One Identity Data Governance Edition 9.2

IT Shop Resource Access Requests User Guide

Data Governance Edition IT Shop Resource Access Requests User Guide
Updated - 19 September 2023, 01:45
Version - 9.2

Contents

Introduction

IT Shop Resource Access requests overview

Governing unstructured data allows you to manage data access, preserve data integrity, and provide content owners with the tools and workflows required to manage their own data.

By publishing a resource to the IT Shop, the resource is placed under governance and is then available for users to request access to it. You can publish and request access to NTFS shares, files and folders, and SharePoint objects from the site level and below. Beginning with Data Governance Edition version 7.0.1, you can request to have a file system share created that can then be made available to others through the IT Shop.

Table 1: Who uses the IT Shop for self-service resource access requests

User	Tasks
Data Governance Administrator	Data Governance Administrators must be assigned to 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.
	The Data Governance Administrator uses the Manager to ensure self-service resource access requests are available in the IT Shop. For more details on setting up the IT Shop, see Setting up resource access requests on page 10 and Setting up share creation requests on page 36.
	The Data Governance Administrator uses the web portal to perform the following tasks after a file share creation ticket is submitted:
	• Select the server for creating the file system share.
	• Define the groups created to access the file system share.
	• Approve or deny requests for creating file system shares.
	• Review approvals made in the past.

User	Tasks
	For more information, see Approving share creation requests on page 44.
Identity/end-user	The Resource Access shelf is available through the Identity & Access Lifecycle shop, which is included by default with the One Identity Manager installation. All active identities are automatically members of this shop and can therefore make requests. End-users or resource consumers use the web portal to perform the following tasks: • Make IT Shop requests to gain access to resources or create file system shares. • Track the status of requests and answer inquires about requests. • Renew a ticket that is about to expire. For more details on making resource access requests, see Requesting access to a governed resource on page 16 and Requesting the creation of a file system share on page 43.
Business owner	Business owners must be assigned to the **Data Governance** | **Direct Owners** application role, which is automatically assigned when ownership is set. 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. The business owner of a resource uses the web portal to perform the following tasks: • Approve or deny requests for resource access. • Request access on behalf of others, such as new identities. • Review approvals made in the past. For more information, see Approving resource access requests on page 20. Business owners who have both the **Data Governance** | **Administrators** and **Data Governance** | **Direct Owners** application roles assigned, can also use the web portal to define who can see and access owned resources. For more information, see Restricting access to self-service resource access requests on page 13.
Identity manager	Identity managers must 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. An identity's manager uses the web portal to perform the following tasks after a file system share creation ticket is submitted:

User	Tasks
	• Approve or deny requests for creating file system shares.
	• Review approvals made in the past.

For more information, see .

About this guide

The One Identity Manager Data Governance Edition IT Shop Resource Access Tickets User Guide is intended for identities interested in learning more about the IT Shop resource access and share creation request process. For Data Governance Administrators, it provides the setup instructions required to make self-service requests available to identities in the IT Shop. For identities, it explains how to initiate a request through the IT Shop and the approval processes used for each type of request. For business owners, group owners and managers, it explains how to approve or deny a request. For Data Governance Administrators, it explains how to select the server to host the new file system share and define the groups that will have permissions to the new file system share. It also provides troubleshooting tips and customization instructions for administrators who are interested in modifying the default configuration and processes used.

For more information on how to use the web portal or set up the IT Shop for governed data, see the following documents:

- *One Identity Manager Web Portal User Guide*
- *One Identity Manager IT Shop Administration Guide*
- *One Identity Manager Data Governance Edition User Guide*

NOTE: This document does not cover all types of product requests that can be made through the web portal. It covers resource access requests for resources placed under governance and file system share creation requests. See the documents listed above for more information about the other features available through the One Identity Manager web portal and IT Shop.

Resource access requests

Using the web portal IT Shop, identities can request access to resources that are governed and published to the IT Shop. When a resource access self-service request is successfully processed and approved, the identity is added to the specified group and access is granted through this group membership.

For more details on setting up the IT Shop, requesting and approving resource access requests, troubleshooting issues, or customizing the default process, see:

- Setting up resource access requests
- Requesting access to a governed resource
- Approving resource access requests
- Troubleshooting resource access requests
- Customizing resource access requests

Setting up resource access requests

As the Data Governance Administrator, use the Manager to perform the following tasks to enable self-service resource access requests within the One Identity Manager IT Shop:

- Identify and assign the business owner for data. For more information, see *Managing business ownership for governed resource* in the *One Identity Manager Data Governance Edition User Guide*.

- Publish a resource (folder or share) to the IT Shop. For more information, see Publishing resources to the IT Shop on page 11.

- (Optional) Define who can see the resource within the IT Shop. For more information, see Restricting access to self-service resource access requests on page 13.

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 identities, 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.

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 identity 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 identity 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.

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 identities 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 identities 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 identities 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 identities 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.

Requesting access to a governed resource

All active identities automatically become members of the Identity & Access Lifestyle shop, which is installed by default, and can therefore make requests, including access requests to governed resources.

File system and SharePoint resources placed under governance and published to the IT Shop are available for self-service requests through the Resource Access service category in the web portal. Selecting the **Resource Access** service category on the **Request** page displays a **Request** page allowing you to request access to governed file system resources or SharePoint resources.

For detailed instructions on how to create resource access requests, see:

Requesting access to a file system resource

Using the IT Shop, you can request access to the following types of file system resources:

- Windows Computer\Share
- NTFS\Folder
- DFS paths

To request access to a file system resource

1. Log on to the One Identity Manager web portal.

2. From the **Home (Welcome)** page, click **Start a new request**.

   The **Request** view appears, which displays the service categories available.

3. Select the **Resource Access** service category.

   NOTE: By default, the recipient is the identity currently logged into the web portal. To change the recipient list, click **Change** to the right of the **Recipient** field. In the **Recipient** dialog, select the identities to be added to the recipient list. To remove an identity from the recipient list, select their name from the **Selected** pane at the bottom of the **Recipient** dialog.

4. Click **Request** in the Request column to the right of the **File system access** product.

   TIP: You can also select the check box to the left of **File system access** and click **Submit request now** button located in the lower right corner of the page..

   The **Requesting file system access** dialog appears, which lists the file system resources that are published to the IT Shop and available for self-service access requests.

   By default, the resources appear in a hierarchical tree view. Click the arrow to the left of a folder to expand it and display the resources available. Click the ☰ **Grid view** button to display a list instead of the tree view. Click the ⤵ **Tree view** button to redisplay the tree view.

   NOTE: By default, all available resources are shown; however, you can use the Managed host's **Assign** link to limit the search to a specific managed host.

5. From the tree view or grid view, select one or more resources from the list to add it to the Selected list (right pane). In addition, the icon to the left of a selected resource changes to a check mark. Click **OK**.

   You can also select the **Enter resource paths manually** check box to enter a resource path (\\servername\foldername). When multiple paths are specified, enter

one path per line. Once you have manually entered the resource paths to include in the request, click **OK**.

> NOTE: To request a DFS Link when **Enter resource paths manually** checkbox is selected, enter the resource path to the DFS link using UNC format and not the associated DFS path.

6. The **My Shopping Cart** page appears, which lists the resources selected on the previous page (and any other requests in your shopping cart). This page also contains a details pane allowing you to specify detailed information for each individual request. If no information is entered in the details pane, a read access request with no time limit is created.

> NOTE: To return to your shopping cart (for example, your session times out before you have completed your request submission), select **Requests not yet submitted** from the **Home** page. You can also click the shopping cart icon (🛒) in the upper right corner of the page and select **Shopping Cart**.

