ClassificationLevelDefaultData.

If you delete the default classification levels in your Data Governance Edition deployment and replace them with new classification levels, you must move or set this registry key if you move the Data Governance service to another machine to prevent the reloading of previously deleted default classification levels.

If you modify the default classification levels in your Data Governance Edition deployment, the data is retained if you move the Data Governance service to another machine.

For more information about this registry key, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Adding a classification level

You can use the Manager or Windows PowerShell to define a new classification level in your Data Governance Edition deployment.

To add a new classification level (Manager)

1. In the Manager, select **Data Governance** | **Classification**.

   The **Classification** view appears listing the current classification levels defined in your Data Governance Edition deployment.

2. Select the **New** task or right-click command.

3. In the **Classification Level** dialog, enter the following information:

   a. **Name**: Specify the name to be associated with the new classification level.

   b. **Description**: Enter descriptive text to be associated with the new classification level.

   Click **OK** to save the new classification level and close the dialog.

4. Back on the **Classification** view, the new classification level appears at the bottom of the list.

   Use the **Move up** and **Move down** tasks to define where in the display order the new classification level is to appear.

To add a new classification level (PowerShell)

1. If necessary, import the QAM.Client.PowerShell.dll assembly:

   `Import-Module "<path>"`

   Where `<path>` is the file path for the QAM.Client.PowerShell.dll assembly. By default, the `<path>` for the Data Governance server machine is "C:\Program Files\One Identity\One Identity Manager\QAM.Client.PowerShell.dll".

2. Run the following cmdlet to define each classification level:

   `Add-QClassifictionLevel [-Name] <String> [-Description] <String> [[-SortOrder] [<Int>]]`

   - `Name`: Specify the name to be associated with the new classification level.

   - `Description`: Enter descriptive text to be associated with the new classification level.

- SortOrder: (Optional) Specify a value to indicate where in the display order the new classification level is to appear.

  NOTE: The classification levels are displayed in ascending order based on SortOrder. If no SortOrder value is specified, the classification level will appear at the top of the list.

Editing a classification level

You can use the Manager or Windows PowerShell to edit an existing classification level in your Data Governance Edition deployment.

NOTE: Any Data Governance Edition customizations (such as attestation or company policies) that use the name of a classification level, will no longer work if you edit the name of the classification level.

To edit a classification level (Manager)

1. In the Manager, select **Data Governance** | **Classification**.
2. Select the classification level to be modified.
3. Select the **Edit** task or right-click command.
4. In the **Classification Level** dialog, edit the following information as required:

   a. Name: Specify a different name to be associated with the new classification level.

   b. Description: Edit the descriptive text to be associated with the new classification level.

   Click **OK** to save your changes and close the dialog.

5. If necessary, use the **Move up** and **Move down** tasks to define where in the display order the classification level is to appear.

To edit a classification level (PowerShell)

1. If necessary, import the QAM.Client.PowerShell.dll assembly:

   Import-Module "<path>"

   Where <path> is the file path for the QAM.Client.PowerShell.dll assembly. By default, the <path> for the Data Governance server machine is "C:\Program Files\One Identity\One Identity Manager\QAM.Client.PowerShell.dll".

2. Run the following cmdlet to define each classification level:

   Set-QClassificationLevel [-ID] <String> [[-Name] [<String>]] [[-Description] [<String>]] [[-SortOrder] [<Int>]]

   - ID: Specify the Identifier of the classification level to be modified.

     NOTE: Run the **Get-QClassificationLevelConfiguration** cmdlet to retrieve a list of configured classification levels, including their assigned identifiers.

- Name: Specify to change the name associated with the specified classification level.

- Description: Specify to change the descriptive text to be associated with the specified classification level.

- SortOrder: Specify to change where in the display order the classification level is to appear.

  NOTE: The classification levels are displayed in ascending order based on SortOrder.

Removing a classification level

You can use the Manager or Windows PowerShell to remove a classification level from your Data Governance Edition deployment.

TIP: Deleting a classification level will automatically remove it from all associated governed data. Run the **Get-QDataUnderGovernanceByClassificationLevel** cmdlet to retrieve a list of the resources still assigned to the classification level before running the delete operation.

NOTE: Any Data Governance Edition customizations (such as attestation or company policies) that use the name of a classification level, will no longer work if you remove the classification level.

To remove a classification level (Manager)

1. In the Manager, select **Data Governance | Classification**.

2. Select the classification level to be removed.

3. Select the **Delete** task or right-click command.

4. Select **Yes** on the **Delete Classification Level** confirmation dialog.

To remove a classification level (PowerShell)

1. If necessary, import the QAM.Client.PowerShell.dll assembly:

   Import-Module "<path>"

   Where <path> is the file path for the QAM.Client.PowerShell.dll assembly. By default, the <path> for the Data Governance server machine is "C:\Program Files\One Identity\One Identity Manager\QAM.Client.PowerShell.dll".

2. Run the following cmdlet to define each classification level:

   Remove-QClassificationLevel [-ID] <String>

   - ID: Specify the identifier assigned to the classification level to be removed.

     NOTE: Run the **Get-QClassificationLevelConfiguration** cmdlet to retrieve a list of configured classification levels, including their assigned identifiers.

Classifying governed resources

Data Governance administrators and business owners can apply a previously defined classification level to governed resources.

- As a Data Governance administrator, use the Set-QClassificationLevelOnDuG PowerShell cmdlet to classify governed data.
- As a business owner, use the **Classification** page in the web portal to classify an owned resource.

To classify governed data (PowerShell)

1. If necessary, import the QAM.Client.PowerShell.dll assembly:

   Import-Module "<path>"

   Where <path> is the file path for the QAM.Client.PowerShell.dll assembly. By default, the <path> for the Data Governance server machine is "C:\Program Files\One Identity\One Identity Manager\QAM.Client.PowerShell.dll".

2. Run the following cmdlet to assign a classification level to a governed resource:

   Set-QClassificationLevelOnDuG [-DuGId] <String> [-ClassificationLevelId] <String> [[-Justification] [<String>]]

   - DuGId: Specify the identifier assigned to the governed resource to be classified (that is, value assigned to UID_QAMDuG parameter).

     NOTE: Run the **Get-QDataUnderGovernance** cmdlet to retrieve a list of governed resources, including their assigned identifiers.

   - ClassificationLevelId: Specify the identifier assigned to the classification level to be assigned (that is, value assigned to UID_QAMClassificationLevelMan parameter).

     NOTE: Run the **Get-QClassificationLevelConfiguration** cmdlet to retrieve a list of configured classification levels, including their assigned identifiers.

   - Justification: (Optional) Enter the reason for assigning this classification level.

To classify an owned resource (web portal)

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.
2. On the **My Responsibilities** view, select the **Governed Data** tile.
3. Open the **All my resources** tab and select the resource.
4. Click **Classification** to display the current classification level assignment.
5. From this page, you can assign a classification level to the selected resource:

   - **Classification level**: Select a classification level from the drop-down menu.
   - **Description**: Read-only field displaying the description of the selected classification level.

- **Justification**: (Optional) Enter a reason for assigning this level of classification to the resource.

6. Click **Save**. A "Your changes have been saved" message appears at the top of page.

Managing governed resources using the web portal

Data governance provides a systematic approach to managing data access, preserving data integrity, and providing you with the tools and workflows to manage your data resources, without relying on IT administrators. By evaluating resource access, you can identify resources that do not have ownership, assign owners, and assess the overall ownership of your governed data.

NOTE: The resource activity data is from the QAMPoIActivity table. Therefore, the activity data shown is based on the POI collection frequency and when the activity occurred. That is, every time POI data is collected for governed data, existing activity entries are replaced with the new activity data that is collected.

Table 49: Who uses the web portal to manage governed resources

User	Governed resource task

Data Governance Administrator	As a Data Governance Administrator, you can perform the following tasks from the **Responsibilities** | **Governance Administration** view:
	
	• **Governed Data Overview**: View statistics and additional details about all governed resources:
	
	  • **Statistics**: View statistics:
	
	    • Top 10 active resources across all governed resources
	
	    • Total number of explicit security deviations
	
	    • Total number of items with blocked security inheritance
	
	  • **Resource overview**: View governed resources by resource type.
	
	  • **Resources with activity**: View the resources with the most activity.
	
	  • **All resources**: View all governed resources in your Data Governance Edition deployment.
	
	For more information, see Governed Data Overview (Data

User	Governed resource task
	Governance Administrator) on page 178.
	• **Governed Data Ownership**: View all governed data that has no assigned owner and assign ownership.
	For more information, see Data Governance Administrator responsibilities on page 185.
	NOTE: Data Governance Administrators must be assigned the **Data Governance** | **Administrators** or the **Identity & Access Governance** | **Compliance & Security Officer** application role.
Business owner	As a business owner of a governed resource, you can perform the following tasks against resources for which you are responsible:
	Responsibilities | **My Responsibilities** | **Governed Data** view:
	• **All my resources**: View a list of governed resources for which you are responsible.
	• **Statistics**: View statistics:
	• Resources with and without policies
	• Top 10 active resources you own
	• Top 10 active users of owned resources
	• Owned resources grouped by host
	• **Activity**: View the most active resources.
	• **Resource types**: View owned resources by resource type.
	• **Policy violations**: View owned resources currently affected by company policies.
	In addition, for each individual resource, you can drill down to perform the following tasks:
	• **Overview**: View a graphical representation of a resource with its necessary details.
	• **Master data**: View the properties of a resource and reject ownership of a resource.
	NOTE: Business owners who have both the **Data Governance** | **Administrators** and **Data Governance** | **Direct Owners** application roles assigned, can modify the properties of a resource.
	• **Classification**: View classification level assignment and assign a classification level to an owned resource.
	• **Recent activity**: View the resource's activity over the last seven days (by default).

User	Governed resource task

- **Access**: View employees who have access to the resource or who have actually accessed the resource.
- **Access Analysis**: Analyze access by organizational structure.

  NOTE: Access analysis data is not available for cloud managed hosts.

- **Reports**: Generate reports for governed resources.
- **Folders**: View a list of folders with blocked security inheritance, folders with deviated security indexes, and governed folders contained within the selected share.
- **Risk**: View a risk analysis about a resource.
- **Attestation**: View attestation cases.
- **Usage**: View accounts and groups that have access to the resource and request modifications of access rights.

For more information, see Business owner responsibilities on page 188.

NOTE: Business owners must be assigned the **Data Governance | Direct Owners** application role which is automatically assigned when ownership is set.

Auditor	Auditors can perform the following tasks from the **Responsibilities | Auditing** view in the web portal:

- **Governed data**: View a list of managed hosts and the governed data for a managed host.
- **Active Directory**: View the access permissions for an Active Directory resource.
- **Employees**: View the group membership of a given employee and detailed access control information for governed data.

For more information, see Auditor responsibilities on page 197.

NOTE: Auditors must be assigned the **Identity & Access Governance | Auditors** application role.

Governed Data Overview (Data Governance Administrator)

The **Governed Data Overview** view provides information to assist you in governing resources. As a Data Governance Administrator, select **Responsibilities** | **Governance Administration** | **Governed Data Overview** to view statistics for and a list of all governed resources.

NOTE: The statistics displayed on the **Statistics** page are calculated on an hourly schedule. To change the schedule, edit the hourly schedule defined in the **QAM statistics** schedule in the Designer (**Getting Started** | **Edit schedules** or **Base Data** | **General** | **Schedules**).

In addition: for the security statistics:

- For the resource activity statistic, ensure the **Collect and aggregate events** option is enabled on the **Resource activity** page in the **Managed Host Settings** dialog. For more information on this resource activity setting, see Resource activity page.

- For the security statistics, set the **CollectPoi.IncludeDeviations** configuration setting to true. You can find this configuration setting in the Data Governance service configuration file (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\DataGovernanceEdition.Server.exe.config). For more information on this configuration setting, see the *One Identity Data Governance Edition Technical Insight Guide*.

NOTE: The resource activity data is from the QAMPoIActivity table. Therefore, the activity data shown is based on the POI collection frequency and when the activity occurred. That is, every time POI data is collected for governed data, existing activity entries are replaced with the new activity data that is collected.

Table 50: Governed Data Overview

Tabs	Description
Statistics	Displays the following statistics for all governed resources: • Top 10 active resources across all governed resources • Total number of explicit security deviations • Total number of items with blocked security inheritance Clicking **Help** displays additional details about the statistic: • Statistics information: A description of what is contained in the graph and the calculation schedule used to generate it. • View source data: The source data used to build the graph.

Tabs	Description
Resource overview	Displays a list of all governed resources, grouped by resource type. From this view, you can review the following information for each type of resource: • Resources (total): Number of resources of this type. • Not owned: Number of resources not owned. • Owned: Number of resource owned. • Percent not owned: Percentage of resources not owned. • Unique data owners: Number of resources with unique data owners. Clicking a resource type displays a list of resources of that type. From this view, you can review the following information for each resource of the selected type: • Path • Governed data type • Owner • Risk index (calculated) • Requires ownership (Yes or No) Clicking an individual resource (**Path**) displays additional detailed about the selected resource. For more information, see Resource's Governed Data view on page 181.
Resources with activity	Displays the top 10 most active governed resources in your Data Governance Edition deployment.
All resources	Displays a list of all the governed resources in your Data Governance Edition deployment. It includes the following information: • Governed data element name • Element type • Data container • Complete folder path • Data owner • Risk index Clicking an individual resource (**Governed data element name**) from this list displays additional details about the selected resource. For more information, see Resource's Governed Data view on page 181. NOTE: If you are not seeing the governed resources you are expecting, check to ensure that the following parameter is set for these governed resources: QAMDuG.IsPointOfInterest = true.

Tabs	Description
	If business ownership for governed resources is set programmatically or through the Object Browser, you must set QAMDuG.IsPointOfInterest = true. Note that business ownership is indicated by setting values for either QAMDuG.UID_PersonResponsible or QAMDuG.UID_AERoleOwner.

Governed Data Overview (Business Owner)

The **Governed Data Overview** view provides information to assist you in governing resources. As a business owner, select **Responsibilities** | **My Responsibilities** | **Governed Data** to view a list of resources for which you are responsible.

NOTE: The resource activity data is from the QAMPoIActivity table. Therefore, the activity data shown is based on the POI collection frequency and when the activity occurred. That is, every time POI data is collected for governed data, existing activity entries are replaced with the new activity data that is collected.

Table 51: Governed Data Overview

Tabs	Description
All my resources	Displays a list of all the governed resources to which you are assigned the business owner. It includes the following information: • Path • Governed data type • Risk index (calculated) Clicking an individual resource (**Path**) from this list displays additional details about the selected resource. For more information, see . NOTE: If you are not seeing the governed resources you are expecting, check to ensure that the following parameter is set for these governed resources: QAMDuG.IsPointOfInterest = true. If business ownership for governed resources is set programmatically or through the Object Browser, you must set QAMDuG.IsPointOfInterest = true. Note that business ownership is indicated by setting values for either QAMDuG.UID_PersonResponsible or QAMDuG.UID_AERoleOwner.
Statistics	Displays a graphical overview of the governed resource you own: • Resources with and without policy violations

Tabs	Description
	• Top 10 active resources you own • Top 10 active users of owned resources • Owned resources, grouped by host Clicking **Help** displays additional details about the statistic: • Statistics information: A description of what is contained in the graph and the calculation schedule used to generate it. • View source data: The source data used to build the graph.
Activity	Displays the top 10 most active governed resources for which you are responsible.
Resource types	Displays a list of resources for which you are responsible, grouped by resource type. This view displays the resource type and the total number of governed resources of each type. Clicking a resource type displays a list of owned resources of that type along with the calculated risk index for each resource. Clicking an individual resource (**Path**) displays additional detailed about the selected resource. For more information, see Resource's Governed Data view on page 181.
Policy violations	Displays a list of resources that are currently in violation of a company policy. Clicking an individual resource (**Path**) displays additional details about the selected resource. For more information, see Resource's Governed Data view on page 181.