7. To enter details for individual access requests, select a resource from the list (left pane) and enter the following information to complete the access request:

   a. Access: Select the type of access you are requesting, read or write access.

   b. Reason: Enter a reason why you are requesting access to the selected resource.

   c. Priority:

   d. Valid from: Click the check box and use the calendar and clock controls to specify a start date and time for accessing the selected resource.

   e. Valid until: Click the check box and use the calendar and clock controls to specify an end date and time for accessing the selected resource.

> NOTE: To apply the same details to all the resources listed, click the **Details** tab, enter the reason or valid time frame, and click **Apply to all**. Click the **My Shopping Cart** tab to return to your shopping cart requests. This new information is displayed in the details pane when an individual resource request is selected in the left pane.

8. After entering the request details, click the **Submit** button. Clicking this button validates whether the requestor has the permissions required to make the requests in the shopping cart and submits all the requests for approval processing.

   The **Shopping Cart** page closes and a "The request was successfully submitted" message appears at the top of the **My Shopping Cart** page.

9. Click **View the request history** to display the **Request History** page to track the status of your requests.

> NOTE: If you made the request for other identities (that is, changed the recipients list on the **Ticket** page), click the **Advanced search** button. Modify the Display requests options by selecting the **Tickets submitted by you for others** check box and click the **Search** button.

Requesting access to SharePoint resources

Using the IT Shop, you can request access to the following types of SharePoint resources:

- SharePoint\Resource Item
- SharePoint\Site
- SharePoint\List
- SharePoint\Folder
- SharePoint\List Item

NOTE: The identity requesting access to a SharePoint resource must have at least one SharePoint user account. This SharePoint user account must have the "Groups can be inherited" option enabled in the Manager (**SharePoint** | **User accounts (user authentication)** | **Change master data**).

To request access to a SharePoint resource

1. Log on to the One Identity Manager web portal.

2. From the **Home (Welcome)** page, click **Start a new request**.

   The **Request** view appears, which displays the available service categories.

3. Select the **Resource Access** service category.

   NOTE: By default, the recipient is the identity currently logged into the web portal. To change the recipient list, click **Change** to the right of the **Recipient** field. In the **Recipient** dialog, select the identities to be added to the recipient list. To remove an identity from the recipient list, select their name from the **Selected** pane at the bottom of the **Recipient** dialog.

4. Click **Request** in the Request column to the right of the **SharePoint access** product.

   TIP: You can also select the check box to the left of **SharePoint access** and click the **Submit request now** button located in the lower right corner of the page.

   The **Requesting SharePoint access** dialog appears, which lists the SharePoint resources that are published to the IT Shop and available for self-service access requests.

   NOTE: By default, all available resources are shown; however, you can use the Managed host's **Assign** link to limit the search to a specific managed host.

5. Select one or more resources from the list to add it to the Selected list (right pane). In addition to adding the resource to the Selected list, the icon to the left of a selected resource changes to a check mark. Click **OK**.

6. The **My Shopping Cart** page appears, which lists the resources selected on the previous page (and any other requests in your shopping cart). This page also contains a details pane allowing you to specify detailed information for each individual request. If no information is entered in the details pane, a read access request with no time limit is created.

NOTE: To return to your shopping cart (for example, your session times out before you have completed your request submission), select **Requests no yet submitted** from the **Home** page. You can also click the shopping cart icon (🛒) in the upper right corner of the page and select **Shopping Cart**.

7. To enter details for individual access requests, select a resource from the list (left pane) and enter the following information to complete the access request:

   a. Access: Select the type of access you are requesting, read or write access.

   b. Reason: Enter a reason why you are requesting access to the selected resource.

   c. Valid from: Click the check box and use the calendar and clock controls to specify a start date and time for accessing the selected resource.

   d. Valid until: Click the check box and use the calendar and clock controls to specify an end date and time for accessing the selected resource.

   NOTE: To apply the same details to all the resources listed, click the **Details** tab, enter the reason or valid time frame, and click **Apply to all**. Click the **My Shopping Cart** tab to return to your shopping cart requests. This new information is displayed in the details pane when an individual resource request is selected in the left pane.

8. After entering the request details, click the **Submit** button. Clicking this button validates whether the requestor has the permissions required to make the requests in the shopping cart and submits the requests for approval processing.

   The **Shopping Cart** page closes and a "The request was successfully submitted" message appears at the top of the **My Shopping Cart** page.

9. Click **View the request history** to display the **Request History** page to track the status of your requests.

   NOTE: If you made the request for other identities (that is, changed the recipients list on the **Ticket** page), click the **Advanced search** button. Modify the Display requests options by selecting the **Tickets submitted by you for others** check box and click the **Search** button.

Approving resource access requests

Approving resource access request is a two-step process. The resource access request approval workflow recommends a "best fit" group for fulfilling the request, which is then forwarded to the business owner to grant or deny access to the resource and to the suggested group. Once approved by the business owner, the request is forwarded to the group owner to decide if the identity can be added to the group.

All pending requests appear in the following locations in the One Identity Manager web client:

- **Home (Welcome)** page: (**Pending requests**)
- **My Actions** view: (**Ticket | My Actions | Pending Tickets**)

Granting or denying a resource access request

A decision workflow is triggered when a resource access request is submitted, allowing business owners to grant or deny resource access and recommend a group for fulfillment. The "best fit" group appears on the **Pending Tickets** page when the business owner logs on to the web portal. If necessary, the business owner can specify a different group by selecting a group from a list of groups that match the access request.

To approve a resource access request

1. Log on to the One Identity Manager web portal.

   All pending requests appear in the following locations in the One Identity Manager web client:

   - **Home (Welcome)** page: (**Pending requests**)
   - **My Actions** view: (**Ticket | My Actions | Pending Tickets**)

2. To view a list of all pending requests awaiting your decision, select the **Pending Tickets** tile from one of these pages.

   The **Pending Tickets** view appears.

3. Select the request you want to approve. Selecting a request in the left pane displays the request details in the right pane.

   NOTE: If no business owner is assigned to a resource, a warning message appears and you will not be able to approve the resource access request. To assign an owner to a resource, select **Responsibilities | Governance Administration | Governed Data Ownership**. The **Assign ownership** view displays all of the governed resources that currently have no assigned owner.

   NOTE: The system automatically assigns the resource to a group and suggests this group to the business owner of the resource. As the business owner, if you determine that the suggested group is not the "best fit" group for the request, you can select a different group by clicking **Select a group**. If no groups are available or no groups are found that match the access request, the request cannot be approved. For more information on how the "best fit" group is determined, see Group access calculations on page 25.

4. Click the ☑**Approve** button in the **Decision** column, then click **Next**.

   The Approvals view appears allowing you to review your decision and enter additional details about your approval decision.

5. (Optional) On the **Approvals** view, enter the following details regarding your decision:

   a. Reason for approvals: Enter a reason for approving the requests. This reason applies to all approved requests listed, unless there is an individual reason given in the Reason column of an approval.

b. Standard reason: Select a standard reason from a list of previously defined reasons.

> NOTE: For more information about defining standard reasons, see the *One Identity Manager IT Shop Administration Guide*.

c. Valid from: This value is set to **immediately** and cannot be changed.

d. Valid until: Click **unlimited** (or the date displayed) to change the end date for this request.

e. Reason: Click **Enter a reason** to specify a reason for your decision that is specific to the selected request.

6. Once you have specified all the required details about your decision, click **Save approvals**.

Once you have made an approval decision, the request disappears from your list of pending requests. To view your approval decisions, select **Ticket | My Actions | Approval History**. Selecting this option displays the **Approval History** view.

To request additional information about a request

1. From the **Pending Requests** view (**Request | My Actions | Pending Requests**), select the request to which you require additional information.

2. Click **more | Ask for help**, located under the request details pane (right pane).

   Clicking this option displays the **Submit an inquiry about this request** dialog showing a list of identities.

3. Select an identity who is to receive the question.

   The **Submit an inquiry about this request** dialog reappears allowing you to enter your question.