Resource's Governed Data view

A governed resource's **Governed Data** view appears when you click an individual resource from the **Governed Data Overview**. This view consists of the following tabbed pages which provides additional details about the selected resource.

Table 52: Resource's Governed Data view

Tab	Description
Overview	A hyper view (graphical representation) of relations between the resource and One Identity Manager.
Master data	The resources' properties, including the ownership properties of a resource. | NOTE: Business owners who have both the **Data Governance**	

Tab	Description
	Administrators and **Data Governance	Direct Owners** application roles assigned, can modify the properties of a resource.
Classification	Classification level assignment.
	In addition to viewing the classification level assignment, you can assign a classification level to an owned resource.
Recent activity	The activity logged against the resource in the last seven days.
Access	The access permissions assigned to an account or group.
	If the permissions are not set correctly, you can request to modify them.
Access Analysis	A graphical representation and details gathered from analyzing access based on organizational structure. This view consists of the following tabs:

- **Access analysis on *<resource type>***: For the selected resource, this page displays graphs showing the access rights assigned to people based on organizational structure.

  NOTE: Access analysis data is not available for cloud managed hosts.

- **Access analysis on backing folder permissions**: For the backing folder associated with the resource, this page displays different graphs showing the access rights assigned to people based on organizational structure.

- **Access Details**: This page displays a list of the people used in the access analysis of the selected resource.

The following access analysis is performed and presented:

- Access analysis by department

  NOTE: In order for the department association to display properly, the **Primary department** property must be set on the **Change master data | Organizational** tab for an employee.

- Access analysis by primary role title

  NOTE: In order for the primary role association to display properly, the **Primary business role** property must be set on the **Change master data | Organizational** tab for an employee.

- Access analysis by location

  NOTE: In order for the location association to display properly, the **City** property associated with the location must be set. That is, set the **Primary location** property on the **Change master data | Address** tab for an employee, and the **City** property on

Tab	Description
	the **Organizations** | **Locations** | *\<location\>* | **Change master data** | **Address** tab.

- Access analysis by access assignment method. Valid access assignment methods are:

  - Alias

  - Deleted

  - Domain

  - Domain Group

  - Domain User

  - Invalid

  - Machine Local Group

  - Machine Local User

  - Office 365 User

  - OneDrive for Business Group

  - SharePoint Claim

  - SharePoint Group

  - SharePoint Identifying Claim

  - SharePoint Online Group

  - Special

  - Unix Group

  - Unix Owner

  - Unix Other

  - Unknown account or group

  - Unknown assignment type

  - Well Known

The data is displayed in pie charts; however, clicking the **Grid view** link will pop up a dialog that displays the data in a grid format.

Clicking a segment in a pie chart or the **View People** button in the grid view displays a list of the people associated with the selected item.

Tab	Description
Reports	A list of Data Governance Edition reports that can be generated for the resource.
Folders	For shares, the folders contained within the selected share. This view consists of the following tabs:

- Folders with blocked security inheritance

Tab	Description
	• Folders with deviated security indexes
	• All folders, which contains a list of the governed folders which are contained within the selected share.
	Clicking a folder from one of these views displays additional details about the selected folder.
Risk	Risk analysis for a resource including the properties and assignments that contribute to the calculated risk index.
Attestation	The attestation cases found for the object.
Usage	A list of employees who have accessed or may access the resource.

Auditing - Managed Hosts view

The **Auditing - Managed Hosts** view displays a list of managed hosts or the governed data for a given managed host. As an auditor, select **Responsibilities** | **Auditing** | **Governed data** to display this view in the web portal.

The view displays the following information for all manged hosts in your Data Governance Edition deployment:

- Display value
- Host type
- Count of governed resources
- Count of points of interest

Clicking a managed host (**Display value**) or the **Show governed data** button in the **Action** column displays the **Auditing - Governed data** view, which includes the following additional details:

- Path
- Governed data type
- Risk index (calculated)

Clicking a governed resource (**Path**) from this view displays the resource's governed data view. For more information, see Resource's Governed Data view on page 181.

Clicking the **View Content** button in the **Action** column displays the governed data for the selected managed host.

Data Governance Administrator responsibilities

Data Governance Administrators will see an additional **Governance Administration** submenu under the **Compliance** and **Responsibilities** menus in the web portal.

From the **Responsibilities | Governance Administration** view, Data Governance Administrators can:

- Use the **Governed Data Overview** view to review statistics, activity, and details about governed resources. For more information, see Reviewing resource statistics and details on page 185.

- Use the **Assign ownership** view to view all governed resources that have no assigned owner. From this page, you can then assign ownership to these resources. For more information, see Assigning ownership to a governed resource on page 186.

In addition, if you are a business owner of governed data (with the **Data Governance | Direct Owners** application role), you can use the **Governed Data** menu item to perform these additional business owner tasks:

- Modify resource properties. For more information, see Modifying resource properties on page 189.

- Make a governed resource available in the IT Shop. For more information, see Making a governed resource available in the IT Shop on page 189.

- Generate additional Data Governance Edition reports. For more information, see Generating governed data reports on page 194.

See Business owner responsibilities for the tasks all business owners can perform using the web portal.

Reviewing resource statistics and details

Use the **Governed data overview** view to review statistics and details about the governed resources in your Data Governance Edition deployment.

To review resource statistics and details

1. From the menu bar, select **Responsibilities | Governance Administration**.

2. On the **Governance Administration** view, select the **Governed Data Overview** tile.

   The **Governed data** overview view appears which consists of four tabbed pages.

3. Open the **Statistics** tab to display a graphical overview of all governed resources. The Statistics available include:

- Top 10 active resources across all governed resources
- Total number of explicit security deviations
- Total number of items with blocked security inheritance

4. Open the **Resource overview** tab to display all governed resources, grouped by resource type.

5. Open the **Resources with activity** tab to display a list of resources with recent activity.

6. Open the **All resources** tab to review a list of all the governed resources.

7. Clicking a resource from any of these views displays the **Governed Data** view for that resource, which contains additional details about the selected resource.

Assigning ownership to a governed resource

The **Assign ownership** view displays a list of all governed resources that have no assigned owner. From this page, you can assign ownership to these resources.

NOTE: An account is only eligible to be set as an owner if they have an associated One Identity Manager Employee.

- In order to assign ownership to an NFS Export resource, ensure that an Active Directory employee is assigned to the UNIX account.

  To assign a One Identity Manager Employee to a UNIX account:

  - In the Manager, select **Employees** | **Employees**.
  - Locate and select the employee, right-click and select **Tasks** | **Assign Unix user accounts**.
  - In the lower pane, locate and double-click the account to be assigned to the selected employee.

- In order to assign ownership to a cloud resource, ensure that an Active Directory employee is assigned to the SHAREPOINTONLINE or ONEDRIVEBUSINESS account.

  To assign a One Identity Manager Employee to a cloud account:

  - In the Manager, select **Employees** | **Employees**.
  - Locate and select the employee, right-click and select **Tasks** | **Assign user accounts**.
  - In the lower pane, locate and double-click the account to be assigned to the selected employee.

To assign ownership to a governed resource

1. From the menu bar, select **Responsibilities** | **Governance Administration**.

2. On the **Governance Administration** view, select the **Governed Data Ownership** tile.

The **Assign ownership** view appears, which lists the governed resources that currently have no assigned owner. By default this includes all resources with no assigned owner on all managed hosts; however, you can use the **Managed host** drop-down menu to limit the display to resources on a single managed host. You can also use the **Search** control to search for a specific resource.

3. On the **Assign ownership** view, select the check box to the left of the governed resource to which you want to assign ownership. You can select multiple resources in the list if you want to assign the same owner.

   NOTE: Clicking on a resource in the list displays the **Overview** page (hyper view of related data) for the resource and provides access to other details about the selected resource.

4. For resources with a perceived owner listed:

   a. Click the **Assign** button in the Perceived owners column.

      TIP: For governed resources with a perceived owner, you do not need to select the check box to the left of the resource to use the **Assign** button..

   b. In the **Perceived owners** dialog, select the required account and click the corresponding **Assign owner** button.

   c. If the suggested accounts are not sufficient, click the hyperlink at the bottom of the dialog to select another employee.

      • In the **Assign owner** dialog, click the **Assign** or **Change** button to display a list of employees.

      • In the **Owner (Employee)** dialog, locate and select an employee.

      • In the **Assign owner** dialog, the selected employee appears, click the **Assign ownership** button.

5. For resources without a perceived owner listed:

   a. Click the **Assign owner** button (bottom right corner of grid).

      TIP: For governed resources without a perceived owner, you must select the check box to the left of the resource to enable the **Assign owner** button.

   b. In the **Assign owner** dialog, click the **Assign** button to display a list of employees.

   c. In the **Owner (Employee)** dialog, select an employee from the list.

   d. In the **Assign owner** dialog, the selected employee appears. Click the **Assign ownership** button.

      NOTE: Prior to selecting the **Assign ownership** button, you can click the **Change** button to assign a different owner.

6. On the **Assign ownership** view, a message appears at the top of the page stating how many resources have been assigned to the selected employee and the resource is no longer displayed.

Business owner responsibilities

If you are a business owner of governed resources, a **Governed Data** tile appears on the **My Responsibilities** view. Clicking the **Governed Data** tile displays the Governed Data view and selecting **All my resources** provides a list of the resources under your ownership. For each resource you own, the following tabbed pages are available where you can perform tasks to manage the resources you own:

- **Overview**: Use to view a graphical representation of a resource with its necessary details.

- **Master data**: Use to view the ownership properties of a resource and reject ownership of a governed resource. For more information, see Rejecting the ownership of a governed resource on page 190.

  > NOTE: Business owners who have both the **Data Governance** | **Administrators** and **Data Governance** | **Direct Owners** application roles assigned, can also modify the properties of an owned resource. For more information, see Modifying resource properties on page 189.

- **Classification**: Use to view classification level assignments and assign a classification level to an owned resource. For more information, see Viewing and assigning classification level to owned resources on page 190.

- **Recent activity**: Use to view the activity logged for the resource in the last seven days (by default).

- **Access**: Use to view accounts and groups that have access to the resource and request modifications of access rights. For more information, see Viewing groups and accounts with access permissions for governed resources on page 192 and Changing access permissions for a governed resource on page 193.

- **Access Analysis**: Use to analyze access by organizational structure. For more information, see Analyzing access by organizational structure on page 193.

  > NOTE: Access analysis data is not available for cloud managed hosts.

- **Reports**: Use to generate reports for the resource. For more information, see Generating governed data reports on page 194.

- **Risk**: Use to view a risk analysis about a resource. For more information, see Viewing the risk analysis for an owned resource on page 196.

- **Attestation**: Use to view attestation cases.

- **Usage**: Use to view employees who have access to a resource or who have actually accessed the resource. For more information, see Analyzing governed data access on page 196.

Modifying resource properties

NOTE: Only business owners who have both the **Data Governance | Administrators** and **Data Governance | Direct Owners** application roles assigned, can use the web portal to modify resource properties.

The **Master data** page for a governed resource displays the selected resource's properties. The properties on this page are read-only to business owners; however, if the business owner is also a Data Governance Administrator (that is, has the **Data Governance | Administrators** and **Data Governance | Direct Access** application roles both assigned), the properties can be edited as described below.

NOTE: Owners of shares created using the **New file system share** self-service request in the IT Shop will not be able to modify these properties. The owner can, however, add a comment and define who can request access to the governed resource.

To modify the properties of a governed resource

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select a resource.

4. Click **Master data** to display the resource's properties.

5. From this page, you can assign or modify the following properties:

   - Owner (Employee)
   - Owner (Application role)
   - Available in IT Shop

   You can also add or modify the following information:

   - Justification (owner change)
   - Comments

   In addition, you can define who can request access to the governed resource based on Department, Location, Cost center, Business roles, or One Identity Manager application roles.

6. After making your modifications, click **Save** to save your selections.

Making a governed resource available in the IT Shop

NOTE: Only business owners who have both the **Data Governance | Administrators** and **Data Governance | Direct Owners** application roles assigned, can use the web portal to modify resource properties.

The **Master data** page for a governed resource contains the properties for the resource, including whether the resource is available through the IT Shop. As a Data Governance

Administrator who is also a business owner, you can publish an owned resource to the IT Shop from this page.

To make an item available in the IT Shop

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select a resource.

4. Click **Master data** to display the resource's properties.

5. Select the **Available in IT Shop** check box.

   This resource can now be requested by other users through the IT Shop.

6. Click the **Save** button.

Rejecting the ownership of a governed resource

The **Master data** page for a governed resource contains the properties for the resource, including the ownership assigned to the resource. As a business owner, you can reject ownership of a governed resource using this page.

To reject the ownership of a resource

1. From the **Home** page, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select a resource.

4. Click **Master data** to display the resource's properties.

5. Click the **Reject ownership** button at the bottom of the page.

6. In the **Reject Ownership** dialog, enter a reason in the text box and click **Submit**.

   An email request is immediately sent and not added to the shopping cart.

To view the resource ownership rejection request, navigate to **Request** | **My Requests** | **Request History**.

Viewing and assigning classification level to owned resources

As a business owner, you can use the web portal to see what classification level is assigned to the resources you own. The classification level information is available on the following pages in the **Governed Data** view:

- **Overview**: The **Governed Data** pane on this page provides a read-only view of the classification level assigned.

- **Classification**: The current classification assignments are displayed on this page.

These pages contain the following details related to classification for the selected resource.

Table 53: Owned resource properties related to classification

Property	Description
Classification Level	The classification level assigned to the resource. NOTE: On the **Classification** page, this field contains a drop-down menu allowing you to assign a different classification level to the selected resource.
Description	Descriptive text (read-only) associated with the selected classification level. This field is only available on the **Classification** page.
Justification	Use this text box to enter a reason for assigning the current classification level. This field is only available on the **Classification** page.

To view classification level assigned to owned resources

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select the resource.

4. Open one of the following pages to view the current classification level assignment:

   - Overview

   - Classification

   NOTE: In addition to viewing the properties on the **Classification** page, you can assign a different classification level to the selected resource.

To classify an owned resource (web portal)

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select the resource.

4. Click **Classification** to display the current classification level assignment.

5. From this page, you can assign a classification level to the selected resource:

   - **Classification level**: Select a classification level from the drop-down menu.

   - **Description**: Read-only field displaying the description of the selected classification level.

- **Justification**: (Optional) Enter a reason for assigning this level of classification to the resource.

6. Click **Save**. A "Your changes have been saved" message appears at the top of page.

Viewing groups and accounts with access permissions for governed resources

The **Access** page for a governed resource displays all Active Directory groups and accounts that have at least one of the five access permissions to the resource:

- AllowChangePermissions: This is checked when "Change Permissions" access control is allowed.
- AllowFullControl: This is checked when "Full Control" access control is allowed.
- AllowRead: This is checked when any type of read permission (such as, Read Permissions, Read Attributes, List Folder/Read Data) is allowed.
- AllowWrite: This is checked when any type of write permission (such as, Create Files/Write Data, Write Attributes, Write Extended Attributes) is allowed.
- AnyAllow: This is checked when any "Allow" permissions are specified.

NOTE: Access control entries on governed resources, as displayed in the web portal by a business owner, may not always appear as expected. For example, the access right "List Folder Contents" will show as "AllowRead" and "AnyAllow" in the web portal. This is because the List Folder Contents right enables the "allow" read permissions.

In addition, if the assigned permissions are not correct, you can submit a request to remove an access permission or modify the access permissions for a resource. For more information, see Changing access permissions for a governed resource on page 193.

To view the groups and accounts with access permissions for a governed resource

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.
2. On the **My Responsibilities** view, select the **Governed Data** tile.
3. Open the **All my resources** tab and select the resource.
4. Click the **Access** tab.
5. Select the **Show assigned permissions** option.

   The Active Directory accounts that are directly on the security descriptor for the resource appear. The access permissions assigned to each account or group is also displayed.

   (Optional) Select the **Include accounts of type "Alias" and "Wellknown"** check box to include those accounts in the access permissions grid.

6. Select the **Show effective permissions** option to expand groups so you can then drill down to see the actual members of the group that have access to the selected resource.

Changing access permissions for a governed resource

The **Access** page for a governed resource displays all Active Directory groups and accounts that have at least one of the five access permissions to the resource. In addition, if the security settings on this resource are incorrect, you can submit a request to modify the access rights.

To change the access permissions for a resource

1. From the menu bar, select **Responsibilities | My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select the resource.

4. Click the **Access** tab.

5. Select the **Show assigned permissions** option to view the access permissions assigned to the Active Directory accounts and groups.

6. To request the removal of a specific permission, click on the associated check mark (for example, click the check mark in the **AllowFullControl** column).

   The **Security modification** dialog appears. The reason is pre-populated, but can be edited if necessary. Click **Submit**.

   The request is immediately sent and not added to the shopping cart.

7. To request a different type of security modification (for example to add an additional permission), click the **Request modification** button.

   In the **Security modification** dialog, enter the type of modification to be made in the Reason text box and click **Submit**.

   The request is immediately sent and not added to the shopping cart.

To view the change resource security request, navigate to **Request | My Requests | Request History**.

Analyzing access by organizational structure

You can use the **Access Analysis** page on the **Governed Data** view to display a graphical representation showing who has access to a governed resource based on organizational structure.

To analyze access by organizational structure:

1. From the menu bar, select **Responsibilities | My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select the resource you want to analyze.

4. Select **Access Analysis** to view a graphical representation or details gather from analyzing access based on organizational structure.

   This view contains the following tabs:

   - **Access analysis on <resource type>**: For the selected resource, this page displays different graphics showing the access rights assigned to people based on organizational structure.

     | NOTE: Access analysis data is not available for cloud managed hosts.

   - **Access analysis on backing folder permissions**: For the backing folder associated with the resource, this page displays different graphics showing the access rights assigned to people based on organizational structure.

   - **Access Details**: This page displays a list of the people used in the access analysis of the selected resource.

   For more information, see Resource's Governed Data view on page 181.

5. The data is displayed in pie charts; however, clicking the **Grid view** link will pop up a dialog that displays the data in a grid format.

6. Clicking a segment in a pie chart or the **View People** button in the grid view displays a list of the people associated with the selected item.

Generating governed data reports

The **Reports** page for a governed resource displays the Data Governance Edition reports that can be generated for the selected resource. The following Data Governance Edition reports can be generated for a resource:

Table 54: Governed data reports

Report	Description
Resource Access	This report identifies which accounts have access to the resource. This can help you meet your compliance and audit goals by ensuring only authorized users can access the specific resources.
	The report includes subfolders and files of the identified resources if the security differs from the parent (for example, if inheritance is overridden or blocked).
	This report helps to identify data with several access points that should be monitored and potentially governed. Content that is available to "Everyone" or "All Sales" for example, can pose a high risk of having a sensitive file placed within it. These entitlements might arise either in error or through malicious intent.

Report	Description
Resource Activity	This report provides a list of activities recorded over a period of time to verify proper resource usage and make decisions on removing access for particular accounts.
	This report requires that resource activity collection be enabled on local managed hosts (Windows computers), SharePoint managed hosts, or remote agents used to scan supported NAS devices. Resource activity collection is NOT available for remotely managed Windows computers, Windows clusters, Generic or Cloud managed hosts.

Business owners who also have the **Data Governance | Administrators** application role, can generate these additional reports from the **Reports** page of the **Governed Data** view in the web portal:

Table 55: Governed data reports (Business owners with Data Governance | Administrators application role)

Report	Description
Data Owners vs. Perceived Owners	This report helps you track down if the probable business owners should be the designed business owners due to change of responsibilities. This report displays all the resource data owners who have had resource access. The perceived owners are displayed for the resource with percentage points based on their level of activity or security as well as the business owner.
Data Ownership Over Time	This report provides information to help you understand how ownership of resources change over time for better control over access to data.
Interesting Resources without an Owner	This report highlights data that has a high level of activity but does not have an owner. The report includes the perceived owner for this resource.
Perceived Owners for Data Under Governance	This report can be used to identify the probable business owners for the data that is marked for governance.
	Historical resource activity or security information is used to determine the perceived owner and provide guidance on who should be assigned as the business owner for a particular resource. For more information, see Managing business ownership for a resource on page 160.

To generate a Data Governance Edition report for a resource

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select the resource.

4. Click **Reports** to open the reports view.

5. Select the **Generate report** button to the right of the report to be generated.

   A dialog appears, allowing you to specify details and options for generating the report.

6. Enter the requested information and select **Send report**.

   The report is sent to your email account.

> TIP: You can also subscribe to the Data Governance Edition reports from **the My Settings | Report Subscriptions** page, which is accessed by selecting ⚙**Settings** in the upper right corner just below the web portal header. For more information on subscribing to reports, see the *One Identity Manager Web Portal User Guide*.

Viewing the risk analysis for an owned resource

As a business owner, you can use the web portal to review the risk analysis for an owned resource. The calculated risk index value assigned to the resources you own is displayed on the **All my resources** page of the **Governed Data** view. You can then drill down to review the properties and assignments used in the risk assessment for an individual resource.

To view the risk analysis for an owned resource

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. On the **Governed Data** view, open the **All my resources** tab to view a list of owned resources and their risk index assignment.

4. Select a resource and on that resource's **Governed Data** page, select **Risk** to review the properties and assignments that contributed to the calculated risk index for the selected resource.

5. Click the **View risk functions** button to view the attributes and assignments used in the risk assessment.

Analyzing governed data access

Roles are used to help manage assignments to employees. You can use the **Usage** page on the **Governed Data** view to see all role members that can be members of a governed resource.

To analyze governed data access

1. From the menu bar, select **Responsibilities** | **My Responsibilities**.

2. On the **My Responsibilities** view, select the **Governed Data** tile.

3. Open the **All my resources** tab and select the resource you want to analyze.

4. Select **Usage** to view the employees who have accessed or may access the selected resource.

5. Select one of the following options:

   - **Show employees who have access permissions to this resource**

     Select this option to show all employees who are entitled to access this resource.

   - **Show employees who have accessed this resource in the last 7 days**

     Select this option to show employees who have accessed the resource in the past seven days.

6. Select a role class from the **Role classes** drop-down menu.

   A hierarchy chart appears allowing you to select a sub-role. Select a sub-role by clicking on the name of the role in the chart.

7. An information icon (ⓘ) displays next to a role where at least one employee is assigned to this base object, is a member of the role or is a child role.

   Click the icon to display the **Assigned employees** dialog, which lists the employees who are members of the object that have access permissions to the selected resource.

   Click **Close** to close the **Assigned employees** dialog.

8. Click the **More Information** button to see the employees that are assigned to the root object.

   The **Legend** dialog appears, displaying the following information:

   - Employees assigned to this root object.

   - Employees assigned to this root object that are members of at least one child role.

   - Employees assigned to this root object that are members of this role.

   - Employees assigned to this root object that are members of this role and at least one child role.

   Click **Close** to close the **Legend** dialog.

Auditor responsibilities

If you have the Auditor application role assigned, you can perform the following auditing tasks:

- Navigate to **Responsibilities** | **Auditing** | **Governed data** to view governed data for a managed host. For more information, see Viewing governed data for a managed host on page 198.

- Navigate to **Responsibilities | Auditing | Active Directory** to view access permissions for an Active Directory resource. For more information, see Viewing the access permissions for an Active Directory resource on page 199.

- Navigate to **Responsibilities | Auditing | Employees** to view the group membership of a given employee and detailed access control information for governed data. For more information, see Viewing membership and access permissions for an employee on page 200.

Viewing governed data for a managed host

Use the **Governed data** tile on the **Auditing** view (**Responsibilities | Auditing**) to display a list of managed hosts or the governed data for a given managed host.

To view governed data for a managed host

1. From the menu bar, select **Responsibilities | Auditing**.

2. On the **Auditing** view, select the **Governed data** tile.

   The **Auditing- Managed Hosts** view appears listing the managed hosts in your environment, including the following details:

   - Display name
   - Host type
   - Count of governed resources
   - Count of points of interest

3. Click the **Show governed data** button for a managed host.

   The **Auditing-Governed** data view appears listing the governed resources for the selected managed host, including the following details:

   - Path
   - Governed data type
   - Risk index (calculated)
   - Comments

   NOTE: Click the **View Settings | Additional columns** button to view a list of additional details that can be added to the display. Select the additional columns to be added and click **Apply**. Use the **Reset view** option to remove any additional information you may have added.

4. Click the **View content** button for a governed resource to view additional governed data under the selected resource.

Viewing the access permissions for an Active Directory resource

Using the **Auditing** option on the **Responsibilities** menu you can view information about employees, business roles, system roles, One Identity Manager application roles, organizational structures, and other services. In addition, if the Data Governance Edition module is installed, you can view the access permissions for an Active Directory resource.

To view the access permissions for an Active Directory resource

1. From the menu bar, select **Responsibilities** | **Auditing**.

2. On the **Auditing** view, select the **Active Directory** tile.

    The **Auditing - Active Directory** view appears displaying a list of Active Directory resources.

3. To limit the list, click the **Assign** link next to **Select an employee**.

    a. The **Select an employee** dialog appears.

    b. Select the employee you want to view.

    c. The **Auditing - Active Directory** view re-appears, listing the Active Directory resources for which the person is responsible for.

4. Click the Active Directory resource you want to explore, and then select the **Show details** button.

    The **Status** page for the resource appears, which allows you to review the following information about the selected object:

    - Overview: A hyper view (graphical representation) of relations between the system entitlement and One Identity Manager.
    - Master data: The properties assigned to the system entitlement.
    - Memberships: The employees who have access to the system entitlement.
    - Child groups: The child groups for the system entitlement.
    - Attestation: The attestation status of the system entitlement.
    - Compliance: The compliance violations against the system entitlement.
    - Usage: The role classes of employees who are members of the selected entitlement.

5. Click the **Access** tab.

6. Click the arrow to the left of a group to expand the list and view parent groups.

    NOTE: If more parent groups are shown, expand the view until either a folder or file is shown. This means you can also view access permissions for parent groups.

    A check mark is displayed in the **Read** and **Write** columns to show the access permissions currently assigned to the file or folder.

7. Click the **Details** button next to a file or folder.

The Access Control List appears showing the assigned permissions. Click **Close** to close the Access Control List.

Viewing membership and access permissions for an employee

When Data Governance Edition is installed, the **Auditing** view for an employee includes an additional **Access** page that lists the groups and accounts to which the selected account is assigned. You can then expand a group or account to view detailed access control information.

When the selected account has access to governed resources, two tabbed pages appear:

- **Memberships**: Shows the groups and account to which the selected employee is assigned.

- **Resources**: Shows the governed resources the selected employee has access to.

NOTE: If the selected employee does not have access to any governed resources, the view contains the list of groups and accounts to which the selected employee is assigned.

For more information on the other auditing tasks and views available through the web portal, see the *One Identity Manager Web Portal User Guide*.

To view the membership and access control information for an employee

1. From the menu bar, select **Responsibilities | Auditing**.

2. On the **Auditing** view, select the **Employees** tile.

3. On the **Auditing - Employee Details** view, select an employee from the list.

4. Click **Access** to display the groups and accounts the selected account is assigned to.

5. Click the **Memberships** tab to view the membership information for the selected employee.

6. Click the arrow to the left of an account to expand the group or account to view detailed access control information.

   NOTE: If more parent groups are shown, expand the view until either a folder or file is shown. This means you can also view access permissions for parent groups.

   A check mark is displayed in the **Read** and **Write** columns to show the access permissions currently assigned to a file or folder.

7. Click the **Details** button next to a file or folder.

   The Access Control List appears showing the assigned permissions. Click **Close** to close the Access Control List.

Data Governance Edition reports

Reporting overview

One Identity Manager Data Governance Edition includes reports to help you identify, summarize, and analyze resource and account access and activity throughout your organization. The reports detailed in this section refer specifically to those that help you to secure the unstructured NTFS and SharePoint data within your enterprise and implement data ownership.

The following components function together to provide the reports and information to administrators and ultimately the business owners, compliance officers, and managers, through the web portal.

- Report Editor

  From here, you can create and edit reports. During report creation, you specify which parameters are visible and can be overwritten and which are pre-populated from the data source.

  NOTE: Data Governance Edition reports are pre-defined default reports delivered with One Identity Manager, and as such, they cannot be edited. However, if they do not suit your needs, you can create a report based on the default by copying it, and entering the required parameters in the **Edit report** dialog.

  For details on working with the Report Editor, see Reports in One Identity Manager in the *One Identity Manager Configuration Guide*.

- Manager

  From here, you prepare reports for subscription, customize the report parameters (specify the parameters that are available and can be overwritten by web portal users), setup email notifications, and publish reports to the IT Shop.

  NOTE: You can also view resource activity, resource access, account activity and account access reports within the Manager. For more information, see Viewing selected reports within the Manager on page 215.

  For details on making reports available within the web portal, see the *One Identity Manager Report Subscriptions Administration Guide*.

- Web Portal

  From here, employees can request access to and view subscribed Data Governance Edition reports that pertain to resources, accounts, and group membership.

  Web portal users can customize the report to suit their needs. For details on accessing and viewing reports within the IT Shop, see Report Subscriptions in the *One Identity Manager Web Portal User Guide*.

  IMPORTANT: In order to process Data Governance Edition report requests from the web portal, a One Identity Manager service (job server) must be running as an account that is able to access the Data Governance server (that is, either a Data Governance service account or an account mapped to an employee with the **Data Governance** | **Administrators** or **Data Governance** | **Access Managers** application role).

  The job servers that host these One Identity Manager services must be marked in the database with the **Data Governance connector** flag using the job server editor in the Designer application. (Specifically, in the Designer, select **Base Data | Installation | Job server | Server functions**.)