4. Enter your question and click **Save** to place the request on hold and send your question.

   A message stating the inquiry has been submitted is displayed at the top of the **Pending Requests** view. In addition, a **Query** step is added to the workflow in the request's details pane.

5. If you no longer need additional information about a request, click the **Recall last question** button. In the **Recall last question** dialog, enter a reason for recalling the question and click **OK**.

When you request additional information, a request inquiry is submitted to the recipient. That is, when that identity logs on to the web portal, they see a new action in the **Request | My Actions | Request Inquiries** action list. In addition, the recipient receives a "Question about a request" email notification with a link to the web portal. From the **Request Inquires** view, they can then respond to your question.

To view their response, open the **Pending Requests** page, select the required request and open the **Workflow** tab in the details pane.

To revoke a request's hold status

> NOTE: Tickets for which you have requested additional information remain "on hold" even after the question has been answered. This hold state allows you to review the answer to determine if you have the information needed to approve or deny the request. In order to proceed with the approval workflow, release the request from the hold status.

1. From the **Pending Tickets** view (**Ticket** | **My Actions** | **Pending Tickets**), select the request you want to release from hold status.

2. Click the **Revoke hold status** button.

   Revoking the hold status of a request releases the request for approval or editing by other approvers.

Processing requests for resource access

If an identity tries to access a resource and they are denied, they can request access through the web portal IT Shop. (For resources to be available, they must first be published to the IT Shop.)

Tickets follow a defined approval process that determines whether access to the data can be granted or not.

Default request workflow

1. An identity makes a request for access to a resource in the web portal.

2. The "best fit" group is calculated and the assigned business owner decides if the identity's request should be granted.

   They can approve or deny membership in the calculated group or select a different group. For details on how Data Governance Edition determines the groups, see Group access calculations on page 25.

3. The request is then forwarded to the group owner where they can decide whether to add the identity to the group requested by the business owner.

4. If a request is denied, it falls back to the requestor to make another choice.

5. If the request is approved, the identity is added to the group.

Figure 1: Ticket for resource access process
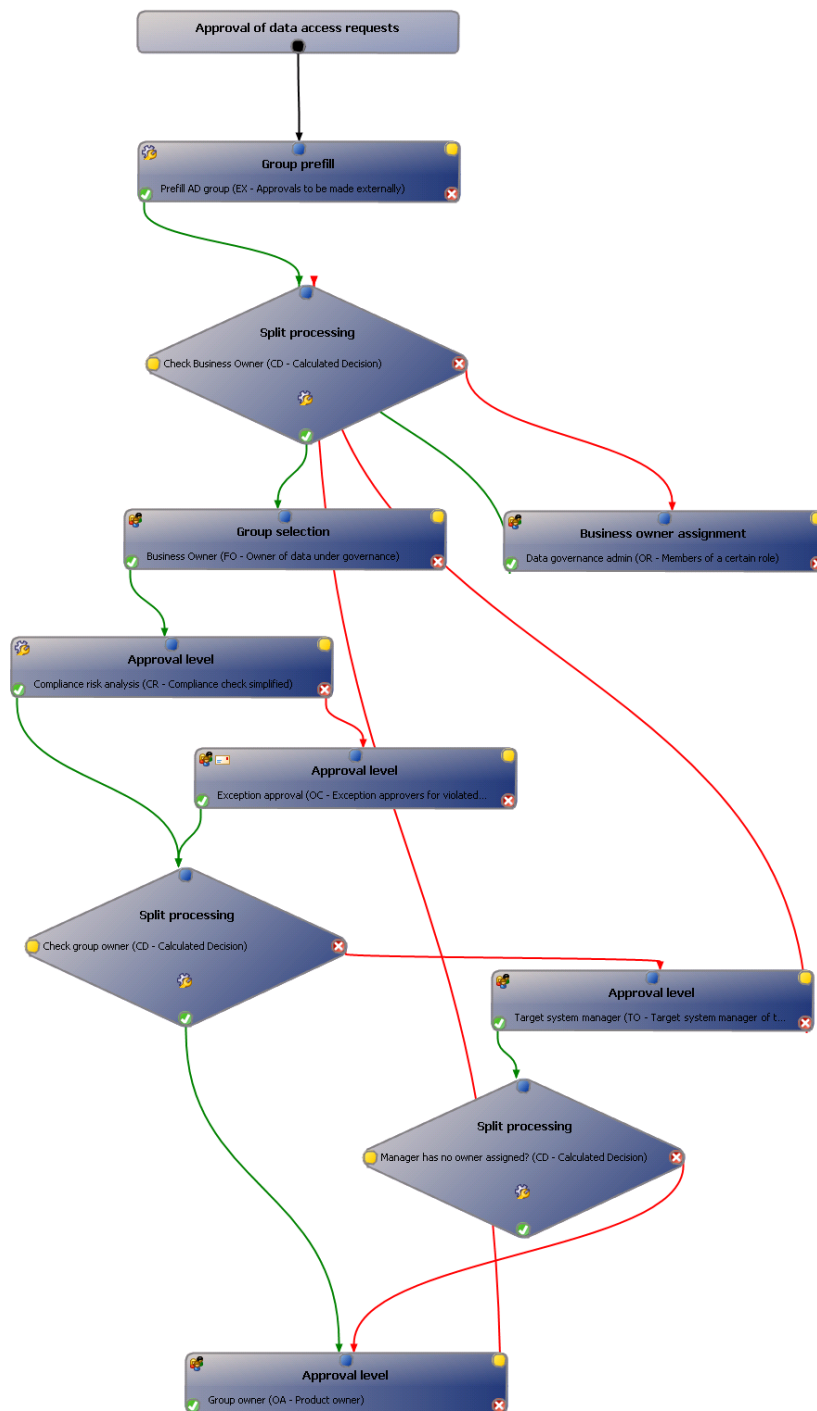
Group access calculations

When an identity requests access to a resource, a calculation is made on how to best provide that access. Generally speaking, it is considered favorable to provide access through group membership rather than placing the account directly on the access control list of the resource. Therefore, only suggestions for gaining access to resources through group memberships are calculated.

NTFS group membership calculations

Data Governance Edition uses the following criteria to determine the "best fit" groups that would provide the requested access to an NTFS resource:

- Origin domain: Groups in the same domain as the requesting identity are considered favorable. Groups from forests outside of the forest of the requesting identity are considered less favorable. Groups from synchronized domains are considered favorable. Domains are synchronized with One Identity Manager through a manual process; they are not done whole forests at a time, but rather, one by one. A group found in a resource's ACL may be from a group that is not in a synchronized domain.

- Distance from the resource: Groups directly in the resources access control list are considered favorable. A group that is nested one or more steps away from the access control list is considered less favorable.

- Group type: Groups are favored in the following order: Global group, Universal group, and Domain Local group. Built-in groups are never considered suitable selections.

- IT Shop: Groups that have been published to the IT Shop are considered favorable. For a group to be in the IT Shop, it must be in a domain that is synchronized and an administrator must have added it specifically to the IT Shop.

- Access rights: Groups that contain the exact rights that were requested are considered favorable. A group with slightly more rights may still be suggested, but is considered less favorable.

- Access inheritance: Groups whose rights to the targeted resource are explicit are favorable. Groups that have been delegated access to the targeted resource through inherited permissions are considered less favorable.

- Domain Local group membership: Domain Local groups with no other Global or Universal groups nested within them are favorable. Domain Local groups with these types of nested groups are considered less favorable.

- Group membership rules: Global groups that exist in the same domain as the identity are favorable. If the group is Universal, the identity must exist in the same forest as the group.

NOTE: The criteria used to determine suitability for group selection is based on Microsoft best practices for setting file and folder security in a distributed environment. Under certain conditions, a security group that would give identities their requested access may

be deemed inappropriate and therefore the group is not available as an option.