Figure 3: Reporting workflow
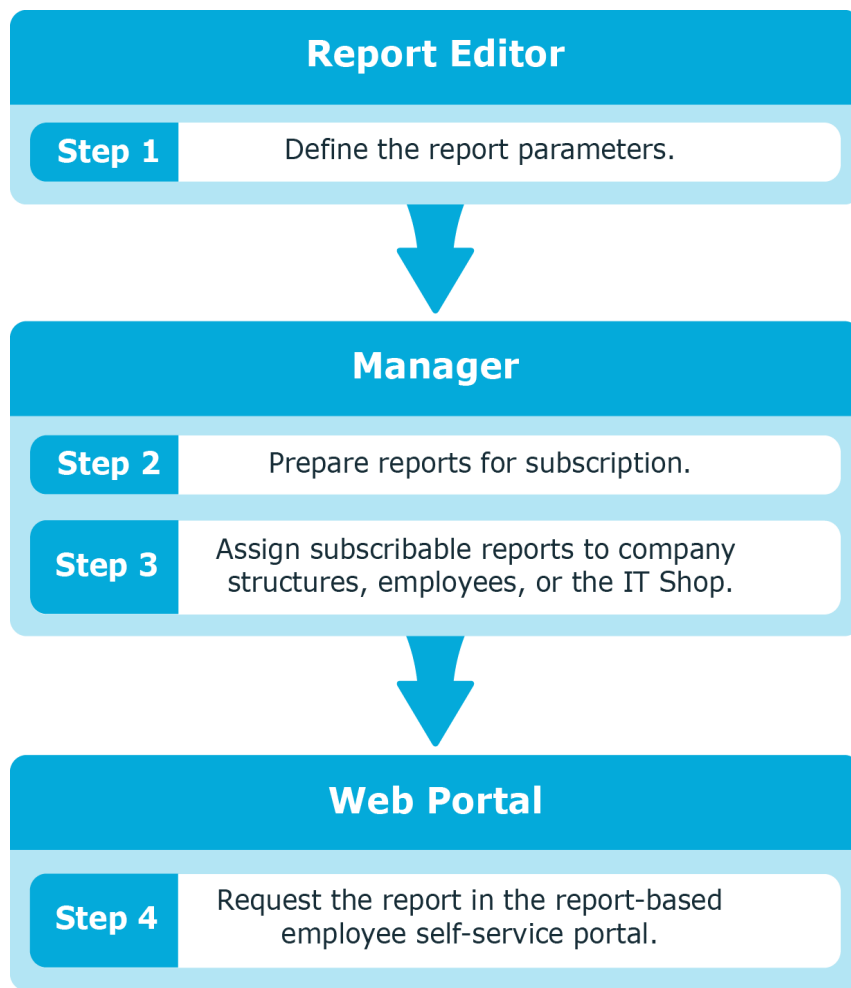
Data Governance Edition report descriptions

The following reports are provided to help you in your data governance endeavors:

Data ownership reports (requires resource activity collection)

- Data owner vs. perceived owner report
- Perceived owners for data under governance report
- Interesting resources without an owner report

Access reports

- Account access report
- Account access (employee) report
- Resource access report

Activity reports (requires resource activity collection)

- Account activity report
- Resource activity report

Group membership reports

- Group members report
- Group members comparison report
- Member of report
- Member of comparison report
- Empty groups report

Rights and identities report

- Local rights and service identities report

Data owner vs. perceived owner report

Through ongoing data governance activities, the assignment of ownership to unstructured data will, over time, improve the overall health of your network.

This report displays all the resources on Windows File Servers, SharePoint farms, supported NAS devices and Cloud managed hosts, their location (network path), and where the current data owners (those that have been assigned a business owner) differ from the perceived owner. Perceived owner is calculated on historical resource activity or security information for the selected resource.

This is a companion report to the "perceived owner calculation" feature in the Manager where you can compute if the current perceived owner is different than the designated business owner. For more information, see Calculating perceived owner on page 163. This report is useful for continuous compliance by identifying cases where the perceived owner should be designated the business owner due to changed responsibilities.

Compliance officers and administrators can run this report for the entire enterprise to ensure that the data is owned by the appropriate user — the user who understands the content and can attest to the list of authorized users. This should be consistently monitored to ensure that the proper user has control over the resources.

Perceived owners for data under governance report

Unstructured data can be substantial across an enterprise, so it is important to understand who is responsible for managing that data. This is paramount for data that has been identified as important or sensitive and placed under governance.

Historical resource activity or security information is used to determine the perceived owner and provide guidance on who should be assigned as the business owner for a particular resource. For more information, see Managing business ownership for a resource on page 160.

Compliance officers and administrators can run this report against the entire enterprise. The report helps to identify whether data ownership is applied properly. This is a useful report to run when you are first bringing resources under governance to understand the resource activity patterns and starting a data stewardship process.

Use the following parameter to define the contents of the report.

Table 56: Perceived owners for data under governance: Report parameters

Parameter	Description
Exclude Resources with Owner	Select this check box to exclude resources that already have an owner assigned from the report.

Account access report

Having a clear picture of who can access data within your organization is key in maintaining data governance. This report displays an account's resource access across all managed hosts within the enterprise and a detailed view of account group membership.

Managers can run this report for any account they manage; Compliance officers and administrators can run it for any account within the enterprise. This report helps to ensure that access has been properly assigned so that employees can perform their day to day duties. The report also identifies how accounts have attained that access and whether the level of access is appropriate.

NOTE: This report is not available for NFS managed hosts.

Use the following report parameters to define the content of the Account access report.

Table 57: Account access: Report parameters

Parameter	Description
Hosts	Specify the managed hosts to be included in the report: • All accessible hosts

Parameter	Description
	• Specific hosts When the **Specific hosts** option is selected, select the individual hosts to be included.
Excluded Accounts	(Optional) Select the users, groups, or built-in security principals to be excluded from the report. Use the **Add** and **Delete** buttons to populate this exclusion list.
Expand Groups	Specify whether you want to include group members in the report. That is, select the **Expand Groups** check box if you want to include access granted through group membership in the report.
Resource Types	Select the resource types to be included in the report. By default, all resource types are included. NOTE: Only resource types that apply to the selected trustee are displayed.
Excluded File Types	(Optional) Specify the file extensions for the types of files to be excluded from the report. Use the buttons on this page to add and remove file extensions from the exclusion list: • **Export**: Exports the current exclusion list to a QAM Extension List (*.qamel) file. Clicking this button displays the **Save As** dialog allowing you to specify a file name and location for saving the file. • **Import**: Imports the file extensions from a QAM Extension List (*.qamel) file. The QAM Extension List file can be a previously exported file or one that was manually created with the .qamel file extension. Clicking this button displays the **Select an import file** dialog allowing you to select the file to be imported. • **Default**: Adds the default list to the exclusion list. • **Remove**: Removes the selected file extensions from the exclusion list. You can remove individual extensions or a category, which will remove all of the extensions listed under that category. • **Add**: Adds the specified file extensions to the exclusion list. Clicking this button displays the **Add Excluded Extension** dialog allowing you to specify the category and extensions to be added to the exclusion list. When entering multiple extensions, separate them with a semi-colon (for example, exe;tmp;log;jpg)
Excluded Folder Names	(Optional) Specify the names of folders to be excluded from the report. Use the buttons on this page to add and remove folders from the exclusion list: • **Export**: Exports the current exclusion list to a QAM Folder List (*.qamtf) file. Clicking this button displays the **Save As** dialog allowing you to specify a file name and location for saving the file.

Parameter	Description

	• **Import**: Imports the folder names from a QAM Folder List (*.qamtf) file. The QAM Folder List file can be a previously exported file or one that was manually created with the .qamtf file extension. Clicking this button displays the **Select an import file** dialog allowing you to select the file to be imported.
	
	• **Default**: Adds the default list to the exclusion list, which includes:
	    • %SystemRoot%
	    • %ProgramFiles%
	    • %ProgramFiles(x86)%
	
	• **Remove**: Removes the selected folder names from the exclusion list.
	
	• **Add**: Adds the specified folder name to the exclusion list. Clicking this button displays the **Specify the folder to exclude** dialog allowing you to enter the folder name to be added to the exclusion list.

Data Under Governance Only	Specify whether to include only resources that are under governance in the report. That is, select the **Data Under Governance Only** check box to include only governed resources in the report.

Account access (employee) report

The Account access (employee) report details an employee's direct and indirect access (through group memberships) to file system or SharePoint resources on the managed hosts. This report returns account access information for all of that Employee's associated identities, eliminating the need to rerun the current Account Access report for each individual identity.

| NOTE: This report is not available for NFS managed hosts.

Use the following report parameters to define the content of the Account access (employee) report.

Table 58: Account access (employee): Report parameters

Parameter	Description
Managed hosts	Select the managed hosts to be included in the report.
Excluded accounts	Optionally select the users, groups or built-in security principals to be excluded from the report. Use the **Add** and **Delete** buttons to populate this exclusion list.
Expand	Specify whether you want to include group members in the report. That

Parameter	Description
Groups	is, select the **Expand Groups** check box if you want to include access granted through group membership in the report.
Resource types	Select the resource types to be included in the report. By default, no resource types are included. Resource types that can be included are: • Cloud\File • Cloud\Folder • NFS\File • NFS\Folder • NTFS\File • NTFS\Folder • Server Identities\Windows Service Identity • SharePoint\FarmAdminRight • SharePoint\ResourceItem • SharePoint\SiteCollectionAdminRight • SharePoint\WebAppPolicy • Windows Computer\Local User Rights • Windows Computer Operating System Administrative Rights • Windows Computer\Share
Excluded Extensions	Optionally specify the names of folders to be excluded from the report. Use the buttons to the right of this field to add and remove extensions from the exclusion list.
Excluded Folders	Optionally specify the names of folders to be excluded from the report. Use the buttons to the right of this field to add and remove folders from the exclusion list. NOTE: You can use the %<*Folder Name*>% format to specify Environment Variables to be excluded from the report. For example, %ProgramFiles%.
Data Under Governance	Specify whether to include only resources that are under governance in the report. That is, select the **Data Under Governance** check box to include only governed resources in the report.

Resource access report

This report identifies the accounts that have access to specific resources within your environment. This can help you meet your compliance and audit goals by ensuring only

authorized users can access the specific resources.

NOTE: The resource browser and resource access reports do not display the limited access users or "previewer" accounts for resources on Cloud managed hosts.

When you run the report, you can select specific resources and isolate specific types of permission, such as modify, full control, read, and execute. The report includes subfolders and files of the identified resources if the security differs from the parent (for example, if inheritance is overridden or blocked).

Business owners can run this report on resources they own; Compliance officers and administrators can run this report for all resources within the enterprise.

This report helps to identify data with several access points that should be monitored and potentially governed. Content that is available to "Everyone" or "All Sales" for example, can pose a high risk of having a sensitive file placed within it either in error or with malicious intent.

Use the following report parameters to define the content of the Resource access report.

Table 59: Resource access: Report parameters

Parameter	Description

Display Options	Specify whether you want to include child resources or access granted through group membership in the report.
	
	 • **Child Resources**: Select the **Access Deviations: Block Inheritance or Explicate Access** check box to include child resources whose access differs from the selected resource.
	
	    NOTE: In the web portal, this is the **Include Child Deviations** check box, which is selected by default.
	
	 • **Groups**: Select the **Expand Groups** check box to include all group members who have access to the resource.
	
	 • **Permissions Options**: Select the **Use Folder Permissions** check box to include folder permissions on EMC and NetApp shares.
	
	    NOTE: This parameter only applies to EMC and NetApp managed hosts.

Account activity report

Constant provisioning and de-provisioning activities can leave your organization open to security breaches and data leakage. Identifying the resource activity of accounts is essential to determining where access should be removed. This report shows you all the activity for a particular account (for example file reads, writes, and creates) against specific managed hosts.

NOTE: This report does not include activity from NFS host types.

NOTE: This report requires that resource activity collection be enabled on local managed hosts (Windows computers), SharePoint managed hosts, or remote agents used to scan supported NAS devices.

Resource activity collection (and therefore, this report) is NOT available for the following host types:

- Windows Cluster/Remote Windows Computer
- Generic Host Type
- EMC Isilon NFS Device
- SharePoint Online
- OneDrive for Business

For more information, see Resource activity page on page 108.

NOTE: This report displays resource activity using UTC, not your local time zone.

Managers can view the activities of any user under their management; Compliance officers and administrators can see activity across the enterprise.

This report helps to identify activities that are outside the scope of an account's roles so that you can take steps to secure the resources.

Resource activity report

Network resources can be accessed frequently by many users over time. Recording and reporting on this activity can help you determine patterns of usage (who uses what resources regularly) and helps to spot atypical behavior (for example, someone who is reading documents they should not have access to). This report provides a list of activities recorded over a period of time to verify proper resource usage and make decisions on removing access for particular accounts. This report can also suggest possible business owners for orphaned data based on activity.

NOTE: This report requires that resource activity collection be enabled on local managed hosts (Windows computers), SharePoint managed hosts, or remote agents used to scan supported NAS devices.

Resource activity collection (and therefore, this report) is NOT available for the following host types:

- Windows Cluster/Remote Windows Computer
- Generic Host Type
- EMC Isilon NFS Device
- SharePoint Online
- OneDrive for Business

For more information, see Resource activity page on page 108.

NOTE: This report displays resource activity using UTC, not your local time zone.

Business owners can run this report for the resources they own; Compliance officers and administrators can run it to view activity across the entire enterprise.

The report helps to answer questions such as: "What changes have been made to sensitive data by the help desk in the last two weeks and is this appropriate?"

Use the following parameters to define the contents of the Resource activity report.

Table 60: Resource activity: Report parameters

Parameter	Description

Time Range	Specify the time range to report on.
	
	 • Last: Select this option to include activity collected over the specified time interval. By default, the report includes activity collected over the last seven days. However, you can use the controls to specify a different interval for the report:
	
	   • Hours
	   • Days
	   • Weeks
	   • Months
	   • Quarters
	   • Years
	
	 NOTE: The **Last** option is not available when generating the report through the web portal.
	
	 • Date range: Select this option to limit the report to a specific date range.
	
	   • Start time: Select the start date and time.
	   • End time: Select the end date and time.
	
	 • Add dates and times: Select this option to include all activity available in the Resource Activity database.
	
	 All dates and times are UTC.

Excluded Accounts	(Optional) Select the users, groups, or built-in security principals to be excluded from the report. Use the **Add** and **Delete** buttons to populate this exclusion list. NOTE: This page is not available for resources on NFS managed hosts.
Activity Exclusions	(Optional) Specify the activities to be excluded from the report: • Read • Write • Create • Delete

Parameter	Description
	• Rename
	• Security Change

Interesting resources without an owner report

This report highlights resources that have a high level of activity but do not have an owner. The report includes the perceived owner for resources.

NOTE: This report requires that resource activity collection be enabled on local managed hosts (Windows computers), SharePoint managed hosts, or remote agents used to scan supported NAS devices.

Resource activity collection (and therefore, this report) is NOT available for the following host types:

- Windows Cluster/Remote Windows Computer
- Generic Host Type
- EMC Isilon NFS Device
- SharePoint Online
- OneDrive for Business

For more information, see Resource activity page on page 108.

Compliance officers and administrators can run this report for the entire enterprise to identify resources that should be placed under governance and have an owner assigned. For details on assigning business owners, see Managing business ownership for a resource on page 160.

Use the following parameters to define the contents of the report.

Table 61: Interesting resources without an owner: Report parameters

Parameter	Description
Start Date	Select this check box and enter the starting date for the report.
End Date	Select this check box and enter the ending date for the report.
Excluded accounts	No objects are selected by default. Click the **Change** link to specify the accounts to be excluded from the report.
Number of Interesting Resources	Indicates the maximum number of resources to be included in the report. If set to 0 (default), then all 'interesting' resources are included.

Data ownership over time report

This report helps you to identify how data ownership has changed over time for better control over data access.

The report only displays single ownership until One Identity Manager is configured to record data changes. Once these parameters have been enabled, the report displays a complete list of when ownership has changed.

For more information on the configuration parameters that must be enabled, see Logging Data Changes in the *One Identity Manager Configuration Guide*.

Use the following parameters to define the interval for the report.

Table 62: Data ownership over time: Report parameters

Parameters	Description
Start Date	Select this check box and enter the starting date for the report.
End Date	Select this check box and enter the ending date for the report.

Group members report

Active Directory security groups can become large over time due to unrestricted provisioning and de-provisioning. This report displays a group's complete direct and indirect membership list.

Group owners can run this report for groups they own; Compliance officers and administrators can run the report against any group in the enterprise.

The report helps identify accounts that should be removed from a group to ensure least privilege within your network.

Group members comparison report

Administrators are often responsible for managing groups that have similar membership requirements. A quick glance may not easily distinguish one group from another. The Group Members Comparison report highlights where group membership differs between two or more groups.

Group owners can run this report for groups they own; Compliance officers and administrators can run the report against any group in the enterprise.

You can also use Account Comparison (in the Manager) to compare the group members access and simulate the effects of a change to group membership before actually applying any changes as a result of the report. For more information, see Account access modeling on page 142.

Member of report

It can be difficult to get an accurate representation of nested group membership. Users can be a member of a group through many levels of nesting, including local groups. This report shows a clear picture of an account's full membership in indexed security groups.

Managers can run this report for any account they manage; Compliance officers and administrators can run the report against any account in the enterprise.

Member of comparison report

Two users who have been provisioned for similar roles may find that they have different levels of access due to differences in group membership. The Member of Comparison report helps identify these differences so they can be corrected.

Managers can run this report for any account they manage; Compliance officers and administrators can run the report against any account in the enterprise.

You can also use Account Comparison (in the Manager) to compare the group members access and simulate the effects of a change to group membership before applying any changes as a result of the report. For more information, see Account access modeling on page 142.

Empty groups report

This report displays any groups that do not have members. This helps determine which groups are candidates for removal.

Group owners can run this report for groups they own and administrators can run it for all groups within the enterprise.

Local rights and service identities report

This report helps you understand who has local rights on a managed host and which identities are being used to run Windows services. It provides the following information:

- Service Identities: Lists the identities used to run services on the selected managed host.

- Local User Rights: Lists the particular rights that a trustee has on a given managed host. An example would be the "Allow Logon Locally" right.

- Admin Rights: Lists trustees with Operating System Administrative rights on a given managed host.

NOTE: If you see a message that indicates the forest or domain could not be contacted, this could be because the trusted domain has not been synchronized with One Identity Manager.

Viewing selected reports within the Manager

Generating Resource Access and Resource Activity reports

You can easily view resource access and resource activity reports directly in the Manager from the **Resource browser**, the **Governed data** view, or the **Manage access** view.

To run a resource access report

1. Right-click the required resource, and select **Resource access report**.

2. In the **Resource access** dialog, you can include varying levels of detail in the report by selecting the display options.

    - Select the **Child resources | Access Deviations: Block Inheritance or Explicit Access** check box to include child resources whose access differs from the selected resource.

    - Select the **Groups | Expand Groups** check box to include all group members who have access to the resource.

3. Click **Finish** to generate the report.

To run a resource activity report

1. Right-click the required resource, and select **Resource activity report.**

2. On the **Time Range** page of the **Resource activity** dialog, specify the time that you are interested in, and click **Next**.

    You can report on the last so many hours, days, weeks, months, quarters, or years, a specific time period, or all dates and times.

    NOTE: All dates and times are displayed in UTC, not necessarily your local time.

3. (Optional) On the **Excluded Accounts** page, select to exclude specific accounts from the report. Click **Add** to display the **Select User or Group** dialog, where you can locate and select the accounts to be excluded. After selecting the accounts to be excluded, click **Next**.

    NOTE: This page is not available for NFS managed hosts.

4. (Optional) On the **Activity Exclusions** page, select the type of activities that you are not interested in and want to exclude from the report:

    - Read
    - Write

- Create
- Delete
- Rename
- Security Change

5. Click **Finish** to generate the report.

Generating Account Access and Account Activity reports

You can easily view account access and account activity reports directly in the Manager by selecting an account in the security editor of the **Resource browser** or an account in the group membership pane of the **Manage access** view.

To run an account access report

1. Right-click the required account, and select **Account access report** from the Tasks view.

2. On the **Hosts** page of the **Account Access** dialog, select the managed hosts that contain the resources whose access you are interested in:

   - All accessible hosts: This check box is selected by default and indicates all hosts are to be included in the report.

   - Specific hosts: Select this check box to specify one or more hosts to be included in the report. Select the check box to the left of a host to include it in the report.

   Click **Next**.

3. (Optional) On the **Excluded Accounts** page, select any accounts that are to be excluded from the report. Click **Add** to display the **Select User or Group** dialog, where you can locate and select the accounts to be excluded. After selecting the accounts to be excluded, click **Next**.

4. On the **Expand Groups** page, you can specify the level of report details by selecting to display group members. If necessary, select the **Expand Groups** check box and click **Next**.

5. On the **Resource Types** page, select the resource types whose access you are interested in (all resource types are selected by default).

6. (Optional) On the **Excluded File Types** page, specify file extensions of the files to be excluded from the report. By default, no file types are excluded.

   Use the buttons on this page to populate the file extensions exclusion list:

   - **Export**: Exports the current exclusion list to a QAM Extension List (*.qamel) file.

   - **Import**: Imports the file extensions from a previously exported or manually created QAM Extension List (*.qamel) file.

   - **Default**: Adds the default list to the exclusion list.

- **Remove**: Removes the selected file extensions from the exclusion list.
- **Add**: Adds the specified file extensions to the exclusion list.

7. (Optional) On the **Excluded Folder Name** page, specify folder names to be excluded from the report. By default, no folders are excluded.

   Use the buttons on this page to populate the folders exclusion list:

   - **Export**: Exports the current exclusion list to a QAM Folder List (*.qamtf) file.
   - **Import**: Imports the folders from a previously exported or manually created QAM Extension List (*.qamtf) file.
   - **Default**: Adds the default list to the exclusion list.
   - **Remove**: Removes the selected folders from the exclusion list.
   - **Add**: Adds the specified folders to the exclusion list.

8. On the **Data Under Governance Only** page, select the **Data Under Governance Only** check box if you only want to include resources that are under governance.

9. Click **Finish** to generate the report.

To run an account activity (employee) report

1. In the Navigation view, select **Employees | Employees**.

2. In the **Employees** result list, select an employee, right-click and select **Tasks | Account Access**.

3. In the **Define parameters** dialog, enter the following information:

   - **Managed hosts**: Click the drop-down button to select the managed hosts you are interested in.
   - **Excluded accounts**: (Optional) Click the drop-down button to select the accounts to be excluded from the report.
   - **Expand Groups**: (Optional) Select this check box to display group members in the report.
   - **Resource types**: Click the drop-down button to select the resource types whose access you are interested in. If you do not specify any resource types, the report will return with 'There is no data to display'.

4. Click **OK** to generate the report.

To run an account activity report

1. Right-click the required account, and select **Account activity report**.

2. On the **Time Range** page of the **Account Activity** dialog, specify the time that you are interested in and click **Next**.

   You can report on the last so many hours/days/weeks/months/quarters/years, a specific time period, or all dates and times.

   | NOTE: All dates and times are displayed in UTC, not necessarily your local time.

3. On the **Hosts** page, select the managed hosts that contain the resources you are interested in and click **Next**.

4. On the **Activity Exclusions** page, select the type of activities that you are not interested in and want to exclude from the report:

- Read
- Write
- Create
- Delete
- Rename
- Security Change

5. Click **Finish** to generate the report.

Troubleshooting

The following troubleshooting tips are provided to assist you with the day-to-day administration of Data Governance Edition:

- Data Governance Edition logs
- No activity data
- No activity data available for SharePoint 2010 managed host
- Not receiving scheduled reports
- Groups missing from the Group Memberships tree view
- Resource activity is not displaying in the web portal for a business owner
- Governed resources are missing from the All my resources view in the web portal

Additional troubleshooting tips may be found in the following guides:

- *One Identity Manager Data Governance Deployment Guide*: Troubleshooting tips related to deploying and configuring Data Governance Edition components.

- *One Identity Manager Data Governance IT Shop Resource Access Requests Guide*: Troubleshooting tips related to self-service resource access requests and share creation requests.

Data Governance Edition logs

The first place to look when you run into an issue with Data Governance Edition is the logs. The Data Governance Edition logs available are:

Data Governance configuration wizard log

Log name: Data Governance Configuration Wizard.exe.dlog

The Data Governance configuration wizard log is stored as a Trace log document (dlog) in the users AppData directory. For example:
C:\Users\MyName.MyDomain\AppData\Local\One Identity\One Identity Manager\Data Governance Configuration Wizard\.

Used for capturing errors encountered while using the Data Governance Configuration wizard to deploy the Data Governance service and create the Resource Activity database.

Data Governance server log

Log name: DataGovernanceEdition. Service.exe.dlog

NOTE: The Data Governance server maintains rolling log files based on settings found in the DataGovernanceEdition.Service.exe.config file, therefore there may be multiple server log files in the Data Governance service installation directory. The first log file is the active log and is being maintained by the server. When this log file reaches a specified size, it is renamed (a number is appended to the name) and a new file is started with the original name.

NOTE: By default, the logging level is set to INFO. To change the logging level to get detailed logging:

1. Locate the DataGovernanceEdition.Service.exe.config file in the Data Governance service installation directory.

2. Open the configuration file and edit the following setting:

   ```
   <rules>

           <logger name="*" minlevel="INFO" writeTo="logfile">
   ```

3. Change INFO to DEBUG to get detailed logging.

4. Save the file.

The server log is stored as a Trace log document (.dlog) in the Data Governance service installation directory. For example: %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\.

Used for capturing the following information:

- Data Governance service communication
- Group resolution and group expansion
- Agent lease expiration information
- Points Of Interest (POI) collection information
- Resource activity updates

ONE IDENTITY
by Quest

- Security changes made on a resource from the Manager
- Incoming web service calls related to Data Governance Edition from the One Identity Manager web site

NOTE: In previous versions of Data Governance Edition, individual server log files were generated. Starting with Data Governance Edition version 7.0.2, the logging information from all of these server logs are now available in this single server log file.

Server logs can be viewed as described below:

- In the Manager, use the **Get All Logs** task to export the server log to a specified location. From that location, double-click the log file to view the log in the Log Viewer. For more information, see Getting server logs on page 223.
- From the Data Governance service machine, double-click the log file or right-click and select **Open** to view the log in the Log Viewer.

Applications and Services event logs

Severity error level events and audit events are written to the Applications and Services event logs on the Data Governance server under the "Data Governance" node.

- Severity error level errors have a "Source" of "Data Governance Edition".
- Audit events contain information on operations run by the server (such as security changes) and have a "Source" of "Data Governance Audit".

Data Governance agent deployment logs

Log name: *<Agent name>*_Agent.log

The agent deployment logs are stored as text files in the Agent Deployment Logs folder in the Data Governance service installation directory. For example: %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\Agent Deployment Logs\.

Used for capturing the agent deployment process for each individual agent. There is a separate agent deployment log for each agent installed in your Data Governance Edition deployment.

Agent deployment logs can be viewed as described below:

- In the Manager, use the **Get All Logs** task to export the agent deployment logs to a specified location. From that location, double-click the log file to view the log. For more information, see Getting server logs on page 223.
- From the Data Governance service machine, double-click the log file or right-click and select **Open** to view the log.

Data Governance agent logs

Log name: DataGovernance.Agent.exe.dlog

NOTE: By default, the logging level is set to INFO. To change the logging level to get detailed logging:

1. Locate the agent's dlog.config file on the host computer in the agent installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services*<Agent instance directory>*\dlog.config).

2. Open the configuration file and edit the following setting:

   ```
   <rules>

           <logger name="*" minlevel="INFO" writeTo="logfile">
   ```

3. Change INFO to DEBUG to get detailed logging.

4. Save the file.

   No agent restart is required.

An agent log is stored as a Trace log document (.dlog) in a subfolder on the host computer in the agent installation folder. For example:

%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services\DGE_*<DeploymentName>_<HostDnsName>*\.

Used for logging communications, synchronization processes and data transfers between the Data Governance server and the agent.

Agent logs can be viewed as described below:

- From the Manager, use the **Export agent log** task to export the selected agent log to a specified location. From that location, double-click the log file to view the log in the Log Viewer. For more information, see Exporting agent log on page 224.

- From the agent machine, double-click the log file or right-click and select **Open** to view the log in the Log Viewer.

Web client logs

The Web client log files are located in the following directory: C:\inetpub\wwwroot\IdentityManager\App_Data\Logs.

This directory contains a series of log files all named with a time stamp.

Errors encountered with the web client IT Shop are recorded to the web client logs.

The best way to get the proper log is to replicate the issue and take the file with the greatest timestamp.

Job server logs

The default URL for a Job Server log is: http://JobServerHost:1880/Log

Often when you have errors with Active Directory synchronization or report execution you can find clues in the One Identity Manager Job Server logs. In addition, errors encountered with the process chains used to process resource access requests in the IT Shop are recorded in the Job Server logs.

With a default configuration, you can browse these logs by launching a web browser and navigating to a specific URL on the computer hosting the Job Server.

Manager client log

Log name: QAM.Client.Log.dlog

If experiencing issues with Data Governance Edition inside the Manager client, enable the Data Governance Edition client side logging to determine if the issue is related to the user interface rather than the Data Governance server.

NOTE: By default, the logging level is set to INFO. To change the logging level to get detailed logging:

1. Locate the Data Governance Edition client log configuration file (%ProgramFiles%\One Identity\One Identity Manager\QAM.Client.Log.config).

2. Open the configuration file and edit the following setting:

   ```
   <rules>

           <logger name="*" minlevel="INFO" writeTo="logfile">
   ```

3. Change INFO to DEBUG to get detailed logging.

4. Save the file.

The Manager client log files are located in the user profile directory:

   C:\Users\<*Your User Name*>\AppData\Local\One Identity\One Identity Manager\Manager

NOTE: To enable the latest LogView logging for the Manager client, modify the Manager configuration file (%ProgramFiles%\One Identity\One Identity Manager\Manager.exe.config) as follows:

Comment out the following:

```
<include file="${basedir}/globallog.config" ignoreErrors="true"/>
```

Add the following:

```
<include file="${basedir}/QAM.Client.Log.config" ignoreErrors="true"/>
```

Getting server logs

From the **Managed hosts** view in the Manager you can export the server logs to a location of your choosing. The log files are exported through a background operation and will exist once the background operation has completed. The export operation can be viewed in the **Background operations** view.

NOTE: Server logs retrieved using the **Get All Logs** task consist of the DataGovernanceEdition.Service.exe.dlog file and associated agent deployment logs.

To get server logs

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. Select **Get All Logs** from the Tasks view or right-click menu.

3. In the **Browse for folder** dialog, select the location where the exported logs are to be stored.

   A compressed zip file is created in the specified location. Clicking this zip file displays the Data Governance service log and an Agent Deployment Logs folder, which contains a log file for each agent deployed.

4. Double-click the Data Governance service .dlog file to display the log viewer to view the service's log.

5. Double-click an agent deployment log file to open Notepad to view the agent's deployment log.

Exporting agent log

From the **Agents** view in the Manager, you can export the agent log for the selected agents to a location of your choosing. The log files are exported through a background operation and will exist once the background operation has completed. The export operation can be viewed in the Background operations view.

To export an agent log

1. In the Navigation view, select **Data Governance** | **Agents**.

2. In the **Agents** view (right pane), select the required agents.

3. Select **Export agent log** from the Tasks view or right-click menu.

4. In the **Browse for folder** dialog, select the location where the exported logs are to be stored.

   A compressed zip file is created in the location specified. Clicking this zip file displays a trace log document for the selected agents.