SharePoint group access calculations

Data Governance Edition uses the following criteria to determine the "best fit" groups that would provide the requested access to a SharePoint resource:

- Group membership: Data Governance Edition favors groups that grant the requested access without any additional permissions. Groups that provide extra permissions are considered less favorable. Groups that confer farm administrator, site collection administrator, or allow for the delegation of permissions are considered ineligible.

- Self-service access: Data Governance Edition favors groups to which the user can request access through the web portal. These groups are likely to be the safest way to gain access to a resource without unintended side affects.

- Active Directory groups: Active Directory groups that are nested within SharePoint groups are given preference. The nesting of Active Directory groups provides a balance between the visibility and features of a SharePoint group, and the provisioning power of an Active Directory group. Global and Universal groups are favored.

- SharePoint groups: If your organization prefers to use SharePoint groups instead of Active Directory, preference can be given to these groups.

- WebApp policy: Data Governance Edition ignores groups that are denied access to a resource through a WebApp policy, even if access is directly conferred elsewhere.

Troubleshooting resource access requests

The following topics explain possible causes and resolutions to issues you may encounter when working with self-service resource access requests:

- No groups available for resource access request
- Wrong group displayed for Share access request

No groups available for resource access request

On the **Pending Requests** page of the web portal, there is no group listed. When **Select a group** is clicked, the following message appears, " No groups available", and the request cannot be approved.

Cause

The system automatically calculates the "best fit" groups and assigns the resource to a group that matches the access requested. When the business owner logs on to the web portal, the "best fit" group is displayed for the self-service access request on the **Pending Requests** page. The business owner can approve the suggested group or manually specify a different group that meets the criteria of the ticket by clicking the **Select a group** button. If no groups are available or no groups are found that match the access request, the request cannot be approved.

When no groups are listed for the selected request, means that Data Governance Edition could not find any groups that match the level of access requested. That is, no groups met the criteria used to calculate the "best fit" group.

- For NTFS group membership calculations, the system takes the following into consideration: origin domain, distance from the resource, group type, whether the group is published to the IT Shop, access rights, access inheritance, Domain Local group membership, and group membership rules.

- For SharePoint group access calculations, the system takes the following into consideration: group membership, self-service access, Active Directory groups, SharePoint groups, and WebApp policy.

For more information on processing requests and how Data Governance Edition calculates the "best fit" group for resource access, see Group access calculations on page 25.

Resolution

If you are requesting access to a share, use the Object Browser to check the UseFolderForITShop property in the QAMDuG table. If this flag is set to True, the backing folder security (Folder Permissions) is being used (not the Share permissions). Verify that there are groups that meet the requested access defined for folder security. See Wrong group displayed for Share access request on page 28 for more information on reviewing a governed share's properties in the QAMDuG table.

Review the criteria used for calculating a "best fit" group and create a group that satisfies the access requested. For example, consider the following when creating a group:

- Access rights: Create a group that contains the exact access rights requested. For example, if an identity requests read access, but all available groups allow more rights (for example, write or full access), no groups are found. Creating a group that is limited to read access would satisfy the access requested.

  NOTE: Review the Advanced options for the group to ensure that only the default permissions are set; setting different advanced permissions may also affect the "best fit" group calculations.

- Group type: Create a Global group and a Domain Local group; nesting the Global group within the Domain Local group. The Domain Local group is ACL'd on the resource, but the Global group should be suggested as the correct group.

> NOTE: Data Governance Edition follows Microsoft best practices when ranking groups, where Global groups are ranked higher than Domain Local groups.

The "best fit" group is determined using a series of calculators that return a value in the range of -2 to +2. Review the Data Governance Service log.txt file to see the groups that were evaluated and the results of these calculations. The calculators cannot be changed; however, you can modify the positive and negative multipliers in the DataGovernanceEdition.Service.exe.config file if necessary. For more information on modifying these multipliers, see .

Additionally, valid groups must be associated with products in the IT Shop and be requestable by the requester.

Wrong group displayed for Share access request

On the **Pending Request** page of the web portal, it appears that the wrong group was assigned to a Share access request, and no other appropriate groups are available.

Cause

The most likely cause for this scenario has to do with whether you selected to use the backing folder security when placing the share under governance. That is, if you selected the **Use backing folder security for self-service** option when placing the share under governance (default), then the backing folder security is used for the share. However, if you cleared the **Use backing folder security for self-service** option when you placed the share under governance, then the share permissions are used for the share.

See the Resolution to determine which permissions are being used.

Resolution

Use the Object Browser to review the properties for the governed share resource in the QAMDuG table. There should be two entries for this governed share in the QAMDuG table; one entry for the share and one entry for the backing folder.

1. In the navigation pane, locate and select **QAMDuG | Data objects under governance**.
2. In the Data objects under governance result list, select the share resource and verify the following properties:
   - DisplayPath: *<Share's path>*
   - UID_QAMResourceType: Windows Computer\Share
3. Locate the **UseFolderForITShop** flag, which contains either a True or False value:

- **True:** Data Governance Edition uses the backing folder security for the share. That is, the Share permissions do not matter.

- **False:** Data Governance Edition uses the Share permissions for the share.

   NOTE: By default, this value is set to True for shares. That is, the **Use backing folder security for self-service** option was selected when you placed a share under governance. You must clear this option to use the Share permissions.

4. Once you have verified that the correct permissions (backing folder security or Share permissions) are being used, modify the permissions as required to define access rights that match the request.

5. It is best to deny the original request and have the requestor submit a new resource access request.

Customizing resource access requests

NOTE: The Resource Access shelf is available through the Identity & Access Lifecycle shop, which is included by default with the One Identity Manager installation. The File system access, SharePoint access and New file system share products are available in the Resource Access shelf by default. In the default installation, several approval policies are assigned to the Identity & Access Lifecycle shop; therefore, requests from this shop are run through predefined approval processes.

You can use the shop to request standard products or you can extend it by adding additional shelves, assigning requestable products, or by setting up your own IT Shop solution. You can also customize the approval processes, including approval policies and approval workflows. For more information on using and customizing the Identity & Access Lifecycle shop, see the *One Identity Manager IT Shop Administration Guide*.

A series of suitability calculators are used to determine the "best fit" groups for providing access to NTFS and SharePoint resources. These suitability calculators can be found in the DataGovernanceEdition.Service.exe.config file in the Data Governance service directory. These calculators cannot be modified; however, the multipliers used in the calculators can be modified to customize the weight information to rank a group. In addition, you can define your own suitability calculator to be used for self-service operations. The following topics explain how to implement these customizations:

- Modifying the calculators
- Creating a group suitability calculator

Prior to making changes to the default suitability calculators, it is recommended that you review and understand how Data Governance Edition determines the "best fit" groups:

- NTFS group membership calculations
- SharePoint group access calculations

Modifying the calculators

The "best fit" group is determined through a series of calculators that work on various criteria. Each calculator returns a value in the range of -2 to +2:

- VeryBad (-2)
- Bad (-1)
- Neutral (0)
- Good (+1)
- VeryGood (+2)

If the value is positive, it is multiplied by the calculator's positive multiplier and added to the total, increasing it. If the value is negative, the value is multiplied by the calculator's negative multiplier and added to the total, decreasing it. The total after all the calculators have been run is used to rank the groups from which the business owner can select. The group with the highest total is marked as the "best fit" group.

NOTE: Multiple suitability calculators can be run against the same group information, and then weighted with their own specific multipliers to give the group a ranking among other groups to determine what the "best fit" group is for access request self-service operations.

The calculators cannot be changed, but you can modify the positive and negative multipliers by changing values in the DataGovernanceEdition.Service.exe.config file in the Data Governance service directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server). Review comments for multipliers in the configuration file to find information on how the values are determined. To remove a calculator, simply set both its positive and negative multipliers to 0.