5. Double-click the .dlog file to display the log viewer to view an agent's log entries.

No activity data

When you run a Resource Activity, Account Activity, or Perceived Owner report, you may not immediately see an action in the report that you know you have performed.

Probable cause

- There is lag time between when an action occurs, such as a file read or write, and when the data is sent from the agent to the server. This delay is dependent upon the following:

  - The aggregation setting on the **Resource Activity** page of the **Managed Host Settings** dialog

- The update schedule. By default, resource activity is synchronized into the One Identity Manager database, once a day, after the first initial synchronization. The initial synchronization happens a few minutes after resource activity collection is enabled. This update schedule is controlled by a Data Governance server configuration setting (PerceivedOwnershipCalcUpdateRefreshIntervalMinutes). See the *One Identity Manager Data Governance Edition Technical Insight Guide* for more information on this configuration file setting.
    - Various internal processes.
- It is possible that you did not have resource activity collection enabled for that managed path during the time span covered in the report.
- If you have enabled resource activity collection, it is possible you have excluded some accounts, files or folders where the activity occurred.
- If Quest Change Auditor is installed and you are collecting resource activity directly from Change Auditor, Change Auditor may not be capturing the events you are expecting.

Resolution

- Verify the managed host type. Resource activity collection is only available for local managed Windows servers, SharePoint farms, and supported NetApp and EMC managed hosts.
- Use the **Edit Host Settings** task from the **Managed hosts** view to verify that the required paths are being managed:
    - Open the **Managed Paths** page of the **Managed Host Settings** dialog. Are the required managed paths listed?
- Use the **Edit Host Settings** task from the **Managed hosts** view to verify that resource activity collection is enabled:
    - Open the **Resource Activity** page of the **Managed Host Settings** dialog.
        - Is the **Collect and aggregate events** option selected?
        - Are the required events selected?
- Verify the accounts, files or folders that are being tracked
    - Click the **Resource Activity Exclusions** button on the **Resource Activity** page of the **Managed Host Settings** dialog.
    - Check each tab to see what objects are being excluded.
- Collaborate with the Change Auditor administrator to determine what data Change Auditor is collecting.

No activity data available for SharePoint 2010 managed host

Probable Cause

For SharePoint 2010 managed hosts, the DataGovernance.SharePointShim.exe process is required and may not be running on the SharePoint server.

NOTE: For multi-agent SharePoint 2010 managed hosts, you will see multiple Shim instances; one for each agent service.

Resolution

Check to ensure that the DataGovernance.SharePointShim.exe process is running on the SharePoint 2010 farm server. If it is not running, start the process or restart the agent.

To start the Shim process

Since multiple Shim instances are displayed for multi-agent SharePoint managed hosts, you must provide the PID of the corresponding Data Governance SharePoint agent as an argument when starting up the Shim process for an agent service.

1. In **Task Manager | Services** tab, locate the PID assigned to the agent service that does not have activity available.

2. At the command prompt, enter the following PowerShell command to start the Shim instance:

   ```
   C:\Program Files\One Identity\One Identity Manager Data Governance
   Edition\Agent Services\DataGovernance.SharePointShim.exe <PID>
   ```

NOTE: This only applies to SharePoint 2010 because in later releases of SharePoint, this is not a separate process.

Not receiving scheduled reports

Probable cause

The One Identity Manager service (job server) is not configured correctly. If you are having issues with scheduled report execution and are not receiving your reports through email, the first place to check is the Job Server log.

Resolution

Scheduled reports are run by the job server with the SMTP Host server mask. To allow this job server to query the Data Governance server, it must be running as an Active Directory account with an associated One Identity Manager Employee with either the **Data**

Governance | Administrators or **Data Governance | Access Managers** application role.

To change the identity the job server runs as, open the Services console on the computer hosting the job server and change the Log On identity. For example, the DGEAdministrator Active Directory account needs to be associated with an Employee record that was granted the **Data Governance | Administrators** role or be a Data Governance service account itself. This new identity allows the job server to authenticate against the Data Governance server and perform the necessary queries required for report execution.

Groups missing from the Group Memberships tree view

To examine group membership in your enterprise, Data Governance Edition requires credentials that allow it to read group memberships in the domains that make up your enterprise structure. These credentials are provided when syncing the domain for Active Directory. For SharePoint group membership, it uses the provided database connection string and reads group information from the SharePoint database. If Data Governance Edition is having trouble resolving group memberships, you will see a link in the lower-left pane (after having selected Manage Access from the client). Clicking this link displays a list of issues that details any problems encountered during group expansion.

Resolution

- Ensure that you have provided credentials with the required access.

Resource activity is not displaying in the web portal for a business owner

Probable cause

Activity for owned data may not display in the web portal if:

- Resource activity collection has not been enabled on the selected managed host.
- Resource activity collection is not supported on the selected managed host (such as, remote managed Windows computers, Windows clusters, Generic or Cloud managed hosts).
- Resource activity collection is enabled, but the data is not included within a specified managed paths.

Resolution

To ensure resource activity is being collected:

1. From the **Managed hosts** view, select the required managed host.
2. Select **Edit host settings** from the Tasks view or right-click menu.
3. In the **Managed Host Settings** dialog, open the **Resource Activity** page.
4. Ensure **Collect and aggregate events** is selected.
5. Also, ensure the appropriate events are selected.
6. Click the **Resource Activity Exclusion** button and review each tab to see what objects are being excluded.

To check what managed paths are selected for activity collection:

1. From the **Managed hosts** view, select the required managed host.
2. Select **Edit host settings** from the Tasks view or right-click menu.
3. In the **Managed Host Settings** dialog, open the **Managed Paths** page.
4. Activity is only being collected for the paths listed on this page.

NOTE: For all managed host types, when placing a resource under governance, the resource must be a managed path or a folder or share under a managed path.

- For remote managed hosts and SharePoint managed hosts, if you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. If the managed host has more than one agent assigned, you are prompted to select the agent to which the managed path is added.

- For local managed hosts, if you are scanning managed paths (that is, there are paths in the managed paths list), and you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. However, if you are scanning the entire server (that is, the managed paths list is empty) and you place a resource under governance, no changes are made to the managed paths list and you continue to scan the entire server.

For more information about these pages on the **Managed Host Settings** dialog, see Managed paths page on page 104 and Resource activity page on page 108.

Governed resources are missing from the All my resources view in the web portal

Probable cause

Business ownership for governed resources was set programmatically or through the Object Browser.

Resolution

If business ownership for governed resources is set programmatically or through the Object Browser, you must also set the following parameter for these governed resources:

QAMDuG.IsPointOfInterest = true.

NOTE: Business ownership is indicated by setting values for either QAMDuG.UID_PersonResponsible or QAMDuG.UID_AERoleOwner.

EMC, NetApp Filer, and SharePoint configuration details

Additional configuration for an EMC storage device

Additional configuration for NetApp filers

Configure SharePoint to track resource activity

Additional configuration for an EMC storage device

EMC storage devices are added to the Data Governance Edition deployment as managed hosts with remote agents. Due to the EMC architecture, you must complete the following procedures when you add an EMC storage device as a managed host.

- Configuring CEE framework
- Creating the cepp.conf file (Celerra or VNX devices)
- Enabling system configuration auditing (Isilon devices)

NOTE: EMC supports only one auditing pool at a time, meaning only one vendor or vendor's product can subscribe to CEPA auditing events for a given computer. Therefore, if Quest Change Auditor for EMC is configured to collect activity from an EMC storage device via the Quest Shared EMC Connector, and you would like activity collection/aggregation in Data Governance Edition, you must configure Data Governance Edition to collect activity directly from Change Auditor. For more information, see the *Post installation configuration* chapter in the *One Identity Manager Data Governance Edition Deployment Guide*.

The activity collected can then be used to generate resource activity reports and calculate the perceived owner. However, in this scenario, it is recommended that you clear the **Collect activity for real-time security updates** option for all EMC managed hosts. The agents managing these host types should be configured to scan on a schedule and not run once. The performance gain in using Change Auditor's event collection will be lost

if the Data Governance agent is also collecting activity from these storage devices for security updates.

Configuring CEE framework

Data Governance Edition 7.0.2 (and higher) requires the EMC Common Event Enabler (CEE) 7.1 (or higher) framework to collect resource activity from an EMC storage device. The Data Governance agent will register with EMC CEE as a VCAPS endpoint. EMC CEE must be installed on the same server as the Data Governance agent. If you are collecting resource activity from the EMC storage device, you can only specify one agent to manage the EMC host.

To configure CEE framework

- Install the EMC CEE framework on one or more Windows servers.

NOTE: EMC CEE must be installed on the same server as the Data Governance agent.

Next steps:

- For Celerra and VNX storage devices, create and configure the cepp.conf file. For more information, see Creating the cepp.conf file (Celerra or VNX devices) on page 231.

- For Isilon storage devices, enable system configuration auditing. For more information, see Enabling system configuration auditing (Isilon devices) on page 233.

Creating the cepp.conf file (Celerra or VNX devices)

You must create a configuration file (cepp.conf file) before using the CEPA auditing feature to monitor file system activity on EMC Celerra or VNX storage devices. The cepp.conf file contains the information needed to connect Data Movers to the Windows computers where the CEE software is installed. It also defines the type of file system events that Data Governance Edition can collect from the EMC device.

To create and configure cepp conf file

1. Using an SSH client (such as Putty.exe), connect to Control Station using its IP and port (the default is 22).

2. Login using administrative credentials. The default user name and password on a Celerra system are nasadmin/nasadmin.

3. Copy or create the cepp.conf file.

- To copy the current configuration file from the Data Mover, run the following command: `server_file` *movername* `-get.cepp.conf cepp.conf`

  Where: *movername* is the name of your Data Mover. The default name is server_2.

- To create the configuration file, open the VI text editor (or other preferred text editor) by running the following command: `vi cepp.conf`

4. Using the text editor, edit the cepp.conf file and ensure the following configuration parameters are in the file:

   `pool name=`*poolname* `servers=`*server1*`|`*server2* `postevents=`*event1*`|`*event2*`|...`

   Where: *poolname* is the name assigned to the set of Windows servers where the Event Enabler software from EMC is installed.

   Where: *server1|server2* is the fully-qualified domain name of the Windows computers hosting the Event Enabler (CEE) software from EMC. If you have more than one server, separate them with a vertical bar (|).

   Where: *event1|event2|…* are the EMC events to be collected during security scans and activity collection. When specifying multiple events, separate them with a vertical bar (|).

   NOTE: Do not register for pre-events or post-err-events in the cepp.conf. These events are ignored by the Data Governance agent and add undue load on the EMC device.

   The following table shows events (postevents=) that can be registered in the cepp.conf and their mapping to Data Governance events that can be collected during security scanning and activity tracking.

EMC cepp.conf event	Data Governance Edition event
CreateFile|CreateDir	Create
DeleteFile|DeleteDir	Delete
RenameDir	Rename
SetAclFile|SetAclDir	SecurityChange
CloseModified	Write
CloseUnmodified	Read

   NOTE: If you configure your EMC managed host to collect real-time security changes and apply them to scanned data, you must include the following events:

   …postevents=CreateFile|CreateDir|DeleteFile|DeleteDir|RenameDir|SetAclFile|SetAclDir

   For performance reasons, you may want to filter out the events that are not required, such as CloseUnmodified which are the "Read" events.

5. Save the file. (Press **Escape** then type :wq)

6. Run the following commands in the SSH client to publish the file to the Data Mover and restart the CEPA facility:

   server_cepp *movername* -service -stop

   server_file *movername* -put cepp.conf cepp.conf

   server_cepp *movername* -service -start

   Where: *movername* is the name of your Data Mover. The default name is server_2.

7. Verify the CEPA status by running the following command:

   server_cepp *movername* -service -status

8. Verify the pool configuration by running the following command:

   server_cepp *movername* -pool -info

Enabling system configuration auditing (Isilon devices)

EMC Isilon devices do not use the cepp.conf file; however, you must enable configuration change auditing and protocol access auditing in order for Data Governance Edition to perform security scans and collect resource activity on the EMC storage device.

NOTE: On the Data Governance server and all agent servers, you must have a Trusted Root Certificate Authority certificate to validate the Isilon server's HTTP certificate.

To enable auditing (OneFS web interface)

1. Connect to the OneFS web interface.

2. Select **Cluster Management**.

3. Select **Auditing**.

4. In the **Settings** pane, select the following check boxes:

   - **Enable Configuration Change Auditing**
   - **Enable Protocol Access Auditing**

5. In the **Audited Zones** pane, add the zones to be audited:

   - Click the **Add Zones** button to add a zone.

6. In the **Event Forwarding** pane, enter the following information:

   - **CEE Server URIs**: Enter the uniform resource identifier (URI) for the Windows server hosting the Common Event Enabler (CEE) software.

     Use the following format: http://*<FullyQualifiedDomainName>*:*<Port>*/cee.

     For example: http://server.test.abc.com:12228/cee

     The default CEE HTTP port is 12228.

Click the **Add another input field** to add additional CEE server URIs.

- **Storage Cluster Name**: Enter the resolved name of the EMC Isilon cluster.

    Use the following format: *<ClusterName>.<DomainName>*.com

    For example: Cluster1.test.abc.com

7. Click **Save Changes**.

Additional configuration for NetApp filers

Data Governance Edition uses the NetApp Data ONTAP file screening policy (FPolicy) to track activities on the filer. This policy allows third-party file screening software to interact with the NetApp filer.

Understanding the following aspects of the deployment process are key to ensuring a successful deployment of NetApp managed hosts:

- Permissions required to access NetApp filer
- Data Governance agent deployment
- FPolicy deployment
- Managed host configuration options
- Performance considerations
- Compatibility with Change Auditor for NetApp

Permissions required to access NetApp filer

The service account for the remote agent responsible for scanning the NetApp filer must meet the following minimum permissions:

- Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.)
- Must be a member of the local Administrators group on the NetApp filer.
- Must have permissions to access the folders being scanned.

Data Governance agent deployment

NetApp filers are added to a Data Governance Edition deployment as managed hosts with remote agents. When selecting an agent for scanning a NetApp filer, take the following into consideration:

- The remote agent must be hosted on a machine in the same domain as the NetApp filer device.

    NOTE: If you host a remote agent in an external domain to monitor a filer, the agent will NOT record the resource activity data.

- There should be a good network connection between the NetApp filer and the monitoring agent servers.

- The machine hosting the agent for NetApp can host agents for other servers, but those servers should be close to the agent host.

- If the NetApp is split up into multiple domains, you must deploy one or more agents for each domain.

FPolicy deployment

FPolicy is required for Data Governance Edition to capture real-time security updates and to collect resource activity. In order to use FPolicy on NetApp 7-Mode managed hosts, CIFS file system protocol must be enabled.

When adding a NetApp 7-Mode managed host, you can use one of the following for FPolicy deployment:

- automatic FPolicy deployment
- use a pre-created FPolicy

However, for NetApp Cluster Mode managed hosts, FPolicy deployment is always automatic.

Using automatic FPolicy deployment for NetApp 7-Mode

When you add a NetApp managed host, an FPolicy is created if either of the following managed host settings are enabled:

- **Collect activity for real-time security updates** on the Security Scanning page
- **Collect and aggregate events** on the Resource Activity page

When you deploy an agent, an empty FPolicy (with no monitored operations) is created by the Data Governance server (performed as the service account for the domain). When the agent starts, it registers with the FPolicy as an FPolicy Server. At the point of registration, the agent will register the operations it will monitor.

NOTE: If another agent is added to the managed host to index a separate root on the NetApp device, a new FPolicy will be created (named after the new agent ID).

The FPolicy:

- is created using the credentials of the domain service account.
- is named after the agent ID (that is, DGE_ *<DeploymentName>_<FQDN of managed host>*).
- is configured to use the version 2 interface.

- includes cifs_set_attr information, which allows Data Governance Edition to receive notification of security changes.

- sets the cifs_setattr option to on (defaults to off in FPolicy).

- is asynchronous.

NOTE: To view all the existing FPolicies on a NetApp device, establish a Telnet or SSH connection to the filer device, log in and type the following at the OnTap command line: "fpolicy".

NOTE: When you remove an agent, the FPolicy is deleted.

Using a pre-created FPolicy on a NetApp 7-Mode filer

Data Governance Edition can be configured to connect to a pre-created FPolicy. The following steps are required to configure Data Governance Edition to use a manually created FPolicy instead of automatic deployment:

- Enable CIFS FPolicy on NetApp filer

- Create FPolicy on the filer

- Configure the Data Governance server and agent

To enable CIFS FPolicy on a NetApp filer

- Run options FPolicy.enable on

To create FPolicy on the filer

- fpolicy create *<PolicyName>* Screen

- fpolicy enable *<PolicyName>*

To configure the Data Governance server and agent

1. Configure the Data Governance server to prevent the creation of FPolicy on the required NetApp filer:

    a. Create the following registry key: "HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Broadway\Server\ManualFPolicyCreation".

    b. Add a string value with the fully qualified domain name of the NetApp filer.

2. In the Manager, deploy a NetApp managed host.

    NOTE: Ensure that the registry key has been created on the server before deploying the agent.

3. Configure the NetApp agent to use the manually pre-created FPolicy.

    a. Stop the agent service.

    b. Locate the following configuration setting in the %Program Files%\One Identity\One Identity Manager Data Governance Edition\Agent Services\DataGovernance.Agent.exe.config file.

    <"Agent">

     <"Services">

```
<"ChangeMonitoring">

    <Setting name="OverrideFPolicyName">
```

    c. Add a string value with the FPolicy name you want the specified agent to register with.

    d. Save the configuration file.

    e. Restart the agent.

FPolicy deployment for NetApp Cluster Mode

FPolicy deployment for NetApp Cluster Mode is always automatic and is done by the agent at run time because of the use of dynamic ports. The FPolicy will be deleted when the agent stops. You cannot specify a pre-created FPolicy.

Managed host configuration options

During the configuration of the managed host:

- Select the required shares (managed paths) to scan.
- (Optional) Select to **Collect activity for real-time security updates**.
- (Optional) Select to **Collect and aggregate resource activity**.

When you add an agent, the managed host properties impact whether FPolicy is deployed, and what properties are set within the FPolicy itself:

- If both **Collect activity for real-time security updates** and **Collect and aggregate activity** are disabled on the managed host, FPolicy will not be created when the agent is deployed.

- If **Collect activity for real-time security updates** or **Collect and aggregate activity** is enabled, FPolicy will be created; however, there will be no registered settings until the agent starts up and receives the updated settings from the Data Governance servers.

- The agent must start its security scan before it registers with FPolicy. This means that managed paths must be set and the agent must hit its configured scanning schedule. (To force this scan, select the **Immediately scan on agent restart or when managed paths change** option and restart the agent.)

Monitored events

The following events are tracked on files and folders, as well as the identities associated with those events, when real-time security updates and/or resource activity collection is enabled:

- File create
- File rename
- File delete

- File write

- File open

- Setattr (Security changes including DACL, and Owner changes)

- Directory rename

- Directory delete

- Directory create

Performance considerations

Enabling FPolicy on NetApp filers may impact system performance. Data Governance Edition uses 'async' mode and does not inspect any file data to try and minimize the performance impact. However, every event does require a round trip network request between the NetApp filer and the Data Governance agent.

Are rescans of all directory structures required to detect change?

To have Data Governance Edition watch for security changes, real-time security updates must be enabled. That is, select the **Collect activity for real-time security updates** option at the bottom of the **Security Scanning** page on the **Managed Hosts Settings** dialog for the target managed host. This will cause the FPolicy to be deployed and the security index to be updated when changes to the structure and security of the file system on the target managed host occur.

Compatibility with Change Auditor for NetApp

If you are using Quest Change Auditor for NetApp to monitor a filer that is also being scanned by Data Governance Edition, you have two options available.

Option 1: Collect activity directly from the Change Auditor database

When Change Auditor is installed, you can configure Data Governance Edition to collect resource activity directly from Change Auditor. When enabled, Change Auditor collects the selected activity events every 15 minutes on all managed hosts. The events received from Change Auditor are harvested by the Data Governance server, aggregated and placed directly into the Data Governance Resource Activity database.

When using Change Auditor to collect resource activity, NetApp managed hosts will not place an FPolicy for Data Governance Edition on the NetApp filer.

In addition, when using Change Auditor to collect resource activity, it is recommended to clear the **Collect activity for real-time security updates** option for NetApp managed hosts. The agents managing these host types should be configured to scan on a schedule

and not run once. The performance gain in using Change Auditor's event collection will be lost if the Data Governance agent is also collecting activity from these storage devices for security updates.

For more information on configuring Data Governance Edition to collect resource activity directly from Change Auditor, see the *One Identity Manager Data Governance Edition Deployment Guide.*

Option 2: Collect activity using Data Governance Edition

You can use Data Governance Edition to collect resource activity; however, for NetApp 7-Mode managed hosts, you must disable real-time security monitoring. You can disable security monitoring from the Resource Activity tab of the **Managed Host Settings** dialog.

To disable security monitoring

NOTE: This approach has the effect of setting the NetApp FPolicy option cifs_setattr to off.

You can verify this by running the following command on the NetApp filer: >fpolicy options *<Agent instance>*

Where *<Agent instance>* is in the following format: DGE_*<DeploymentName>_<FQDN of managed host>*

You will still see setattr as a monitored operation in FPolicy.

1. In the Navigation view, select **Data Governance** | **Managed hosts**.

2. In the **Managed hosts** view, select the required managed host.

3. Select **Edit host settings** in the Tasks view or right-click menu.

4. Open the **Resource Activity** page of the **Managed Hosts Setting** dialog and click the check box to clear the **Security change** event.

5. After making the required change, click **OK** to save your selections and close the dialog.

NOTE: This will need to be completed for every NetApp agent. If it is necessary to disable "Security change" due to compatibility settings with Change Auditor for NetApp, ensure the Resource Activity setting is modified prior to the start of the agent scan.

Configure SharePoint to track resource activity

To gather and report on resource activity in SharePoint, ensure that SharePoint native auditing is properly configured for any resources of interest. You can also optionally install the SharePoint Auditing Monitor farm solution to obtain activity for events not available in the native SharePoint auditing system.

Configure auditing on SharePoint farms

You can enable auditing at different levels in the SharePoint farm. It is recommended that you enable auditing at the site collection level to ensure that all events are collected. The methods available for configuring auditing vary depending on the SharePoint edition installed. Sometimes, you can use Central Administration; in all cases you can use Windows PowerShell. It is recommended that you enable all SharePoint native events to ensure maximum coverage for data governance activities, but you may select a smaller set to improve performance if necessary.

Consult your Microsoft documentation for complete information on configuring auditing.

Install the QAM.SharePoint.Auditing.Monitor farm solution

If you install the SharePoint farm solution, you can supplement the events captured by native auditing. Install "QAM.SharePoint.Auditing.Monitor.wsp" from the agent installation folder (by default %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services.) Consult your Microsoft documentation for information on installing a farm solution.

NOTE: You must enable SharePoint native auditing. The farm solution is not a replacement for native auditing, it is an enhancement.

This farm solution captures some events that are unavailable through native SharePoint auditing, specifically:

- Adding a folder
- Adding a library
- Renaming a list or library
- Creating a site

Map SharePoint events to Data Governance events

When you track resource activity using Data Governance Edition, the results appear in views, reports, and dashboards. To simplify things, SharePoint events are grouped for

easier reporting. The following table outlines the events you see in your reports, and the corresponding SharePoint events.

Table 63: Mapping Data Governance events to native SharePoint events

Data Governance events	Native SharePoint events
Create	Undelete
	Item copied
	Item added
Delete	Item deleted
Rename	Item restored from Recycle Bin
Read	Checkout
	View
Security Change	Audit mask change
	Inheritance breakage
	Inheritance restore
	Permission level granted
	Permission level revoked
Write	Item checked in
	Item moved
	Item renamed
	Item updated
	Version deletion
	Version restored
	Item updated
	Attachment added

Appendix B

PowerShell commands

This appendixprovides a list of the Windows PowerShell commands available to deploy and configure Data Governance Edition components and administer Data Governance Edition to manage the unstructured data in your organization.

- Adding the PowerShell snap-ins
- Finding component IDs
- Data Governance Edition deployment
- Service account management
- Managed domain deployment
- Agent deployment
- Managed host deployment
- Account access management
- Resource access management
- Governed data management
- Classification management

For full parameter details and examples, see the command help or the *One Identity Manager Data Governance Edition Technical Insight Guide*. For a list and full parameter details and examples of the PowerShell commands available for creating and maintaining managed resources (such as, file shares created through the IT Shop self-service request functionality), see the *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide*.

Adding the PowerShell snap-ins

Data Governance Edition comes with a Windows PowerShell snap-in for you to use to manage your environment.

If you installed Windows PowerShell on your computer after you installed the Data Governance server, you must register the cmdlets before you can start using them in Windows PowerShell.

To import the Data Governance Edition PowerShell module

1. Open a Windows PowerShell window and type the following at the Windows PowerShell command prompt:

   `Import-Module "<path>"`

   Where <path> is the file path for the QAM.Client.PowerShell.dll assembly. By default, the <path> for the Data Governance server machine is "C:\Program Files\One Identity\One Identity Manager\QAM.Client.PowerShell.dll".

2. To verify that the module was added, type the following at the Windows PowerShell command prompt:

   `Get-Module -All`

   The registered PowerShell modules are listed.

NOTE: Run the `Set-QServiceConnection` command before you can use any of the Data Governance Edition commands.

Adding the module automatically to new sessions

If you do not want to manually add the Data Governance Edition PowerShell module each time you start a new Windows PowerShell session, you can modify the Windows PowerShell profile file so that it is added automatically for you.

To add the Data Governance Edition PowerShell module automatically when you start a new Windows PowerShell session

- Add the following line to the Windows PowerShell profile file (profile.ps1) file:

  `Import-Module "<path>"`

  The location of the Windows PowerShell profile file is as follows: WINDOWS\system32\windowspowershell\v1.0

NOTE: If you get the error message "…profile.ps1 cannot be loaded because the execution of scripts is disabled" the next time you start a new Windows PowerShell session, type the following at the Windows PowerShell command prompt:

`Set-ExecutionPolicy RemoteSigned`

Then, type the following at the Windows PowerShell command prompt to confirm that the execution policy has been changed:

`Get-ExecutionPolicy RemoteSigned`

Finding component IDs

Many of the Windows PowerShell commands you can use to manipulate your deployment require that you know the component's ID.

To determine the managed host, container parent, container, resource node, or agent ID

- Run the `Get-QManagedHosts` command.

To determine the service account or managed domain ID

- Run the `Get-QManagedDomains` command.

To determine the deployment name

- Run the `Get-QDeploymentInfo` command.

Data Governance Edition deployment

The following commands in the OneIdentity.DataGovernance snap-in can be used to deploy and configure the Data Governance Edition. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 64: Data Governance Edition deployment commands

Use this command	If you want to
Get-QDeploymentInfo	View deployment information for your Data Governance server including the deployment name.
Get-QEncryptionOptions	Retrieve the current encryption options used by One Identity Manager and show whether Data Governance Edition has been configured to use encryption.
Get-QServerAllLogs	Export all server logs to the designated folder.
Get-ServerVersion	View the version of the currently running Data Governance server.
Initialize-QDataGovernanceActivity	Initialize a database to store data generated when a managed host has resource activity tracking enabled. NOTE: This information is required for several reports, including the Resource Activity report. This is separate from the One Identity Manager database that stores configuration and security information.
Initialize-QDataGovernanceServer	Establish the database connection between One Identity Manager and Data Governance Edition. The Data Governance server must be initialized before you can use Data Governance Edition to manage your resources.
Register-QServiceConnectionPoint	Register service connection points in an Active Directory domain.

Use this command	If you want to
	NOTE: This can be helpful when the service account registered for a domain does not have sufficient permissions to create a service connection point (SCP).
Remove-QServiceConnectionPoint	Remove the DataGovernance.Server Service Connection Point (SCP) from an Active Directory domain.
	NOTE: This cmdlet can be helpful when you want to remove all Data Governance Edition SCPs from a single Data Governance Edition deployment or all deployments. To recreate an SCP which you inadvertently removed, restart your Data Governance service.
Set-QDeploymentInfo	Change the deployment parameters for the Data Governance server including the deployment name.
	NOTE: Changing this value can prevent the Data Governance service from communicating with existing agents. It is not recommended to change the deployment name of an existing server.
Set-QEncryptionOptions	Encrypt the Data Governance service account.
	NOTE: Only use this command if you have enabled encryption for the One Identity Manager database.
Set-QServiceConnection	Set the server name and port information used by the Data Governance Edition commands to connect to the Data Governance server.
	NOTE: You must run this command before you can use any of the Data Governance Edition commands.

Service account management

Data Governance Edition consolidates security information across many domains and forests by accessing these network entities using stored credentials (service accounts). These service accounts are Active Directory users granted the appropriate permissions in their respective domains and registered with Data Governance Edition.

The following commands are available to you to manage service accounts. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 65: Service account management commands

Use this command	If you want to
Add-QServiceAccount	Register an account as a service account for Data

Use this command	If you want to
	Governance Edition. When you add this service account, it is automatically granted the required Log On as a Service local user right on the Data Governance server.
Get-QLogonServiceAccount	Determine if the account can be used as a service account.
Get-QServiceAccounts	View a list of service accounts that have been created for the Data Governance server. NOTE: You can optionally specify a service account id if you are only interested in a particular service account.
Remove-QServiceAccount	Remove a service account from the deployment. NOTE: Remove any associated managed domains BEFORE removing a service account.
Set-QServiceAccountUpdated	Have the Data Governance server update a service account.

Managed domain deployment

Before you can gather information on the data in your enterprise, you must specify the domain that contains the computers and data that you want to manage. Then assign the service account to access the resources within them.

The following commands are available to you to deploy managed domains. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 66: Managed domain deployment commands

Use this command	If you want to
Add-QManagedDomain	Add a new domain to the Data Governance Edition deployment.
Get-QManagedDomains	View the list of managed domains in a deployment. NOTE: You can optionally specify a managed domain ID if you are only interested in a particular domain.
Remove-QManagedDomain	Remove a managed domain from your deployment.

Agent deployment

The following commands are available to you to manage your agent deployment. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 67: Agent deployment commands

Use this command	If you want to
Get-QAgentEvents	View saved events for the specified agent from the One Identity Manager database. You can use this command to output the stored agent messages to the console or a text file to quickly identify issues.
Get-QAgentMetrics	View an agent's activity and performance.
Set-QAgentConfiguration	Set the managed paths to be scanned. NOTE: When you set the managed paths using the cmdlet, existing managed paths are overwritten. NOTE: This cmdlet does not support setting managed paths for Cloud managed hosts.
Set-QAgentStateUpdated	Notify the Data Governance server that an agent has been updated and the server should process it.
Upgrade-QAgents	Upgrade the agents in your deployment. NOTE: You can identify the agents to upgrade through their agent ID or on a managed host basis.