NOTE: Keep in mind that the multiplier values are only relative to one another. If you doubled all the multipliers, there would be no change in the resulting set of groups returned to the user. If you want your desired criteria to be considered more important, set the multipliers on those calculators to be higher relative to the rest.

In addition, the following configuration options, also in the configuration file, affect what groups are shown to the business owner:

- SelfService.SuitabilityThreshold (Default: 100).

  This value determines the lowest possible suitability score that can be returned by the self-service access request. Any group whose calculated suitability falls below this threshold is not displayed to the business owner.

- SelfService.AllowNonPublishedGroups (Default: false) and SelfService.AllowUnsynchronizedGroups (Default: false).

  These values prevent any groups that are not synchronized by One Identity Manager or not published to the IT Shop from displaying in the self-service options in the web portal.

For more detailed information about the self-service suitability calculation multipliers and self-service configuration options, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Creating a group suitability calculator

> NOTE: You can create a calculator in any .NET compatible language. The following example is based on a C# implementation.

To create the calculator

1. Start a new "Class Library" project in your editor.

   > NOTE: Ensure that the project is compiling for .NET v3.5 or lower. When run in context with the Data Governance server, .NET v4.5.1 or lower is used.

2. Add references for the following Data Governance assemblies (they are located in the %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server folder):

   - QAM.Common.Interfaces.dll
   - QAM.Common.Shared.dll
   - QAM.Server.Util.dll

3. Author a class that derives from the QAM.Server.Util.SelfService.BaseGroupSuitabilityProcessor class.

   This base class implements the QAM.Server.Util.SelfService.IDetermineGroupSuitability interface, which is required for subsequent steps.

4. Override the base class' Execute() method, and in this method enter the SuitabilityDelta property. This is an enumeration which contains values ranging from VeryBad to VeryGood:

   - VeryBad
   - Bad
   - Neutral
   - Good
   - VeryGood
   - Ineligible (This removes the group as a contender.)

   Based on this criteria, a group is scored high or low and weighted up or down with the PositiveMultiplier and NegativeMultiplier properties.

5. Author a class that implements the QAM.Server.Util.SelfService.IDetermineGroupSuitabilityFactory interface. The one method in this interface should return an instance of the first class; the one that implements IDetermineGroupSuitability.

   Once you have implemented the two classes, compile the DLL and place it in a folder on the Data Governance server. To instruct the Data Governance server to use this calculator to determine the best groups for self-service requests, create a plugin file in the %Program Files%\One Identity\One Identity Manager Data Governance Edition\Server folder.

> NOTE: A file called "base.SuitabilityCalculators.xml" exists, because it is shipped with the Data Governance server. Unless you need to disable an existing calculator, it is recommended not to modify this file.

6. Create a file in the server folder named [CustomName].SuitabilityCalculators.xml.

   The content should look like the following:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<Plugins>
  <Plugin
    Assembly="ExampleCalculator.dll"
    Type="ExampleCalculator.MyCalculatorFactory">
    <Property>NTFS</Property>
    <Property>Windows Computer\Share</Property>
  </Plugin>
</Plugins>
```

   Where the value of the Assembly attribute is the name (or full path) to the assembly containing your custom Group Suitability Calculator factory class and the value of the Type attribute is the fully qualified Namespace.Classname of your Group Suitability Calculator factory class. If the Assembly path is not absolute, it is interpreted as being relative to the %Program Files%\One Identity\One Identity Manager Data Governance Edition\Server folder.

   The values in the <Property> nodes can be any resource namespace or fully qualified resource type that Data Governance Edition supports, although self-service requests can currently be made for only files, folders, shares, and SharePoint resources.

7. Once you restart the Data Governance server, the new calculator is used for self-service requests.

Example implementation of class deriving from BaseGroupSuitabilityProcessor

```
/// <summary>
/// A simple suitability calculator to show how to influence group scores for self-service operations
/// </summary>
public class MyCalculator : QAM.Server.Util.SelfService.BaseGroupSuitabilityProcessor
{
    /// <summary>
    /// Initializes a new instance of the MyCalculator class
    /// </summary>
    /// <param name="targetGroup">
    /// The group to be associated with this instance of this calculator
    /// </param>
```

```csharp
public MyCalculator(QAM.Common.Interfaces.AccessSelfServiceGroupInformation
targetGroup)
 : base(targetGroup)
{
        // Optionally set our multipliers. This can also be done in the
        // DataGovernanceEdition.Service.exe.config file
        // like this:
        //
        // <add key="MyCalculator.PositiveMultiplier" value="1000000"/>
        // <add key="MyCalculator.NegativeMultiplier" value="100"/>
        //
        // It can be advantageous to set these values in the configuration file so that
        // a recompile is not necessary to change the weighting of the calculator.
        //
        // The default multiplier is 100, so this one will drastically boost the score
        // of this calculator
        this.PositiveMultiplier = 1000000;
        this.NegativeMultiplier = 100;
}
/// <summary>
/// At the end of the execution of this method, the SuitabilityDelta property should
be filled in.
/// </summary>
public override void Execute()
{
        // Using the Target group, determine on a scale of -2 to +2 how suitable it is,
        // or if it should be marked as completely ineligible.
        //
        // For this example, we will give groups that contain the string "Read" a
        super-high
        // boost based on our "very good" score and the positive multiplier of
        one  million.
        // If they do not meet this arbitrary requirement of containing "Read",
        we  will  mark
        // the group as ineligible.
        int indexOfRead = this.TargetGroup.SamAccountName.IndexOf(
        "Read",
        System.StringComparison.OrdinalIgnoreCase);
```

```
            if (-1 < indexOfRead)

            {

                    this.SuitabilityDelta =

            QAM.Server.Util.SelfService.GroupSuitabilityModifier.VeryGood;

            }

            else

            {

                    this.SuitabilityDelta =

            QAM.Server.Util.SelfService.GroupSuitabilityModifier.Ineligible;

            }

        }

}
```

Example of a class implementing IDetermineGroupSuitabilityFactory

```
/// <summary>
/// A class to wrap the factory method that creates our suitability calculator
/// </summary>
public class MyCalculatorFactory :
QAM.Server.Util.SelfService.IDetermineGroupSuitabilityFactory

    {/// <summary>

    /// A factory method to create an instance of our suitability calculator

    /// </summary>

    /// <param name="group">The group for which we want to compute the suitability
    score</param>

    /// <returns>The calculator that will compute the suitability score for our
    group</returns>

    public QAM.Server.Util.SelfService.IDetermineGroupSuitability Create(

    QAM.Common.Interfaces.AccessSelfServiceGroupInformation group)

    {

            return new MyCalculator(group);