Managed host deployment

A managed host is any network object that can host resources and can be assigned an agent to monitor security and resource activity. Currently supported hosts include Windows computers, Windows clusters, NetApp storage devices, EMC storage devices, DFS, and SharePoint farms.

You can also add generic managed hosts (Server Message Block (SMB) shares running on any Active Directory joined computer) to remotely scan their resources.

The following commands are available to you to deploy managed hosts. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 68: Managed host deployment commands

Use this command	If you want to
Add-QDfsManagedHost	Register a domain-based distributed file system root. This enables you to view and manage the access on resources that are physically distributed throughout your network.
Add-QManagedHostByAccountName	Add a managed host to your deployment and configure its settings. NOTE: This cmdlet does not support adding Cloud managed hosts.
Clear-QResourceActivity	Clear the resource activity for a given managed host. This enables you to remove activity data from the database on demand when it is no longer required. For scheduled activity cleanup, use the activity compression/deletion settings in the Data Governance server configuration file instead. NOTE: Once you clear the activity, it cannot be recovered.
Get-QHostsforTrustee	View a selected user or group's access on all managed hosts in your environment.
Get-QManagedHosts	View a list of all the managed hosts in your deployment. NOTE: If you are interested in only one managed host, you can specify the host's name or the ID (GUID format) of the managed host. You can also specify all the managed hosts in a particular container.
Remove-QManagedHost	Remove a managed host from your deployment.
Set-QManagedHostProperties	Change the properties of a managed host. NOTE: You must know the managed host ID
Set-QManagedHostUpdated	Inform the Data Governance server that the managed host state should be updated.
Trigger-QDfsSync	By default the Data Governance server synchronizes the DFS structure into the One Identity Manager database every 24 hours. Use this cmdlet to force a DFS synchronization of a DFS managed host, making the DFS path immediately available within the Resource browser.

Use this command	If you want to
	NOTE: You must specify the ID (GUID format) of the managed host to be synchronized. To synchronize all of the DFS managed hosts in your deployment, set the ManagedHostID to All.

Account access management

As people join, depart, and move through your organization, you need to change their data access. With Data Governance Edition, you can validate that users and groups have been granted access to all the resources they need, ensure that they do not have access to excess resources, and manage their access when problems arise.

The following commands are available to you to manage account access. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 69: Account access management commands

Use this command	If you want to
Get-QAccountAccess	View where users and groups have access on a managed host. NOTE: This PowerShell cmdlet does not support Cloud managed hosts.
Get-QAccountAccessOnHosts	View the resource access for a given account (Domain\SAMAccountName) across all available hosts. NOTE: This PowerShell cmdlet does not support Cloud managed hosts.
Get-QAccountActivity	View the activity associated with a user on a managed host. NOTE: This PowerShell cmdlet does not support Cloud managed hosts.
Get-QAccountAliases	View the group membership for a specified account. For example, if one of these groups (aliases) has access to a resource, the original account also has this access.
Get-QAccountsForHost	View all account access for a specific managed host.
Get-QADAccount	View the Active Directory objects from the One Identity Manager and QAM (Data Governance Edition) tables: ADSAccount, ADSGroup, ADSOtherSID, QAMLocalUser and QAMLocalGroup.
Get-QGroupMembers	View all the members of a group, including members of child

Use this command	If you want to
	groups. Because user and group access may be the result of several layers of nested groups, this helps you to assess how a specific account has gained access to a resource.
Get-QIndexedTrustees	View all of the entries from the QAMTrustee table who are also listed within the QAMSecurityIndex table, denoting an indexed trustee.

Resource access management

A key challenge in improving data governance is keeping track of permissions within your environment. To ensure that data is secured in a manner that meets your business needs, you must be able to easily identify who has been given access and manage that access appropriately.

The following commands are available to you to manage resource access. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 70: Resource access management commands

Use this command	If you want to
Export-QResourceAccess	Export the security information on a selected resource.
Get-QChildResources	View the resources contained in a specific root on a managed host. You can use this to enumerate the contents of remote folders and shares.
	In particular, it would be similar to the standard Windows PowerShell Get-ChildItems cmdlet but it functions using the Data Governance server as a proxy, so the client machine does not necessarily need direct access to the target machine.
	NOTE: This PowerShell cmdlet does not support Cloud managed hosts.
Get-QFileSystemSearchResults	Search an NTFS folder or share for files. Using this command, you can search multiple data roots at once.
Get-QHostResourceActivities	Retrieve a list of the operations, including the resource ID assigned to each operation, performed against a managed host during a given time frame.
	NOTE: This PowerShell cmdlet does not support Cloud managed hosts.
Get-QPerceivedOwners	Calculate the perceived owners for a resource. This

ONE IDENTITY
by Quest

Use this command	If you want to
	information can help to determine the true business owners and custodian for data.
	NOTE: The perceived owner for data is calculated from the resource activity history or security information collected by Data Governance Edition. Activity is collected based on the aggregation time span settings and recorded in the Data Governance Resource Activity database.
Get-QResourceAccess	Retrieve the security information of selected resources from a specific managed host, and child objects whose security differs from the parent.
Get-QResourceActivity	Retrieve the activity associated with a resource.
	NOTE: Resource activity collection (and therefore this cmdlet) is not supported for the following host types: • Windows Cluster/Remote Windows Computer • Generic Host Type • EMC Isilon NFS Device • SharePoint Online • OneDrive for Business
Get-QResourceSecurity	View the security on a given resource in the SSDL format.
Set-QResourceSecurity	Set security on a given resource.
	NOTE: The existing security descriptor is completely replaced.

Governed data management

Governing unstructured data allows you to manage data access, preserve data integrity, and provide content owners with the tools and workflows to manage their own data.

The following commands are available to you to manage governed data. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 71: Governed data management commands

Use this command	If you want to
Get-QDataUnderGovernance	View the data within your organization that has been placed under governance. Data is

Use this command	If you want to
	considered "governed" when it has been explicitly placed under governance or published to the IT Shop.
Get-QPerceivedOwnerPoI	View the name of the perceived owner for the specified governed resource. You can use the calculated perceived owners to identify potential business owners for data within your environment.
Get-QSelfServiceClientConfiguration	View the options that are available for self-service requests within the IT Shop.
Get-QSelfServiceMethodsToSatisfyRequest	View the group membership that is required to satisfy an access request. When employees request access to a resource, an approval workflow is put into action. Before the request for resource access can be granted, the business owner must select a group to which that employee could be added to fulfill their request. NOTE: This PowerShell cmdlet does not support NFS or Cloud resources (since these types of resources cannot be published to the IT Shop).
Remove-QDataUnderGovernance	Remove data from governance. NOTE: Removing a resource from governance, also removes it from the IT Shop.
Set-QBusinessOwner	Set the business owner on a governed resource to establish a custodian for data. The business owner should be an employee who understands the nature of the data and the list of authorized users. Ownership can be established for an individual employee or for all employees in an application role.
Set-QDataUnderGovernance	Place a resource under governance. Once data is "governed", the Data Governance server periodically queries the agent responsible for scanning that data and retrieves detailed security information concerning it and any child data. The data is then placed in the central database to be used by policies and attestations.

Use this command	If you want to
	You can also use this command to set the business owner on governed resources to establish a custodian for data. The business owner should be an employee who understands the nature of the data and the list of authorized users. Ownership can be established for an individual employee or for all employees in an application role.
Set-QSelfServiceClientConfiguration	Set the options that are available for self-service requests within the IT Shop.
Trigger-QDataUnderGovernanceCollection	Trigger data collection for governed resources for a given managed host.
Upgrade-QDataUnderGovernanceRecords	Upgrade the format of existing governed data in the database after an upgrade from version 6.1.1 or earlier. NOTE: This is a requirement for upgrading to version 6.1.2 or 6.1.3.

Classification management

Classification is included in Data Governance Edition, however you should first define the classification levels in Data Governance Edition to match those defined by your company. Once defined, you can use these classification levels to classify governed resources.

The following commands are available to manage the classification levels used in your Data Governance Edition deployment and to assign a classification level to a governed resource. For full parameter details and examples, see the command help, using the **Get-Help** command or the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Table 72: Group template management commands

Use this command	If you want to
Add-QClassificationLevel	Define a new classification level for use in your Data Governance Edition deployment.
Get-QClassificationLevelConfiguration	Retrieve details about the classification levels configured in your Data Governance Edition deployment.
Get-QDataUnderGovernanceByClassificationLevel	Retrieve a list of governed resources assigned a specific classification level.

Use this command	If you want to
Remove-QClassificationLevel	Remove a classification level from your Data Governance Edition deployment.
Set-QClassificationLevel	Update an existing classification level in your Data Governance Edition deployment.
Set-QClassificationLevelOnDug	Assign a classification level to a governed resource.

Governed data attestation policies

One Identity Manager ships with a predefined set of attestation policies for governed data. These predefined policies are available when the Data Governance Edition module is installed and can be found in the **Attestation policies** | **Predefined** folder in the **Attestation** navigation view in the Manager.

Once the schedule is enabled, attestation policies are all enabled by default. You can, however, disable an attestation policy using the **Change master data** task from the **Attestation policy** overview in the Manager.

The following attestation policies are available by default for governed data.

Table 73: Governed data attestation policies

Attestation policy	Predefined approval policy	Description
Data Governance: Accounts with direct access attestation	Attestation of account entitlements by employee manager.	Notify the employee marked as "responsible" for an account (that is, as a manager or as the person responsible for a particular privileged account), to attest to the entitlements of these "managed" accounts.
Data Governance: Groups with direct access attestation	Attestation of group entitlements by group owner. NOTE: If you have Cloud managed hosts in your Data Governance Edition deployment, change this setting to one of the following: • Attestation by target	Group product owner attests single group entitlements granting direct access.

Attestation policy	Predefined approval policy	Description
	system manager • Attestation of group entitlements by selected approvers	
Data Governance: Resource ownership attestation	Attestation by resource owner.	Resource owner attests ownership of governed resources, thereby approving their ownership.
Data Governance: Resource security attestation	Attestation by resource owner.	Managed resource owner attests to the security configuration of governed resources, focusing on highest entitlements only.
Data Governance: Resource security deviation attestation	Attestation by resource owner.	Resource owner attests governed resources with deviations in access security.

Tips for using governed data attestations:

- Designer: The **Base Data** | **General** | **Schedules** | **Attestation check** is enabled by default and runs daily at 16:00 PM. You can click the **Start** button on the Attestation check properties pane to initiate an immediate attestation check.

For more information on the One Identity Manager attestation feature, including how to define attestations, execute attestations and introduce automatic or manual correction measures, see the *One Identity Manager Attestation Administration Guide*.

Governed data company policies

One Identity Manager ships with a predefined set of company policies for governed data which can be enabled. These predefined policies are available when the Data Governance Edition module is installed and can be found in the **Policies** | **Working copies of policies** | **Predefined** folder in the **Company Policies** navigation view in the Manager.

The predefined governed data policies include:

Table 74: Governed data policies

Policy	Description
Access not granted on governed data for the predefined group "Everyone"	A policy violation occurs when the built-in Active Directory group "Everyone" has any access assigned. NOTE: This company policy is not available for Cloud accounts.
Full access not granted on governed data for the predefined group "Everyone"	A policy violation occurs when the built-in Active Directory group "Everyone" has any "Full Control" access assigned. NOTE: This company policy is not available for Cloud accounts.
Governed data must be assigned to a Classification level	A policy violation occurs when governed data is found that does not have a classification level assigned.
No governed data with access assigned to accounts other than AD security groups	A policy violation occurs when governed data is found with access assigned to accounts other than Active Directory security groups.
No governed data with conflicting NTFS permissions for Allow/Deny	A policy violation occurs when governed data is found with conflicting Allow/Deny access assigned.
No governed data with high risk index (> 0.75) accessible by accounts of external employees	A policy violation occurs when an external employee has access assigned to governed data with a high risk index.

Tips for using governed data policies:

- Manager: Working copies of company policies are disabled by default. You can, however, enable these policies using the **Enable working copy** task from the **Change master data** view of a policy.

- Manager: After enabling a working copy, you can use the following tasks to test a working copy of a policy:

  - **Show condition**: Displays a list of governed data that is in violation of the selected policy.

  - **Recalculate policy**: Evaluates the selected policy and logs any policy violations that occurred.

- Web portal: As a business owner of the resource, after recalculating a policy, any policy violations appear (**Responsibilities** | **My Responsibilities** | **Governed Data** | **Policy violations**).

- Designer: The **Base Data** | **General** | **Schedules** | **Policy check** is enabled by default and runs monthly at 11:00 AM. You can click the **Start** button on the Policy check properties pane to initiate an immediate policy check.

For details on managing policies, see Company Policies in the *One Identity Manager Company Policies Administration Guide*.

Governed data risk index functions

One Identity Manager ships with a predefined set of risk index functions used to calculate the risk index for governed data. These predefined risk index functions are available when the Data Governance Edition module is installed and can be found in the **Risk index functions** | **Governed data (QAMDuG)** | **Properties** folder in the **Risk Index Functions** navigation view in the Manager.

The predefined governed data risk index functions include:

Table 75: Governed data (QAMDuG) risk index functions

Risk index function name	Description	Default weighting / Change value
Attestation of data under governance	Reduces the risk of a governed resource when an attestation policy is enabled.	0.02
Defined owner for data	Reduces the risk of a governed resource when a business owner has been assigned.	0.01
Full access for "Everyone"	Increases the risk of a governed resource when "Everyone" is granted full access to the resource.	0.2
Full access for accounts	Increases the risk of a governed resource when there are accounts other than "Everyone" that is granted full access to the resource.	0.1
Last access > 30 days	Reduces the risk of a governed resource when the last access date is greater than 30 days.	0.04
Last access > 60 days	Reduces the risk of a governed resource when the last access date is greater than 60 days.	0.06
Last access > 90 days	Reduces the risk of a governed resource when the last access date is greater than 90 days.	0.08
Last access > 180 days	Reduces the risk of a governed resource when the last access date is greater than 180 days.	0.1

Risk index function name	Description	Default weighting / Change value
No classi-fication level assigned	Increases the risk of a governed resource when no classification level has been assigned.	0.1
Policy violation	Increases the risk of a governed resource when a company policy violation occurs.	0.2
Published to IT Shop	Increase the risk of a governed resource when the resource is published to IT Shop.	0.1
Read only access	Increases the risk of a governed resource when read-only access is granted.	0.05
Write access	Increases the risk of a governed resource when read and write access is granted.	0.1

Tips for using governed data risk index functions:

- Designer: The **Base Data** | **General** | **Schedules** | **Calculate risk indexes of governed data** is disabled by default. Before risk calculations can be performed on governed data, this schedule must be enabled. You can click the **Start** button on the Calculate risk indexes of governed data properties pane to initiate an immediate risk index calculation.

- Manager: The Data Governance Edition risk index functions are enabled by default. You can, however, disable a risk index function using the **Change master data** task on the Function overview.

- Web portal: As a business owner, you can see the risk index assigned to owned resources (**Responsibilities** | **My Responsibilities** | **Governed Data** | **All my resources**).

- Web portal: As a business owner, you can see what functions contributed to the calculated risk index (**Responsibilities** | **My Responsibilities** | **Governed Data** | **All my resources** | *<selected resource>* | **Risk**).

For more information on One Identity Manager's risk assessment feature, see the *One Identity Manager Risk Assessment Administration Guide*.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

ONE IDENTITY by Quest

ONE IDENTITY
by Quest

One IDENTITY
by Quest