    }

}
```

Supported resource types

- NFS\File
- NFS\Folder
- NTFS\Folder
- NTFS\File
- Service Identities\Windows Service Identity

- SharePoint\Farm
- SharePoint\FarmAdminRight
- SharePoint\Folder
- SharePoint\List
- SharePoint\ListItem
- SharePoint\ResourceItem
- SharePoint\ServiceApplicationPermission
- SharePoint\Site
- SharePoint\SiteCollection
- SharePoint\SiteCollectionAdminRight
- SharePoint\WebApplication
- SharePoint\WebAppPolicy
- Windows Computer\Local User Rights
- Windows Computer\Operating System Administrative Rights
- Windows Computer\Share

Share creation requests

Using the web portal IT Shop, identities can use the new managed resource feature to request that a file system share be created. Similar to resource access requests, when a file share creation self-service request is successfully processed and approved, the recipient (identity) is added to the specified group and access is granted through this group membership. In addition, if the self-service request indicates that the new share is to be published to the IT Shop, it will be available for other identities to request access to it.

The basic configuration and default process included in this release of Data Governance Edition is meant for creating file system shares in a single domain. This basic configuration fulfills self-service share creation requests by creating new file shares and granting access through group membership, based on Microsoft best practices. For more details on setting up the IT Shop, requesting and approving share creation requests, troubleshooting issues, or customizing the default configuration or process, see:

- Setting up share creation requests
- Requesting the creation of a file system share
- Approving share creation requests
- Troubleshooting share creation requests
- Customizing share creation requests

Setting up share creation requests

As a Data Governance Administrator, perform the following tasks to enable the self-service share creation requests within the One Identity Manager IT shop:

- Run a full Active Directory synchronization to map and synchronize target domains and containers in One Identity Manager. For more information on performing an Active Directory synchronization, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.

  NOTE: The synchronization base object in Active Directory requires Read and Write access rights.

- Specify the managed hosts that can be used to host managed resources (file shares). For more information, see Specifying target machines on page 37.

- For every managed domain, specify an Active Directory container and a full control group where groups created by Data Governance Edition for managed resources will be stored. For more information, see Updating managed resource type domain object with full-control group and Active Directory container on page 38.

- Create and specify the share root paths where new file shares are to be created. For more information, see Creating and specifying share root paths on page 40.

- Edit Active Directory group insertion process parameters to enable retries. For more information, see Editing Active Directory group insertion process parameters on page 41.

- (Optional) Enable the creation of a restriction list based on the organizational properties of the requester's Identity record. For more information, see Restricting access to managed resources on page 41.

Specifying target machines

Once you have completed the Active Directory synchronization and added your managed hosts, specify the managed hosts that can be used to host a managed resource (for example, file shares created through the IT Shop self-service request functionality).

To identify a managed host as a managed resource host (Object Browser)

1. Open the Object Browser.

2. In the navigation pane, locate and select **QAMNode** | **Managed Hosts**.

3. In the **Managed Hosts** result list pane, select the target managed host.

4. Under Simple properties, locate the **IsManagedResourceHost** property and set the value to **True**.

5. Click the **Save** toolbar button.

6. Repeat for all managed hosts that can host file shares.

To identify a managed host as a managed resource host (PowerShell)

1. If necessary, run the following cmdlet to 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 enable the IsManagedResourceHost property:

   Set-QManagedHostProperties -ManagedHostId <String> -IsManagedResourceHost $true

ONE IDENTITY by Quest

- ManagedHostId: Specify the ID (GUID format) of the managed host whose properties are to be updated.
- IsManagedResourceHost: Changing this value to $true specifies that this managed host can be used to host a managed resource.

NOTE: You can also enable the IsManagedResourceHost property when adding new managed hosts using the Add-QManagedHostByAccountName Powershell cmdlet.

Updating managed resource type domain object with full-control group and Active Directory container

For every domain where you have managed hosts flagged as managed resource hosts (managed hosts that have the **IsManagedResourceHost** property set to **True**), you need to specify an Active Directory container and a full control group for each managed resource type. In this release, the basic configuration includes only one managed resource type, Simple Share; therefore, in each managed domain, specify the Active Directory container where new groups are to be created and specify the group to be given full administrative control to the share.

NOTE: Only groups, containers and domains that have been previously synchronized into the One Identity Manager database are available for use.

NOTE: Managed resource functions are used by the default process to locate an appropriate Active Directory container, locate suitable job servers for file system operations and implement restriction list processing when creating a new managed resource share. To use custom scripts for any of these functions, see Managed resource functions on page 61.

To update a managed resource type domain object (Object Browser)

1. Open the Object Browser.

2. In the Navigation view, locate and select **QAMManagedResourceTypeDomain** | **Managed Resource Type Domain**.

3. In the **Managed Resource Type Domains** result list pane, click the ⊞ **Insert** toolbar button or right-click command.

4. In the new **Managed Resource Type Domains** page (right pane), specify the following:

   - UID_ADSContainer: Use the drop-down menu to select the Active Directory container to use for managed group creation for a given managed resource type in the specified Active Directory domain.

   - UID_ADSDomain: Use the drop-down menu to select the Active Directory domain this object applies to.

- UID_FileOperationsServerTag: Use the drop-down menu to select the Server tag (Server Function) that identifies which job servers can fulfill functions involving file operations. That is, operations involving the creation of folders and shares on managed hosts. If this parameter is not specified, the **Data Governance connector** (QAM-Connector-DGE server function) is used. For more information on using a custom script to locate the job server, see Managed resource functions on page 61.

- UID_FullControlGroup: Use the drop-down menu to select the full control group to be used to provide administrative access to new file shares that are created.

- UID_QAMManagedResourceType: Use the drop-down menu to select the managed resource type. By default, Simple Share is the only value available.

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

   The new managed resource type domain object appears in the **Managed Resource Type Domains** result list pane.

To update a managed resource type domain object (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 add a new managed resource type domain:

   Add-QManagedResourceTypeDomain -ManagedResourceTypeID <String> -DomainID <String> [-ContainerID [<String>]] -FullControlGroupID <String> [-FileOperationsServerTagID [<String>]]

   - ManagedResourceTypeID: Enter the ID assigned to the managed resource type (Simple Share) associated with this object.

   - DomainID: Enter the ID assigned to the Active Directory domain this object applies to (UID_ADSDomain in ADSDomain table).

   - ContainerID: (Optional) Enter the ID assigned to the Active Directory container to use for managed group creation for the specified managed resource type in the specified Active Directory domain (UID_ADSContainer in ADSContainer table)

   - FullControlGroupID: Enter the ID assigned to the full control group to be used to provide administrative access to new file shares that are created.

   - FileOperationsServerTagID: (Optional) Enter the value assigned to the Server tag (Server Function) that identifies which job servers can fulfill functions involving file operations. That is, operations involving the creation of folders and shares on managed hosts. Enter the value assigned to the server tag when it was created, which may be an ID, such as QAM-Connector-DGE, for predefined server tags or a GUID for custom server tags. If this parameter is not specified, the Data Governance connector (QAM-Connector-DGE server

function) is used. For more information on using a custom script to locate the job server, see

For more information, see

Creating and specifying share root paths

In addition to specifying the target machines, you must also specify the share root paths where new shares are to be created.

On each server that is hosting a target local managed resource host, identify an existing root folder or create a root folder where you want shares created under. For example, C:\ShareRoot.

NOTE: Make note of the UNC resolvable path to that folder. For example, if C:\ShareRoot is not shared, the path would be c$\ShareRoot.

To specify share root paths

Use the Object browser or Windows PowerShell to specify the share root paths where shares are to be created.

1. Open the Object Browser.

2. In the **Navigation** view, locate and select **QAMManagedShareRootPaths**.

3. In the **Managed Share Root Paths** result list pane, click the ➕ **Insert** toolbar button or right-click command.

4. In the new **Managed Share Root Paths** page, specify the following:

   - UID_QAMNode: Use the drop-down menu to select the managed host (QAMNode) to which the path applies.

   - Description: (Optional) Enter a description for the share root path.

   - RootPath: Specify the root path, for example D$\ShareRoot1.

     NOTE: Only local managed hosts are supported at this time. Do not include the machine name as part of the path.

   NOTE: UID_QAMManagedShareRootPath: This value is automatically generated by One Identity Manager.

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

   The new managed share root path appears in the **Managed Share Root Paths** result list pane.

OR

1. On the Data Governance server, run the following PowerShell cmdlet, changing the -QAMNodeID and -RootPath values appropriately:

   Add-QManagedShareRootPath -QAMNodeID "ManagedHost ID" -RootPath "c$\ShareRoot"

Edit Active Directory group insertion process parameters

Use the Designer to enable retries for **ADS_ADSGroup_Insert** process.

1. Open the Designer.
2. In the **Navigation** view, locate and select **Process Orchestration**.
3. Select **Processes | ADSGroup | ADS_ADSGroup_Insert**.
4. Click on **Insert Group** process step in the **Process Overview** form.
5. In the **Process** step properties view, click on **Error handling**.
6. Select the checkbox corresponding to **Wait mode on error**.
7. Enter a value greater than 1 for both **Latency[min]** and **Retries**.

   NOTE: These values can vary depending on the environment.

8. Commit the changes to the main database. Use the **Database | Commit to database** menu item.
9. Once the changes are committed to the main database, compile the database. Use the **Database | Database Compiler** menu item.

Restricting access to managed resources

Data Governance Edition provides a default restriction list processing subroutine that runs as part of the QAM Create DGE Managed Resource process chain used to create a managed resource share. By default, no restriction list is set; however, you can enable the SetRestrictionList parameter on the QAMManagedResourceType record to automatically create a restriction list based on the department, location and cost center organizational properties of the requester's Identity record. That is, with the SetRestrictionList parameter enabled:

- If the requester has a location set, set a restriction on that location.
- If the requester has a department set, set a restriction on that department.
- If the requester has a cost center set, set a restriction on that cost center.

For example, if the identity submitting the share creation request has a department defined on their Identity record, this department is added to the restriction list. Meaning the new share will only be available for access requests by users belonging to that same department as defined by their Identity record. Keep in mind, using the default restriction list processing subroutine means that if the requester has more than one of these organizational properties set (for example, location, department and cost center), all of

these organizational properties are added to the restriction list and users must match all of these restrictions in order to request access to the new share.

If the default restriction list processing subroutine does not meet your needs, you can replace it with a custom script. For more information, see Managed resource functions on page 61.

To enable the default restriction list processing subroutine for the Simple Share resource type (Object Browser)

1. Open the Object Browser.

2. In the Navigation view, locate and select **QAMManagedResourceType**.

3. In the **Managed Resource Types** result list, select **Simple Share**.

4. In the **Simple Share (ManagedResourceType)** page (right pane), set the **SetRestrictionList** value to **True**.

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

To enable the default restriction list processing subroutine for the Simple Share resource type (PowerShell)

1. If necessary, run the following cmdlet to 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 enable the SetRestrictionList parameter for the Simple Share managed resource type:

   Set-QManagedResourceType -ID *<UID_QAMManagedResourceType Value>* - SetRestrictionList $true

   - Id: Specify the ID of the Simple Share managed resource type.

   - SetRestrictionList: By setting this value to $true, a restriction list is set for this type of managed resource.

For more information, see Set-QManagedResourceType on page 80.

To view organizational properties automatically added to the restriction list (Manager)

When a new file share is created through a self-service request in the IT Shop, you can use the Manager to view the organizational structure restrictions applied.

1. Open the Manager.

2. Select **Data Governance** | **Managed hosts** from the navigation view.

3. Select the required managed host and select **Governed data** from the tasks view or right-click menu.

4. Locate and double-click the resource that is published to the IT Shop.

The **Change master data** view for the resource appears.

5. Select **Assign organizations** from the tasks view or right-click menu.

   The **Organization assignments** page appears, which consists of three tabbed pages (Departments, Locations, and Cost centers). Organization properties used to restrict access to the share will be listed in the top pane of each of these tabs.

Requesting the creation of a file system share

All active identities automatically become members of the Identity & Access Lifestyle shop, which is installed by default, and can therefore make requests, including file system creation requests.

You submit a self-service share creation request using the Resource Access service category in the One Identity Manager web portal. Selecting the **Resource Access** service category displays a **Request** page allowing you to request the creation of a file system share.

To request the creation of a new share

1. Log on to the One Identity Manager web portal.

2. From the **Home (Welcome)** page, click **Start a new request**.

   The **Request** view appears, which displays the available service categories.

3. Select the **Resource Access** service category.

   The **Request** page appears.

   NOTE: By default, the recipient is the identity currently logged into the web portal. To change the recipient list, click **Change** to the right of the **Recipient** field. In the **Recipient** dialog, select the identities to be added to the recipient list. To remove an identity from the recipient list, select their name from the **Selected** pane at the bottom of the **Recipient** dialog.

4. Click **Request** in the Request column to the right of the **New file system share** product.

   TIP: You can also select the check box to the left of the **New file system share** product in the grid and click **Submit Request now** button located in the lower right corner of the page.

5. In the **Requesting new file system share** dialog, enter the following information:

   - Name for the new file share
   - Purpose for the new file share

   The **Allow others in your organization to be able to request access to this resource** option is selected by default, making the share available to others through

the IT Shop. If you do not want others in your organization to request access to this share, clear this check box.

Click **OK**.

6. The **My Shopping Cart** page appears, where a **New file system share** request is listed along with the recipient and status.

   NOTE: If you need to return to your shopping cart (for example, your session times out before you have completed your request submission), select **Requests not yet submitted** from the **Home** page. You can also click the shopping cart icon (🛒) in the upper right corner of the page and select **Shopping Cart**.

7. Click the **Submit** button to validate whether the requestor has the permissions required to make the requests in your shopping cart and submit the requests for approval processing.

   The **Shopping Cart** page closes and a "The request was successfully submitted" message appears at the top of the **My Shopping Cart** page.

8. Click **View the request history** to display the **Request History** page to track the current status of your requests.

   NOTE: If you made the request for other identities (that is, changed the recipients list on the **Ticket** page), click the **Advanced search** button. Modify the Display requests options by selecting the **Tickets submitted by you for others** check box and click the **Search** button.

Approving share creation requests

All IT shop requests are subject to a defined approval process where authorized identities grant or deny approval for the request. A share creation request approval workflow is a two-step process. First the identity's manager approves the request. Once the manager approves the request, the Data Governance Administrator specifies the server that will host the new share and the groups to be created to provide access.

NOTE: If an identity does not have a manager assigned, that approval step is bypassed and the request goes directly to the Data Governance Administrator.

For managers and Data Governance Administrators, all pending requests appear in the following locations in the One Identity Manager web client:

- **Home (Welcome)** page: **Pending requests**
- **My Actions** view: (**Request | My Actions | Pending Requests**)

Granting or denying file system share creation requests

To approve a file share creation request (Identity's Manager)

NOTE: If an identity does not have a manager assigned, this approval step is bypassed and the request goes directly to the Data Governance Administrator.

1. Log on to the One Identity Manager web portal.

   All pending requests appear in the following locations in the One Identity Manager web client:

   - **Home (Welcome)** page: (**Pending requests**)
   - **My Actions** page: (**Request | My Actions | Pending Requests**)

2. To view a list of all pending requests awaiting your decision, click the **Pending requests** tile from one of these pages.

   The **Pending Requests** view appears.

3. Select the request to be approved. Selecting a request in the left pane displays the request details in the right pane.

4. Click the ☑**Approve** button in the **Decision** column, then click **Next**.

   The **Approvals** view appears allowing you to review your decision and enter additional details about your approval decision.

5. (Optional) On the **Approvals** view, enter the following details regarding your decision:

   a. Reason for approvals: Enter a reason for approving the requests. This reason applies to all approved requests listed unless there is an individual reason given in the Reason column of an approval.

   b. Standard reason: Select a standard reason from a list of previously defined reasons.

      NOTE: For more information about defining standard reasons, see the *One Identity Manager IT Shop Administration Guide*.

   c. Valid from: This is set to **immediately** and cannot be changed.

   d. Valid until: Does not apply to this type of request. This is set to **unlimited** and changing the end date has no effect on the request.

   e. Reason: Click **Enter a reason** to specify a reason for your decision that is specific to the selected request.

6. Click **Save approvals**.

Once you make an approval decision, the request disappears from your list of pending requests. To view your approval decisions, select **Request | My Actions | Approval History**. Selecting this tile displays the **Approval History** view.

To request additional information about a request

1. From the **Pending Requests** view (**Request | My Actions | Pending Requests**), select the request to which you require additional information.

2. Click **more | Ask for help**, located under the request details pane (right pane).

   Clicking this option displays the **Submit an inquiry about this request** dialog showing a list of identities.

3. Select an identity who is to receive the question.

   The **Submit an inquiry about this request** dialog reappears allowing you to enter your question.

4. Enter your question and click **Save** to place the request on hold and send your question.

   A message stating the inquiry has been submitted is displayed at the top of the **Pending Requests** view. In addition, a **Query** step is added to the workflow in the request's details pane.

5. If you no longer need additional information about a request, click the **Recall last question** button. In the **Recall last question** dialog, enter a reason for recalling the question and click **OK**.

When you request additional information, a request inquiry is submitted to the recipient. That is, when that identity logs on to the web portal, they see a new action in the **Request | My Actions | Request Inquiries** action list. In addition, the recipient receives a "Question about a request" email notification with a link to the web portal. From the **Request Inquires** view, they can then respond to your question.

To view their response, open the **Pending Requests** page, select the required request and open the **Workflow** tab in the details pane.

To revoke a request's hold status

NOTE: Tickets for which you have requested additional information remain "on hold" even after the question has been answered. This hold state allows you to review the answer to determine if you have the information needed to approve or deny the request. In order to proceed with the approval workflow, release the request from the hold status.

1. From the **Pending Tickets** view (**Ticket | My Actions | Pending Tickets**), select the request you want to release from hold status.

2. Click the **Revoke hold status** button.

   Revoking the hold status of a request releases the request for approval or editing by other approvers.

To select where the file share is to be created (Data Governance Administrator)

1. Log on to the One Identity Manager web portal.

   All pending requests appear in the following locations in the One Identity Manager web client:

- **Home (Welcome)** page: (**Pending requests**)
- **My Actions** view: (**Request** | **My Actions** | **Pending Requests**)

2. To view a list of all pending requests awaiting your decision, select the **Pending Requests** tile from one of these pages.

   The **Pending Requests** view appears.

3. On the **Pending Requests** view, select the required request.

   NOTE: If the manager approval step was bypassed, the following warning appears "Request does not have manager".

4. Click the **Select server and groups** button.

   The **New File Share** dialog appears, which consists of two tabbed pages:

   - **File Share**: Use this page to select the server to host the file share and the root path for the new file share. You can also specify whether to publish the share to the IT Shop.
   - **Permissions**: Use this page to specify the group naming pattern to be used for the groups that are created to support the new file share.

   TIP: By default a server host and group naming pattern are selected for you; you can use these pages to change these default selections. However, you must specify the root path in order to proceed. If the **OK** button at the bottom of the dialog is disabled, ensure that you have selected a root path.

5. On the **File Share** page, select the server that is to host the share and the root path for the new file share.

   NOTE: The server must be an appropriately configured managed host. For more information on configuring a managed host for hosting file shares and adding a share root path, see Setting up share creation requests on page 36.

   If you see the following message, "For the domain of the selected File Share host, please specify an Active Directory container in which to create permissions groups and please specify an Active Directory group that will have full control of this new File Share", see the directions provided in Updating managed resource type domain object with full-control group and Active Directory container on page 38.

   a. Share Name: This field displays the name specified in the request. If necessary, use this field to rename the share.

   b. Publish to IT Shop: To publish the share to the IT Shop, select the check box. If you do not want the share available to others through the IT Shop, clear the check box. This check box reflects the option specified in the request; but can be changed using this check box.

   c. File Share Host: Select one of the following methods for specifying a server to host the file share:

      - **Use a script to select a server**: This option is selected by default and the system selects a random server based on the QAM_RandomNode script. Click **Change** to display a list of server selection scripts that can be run to select a different server.

- In the **Sever Selection Scripts** dialog, locate the script to be run and click **Run Script**.

- Once the script has completed, the **Result** column displays the servers that meet the criteria defined in the script. Select a server from this list and click **Close**.

  NOTE: To add server selection scripts to your Data Governance Edition deployment, use the Object Browser (QAMServerSelectionScript) or Windows PowerShell (Add-QServerSelectionScript). For more information, see Server selection scripts on page 60.

- **Manually specify the server**: To manually select a server, select this option and click **Assign** or **Change** to display a list of managed hosts that are flagged as managed resource hosts.

  - In the **Managed host** dialog, select a managed host from the list and click **Close**.

  NOTE: For DFS managed hosts, if the DFS namespace is not listed, ensure that both the DFS server hosting the DFS namespace and the share server where the DFS link is pointing to have been added as managed hosts. Also, check to ensure that your DFS managed host is flagged as a managed resource host (has the **IsManagedResourceHost** property set to **True**).

  The selected server appears on the **File Share** page. To change your selection, select the option to be used to select the server and click **Change**.

d. Root Path: Select a root path under the specified server where the new file share is to be created.

  - Select one of the following options:

    - **Select a non-DFS path**

    - **Select a DFS root path**

      NOTE: If there are no DFS root paths shown in the **Browse** dialog, check that the QAMDfsTarget table is populated with your DFS paths.

  - **Choose a root path for the new file share**: Click **Assign** to display a list of managed share root paths.

    - In the **Managed Share Root Path** dialog, select a root path and click **Close**.

    NOTE: To add or modify share root paths, use the Object Browser (QAMManagedShareRootPaths) or Windows PowerShell (Add-QManagedShareRootPath). For more information, see Creating and specifying share root paths on page 40.

  The selected root path appears on the **File Share** page. To change your selection, click **Change**.

6. (Optional) On the **Permissions** page, specify the naming pattern to be used to build the new groups.

NOTE: Click the expansion arrow to the left of the Domain Local group to view the nested Global group.

    a. Click **Edit** to the right of a group.

    b. In the **Group Name** dialog, add literal values and variables to define the group naming pattern to be used to create the new Active Directory group.

       NOTE: See Group naming patterns on page 58 for more details on defining a group naming pattern and the variables available for use.

    c. Click **OK** to save your selection and close the dialog. The new pattern appears in the **Pattern to dynamically build group name with** column.

7. Click **Close** to save your selections and close the dialog.

8. Click the ☑**Approve** button in the **Decision** column, then click **Next**.

The **Approvals** view appears allowing you to review your decision and enter additional details about your approval decision.

9. (Optional) On the **Approvals** view, enter the following details regarding your decision:

    a. Reason for approval: Enter a reason for approving the requests. This reason applies to all approved requests listed, unless there is an individual reason given in the **Reason** column of an approval.

    b. Standard reason: Select a standard reason from a list of previously defined reasons.

       NOTE: For more information about defining standard reasons, see the *One Identity Manager IT Shop Administration Guide*.

    c. Valid from: This is set to **immediately** and cannot be changed.

    d. Valid until: Does not apply to this type of request. This is set to **unlimited** and changing the end date has no effect on the request.

    e. Reason: Click **Enter a reason** to specify a reason for your decision that is specific to the selected request.

10. Click **Save approvals**.

Once you make an approval decision, the request disappears from your list of pending requests. To view your approval decisions, select **Request | My Actions | Approval History**. Selecting this tile displays the Approval History view.

Once the file share is created, an email is sent to the requestor with the location and name of the new share.

Processing requests for file system share creation

When an identity requests that a new file system share be created through the IT Shop, the request follows a defined approval process that determines whether the share is created.

Default request workflow

1. An identity uses the web portal IT Shop to make a request for creating a new file system share.

2. If the identity has a manager assigned, the identity's manager decides if the identity's request should be granted.

3. The request is then forwarded to the Data Governance Administrator who specifies the server to host the new share, the root host and the groups created to provide access to the share.

4. When a self-service share creation request is successfully processed and approved, the default configuration for creating a file share and granting access through group membership is performed, which includes:

   - Six groups, three Global groups and three Domain Local groups, are created specially for accessing the share. The Global groups are nested within the Domain Local groups, following Microsoft best practices.

     - Domain Local group with Full Control permissions

       - Global group with Full Control permissions

     - Domain Local group with Read permissions

       - Global group with Read permissions

     - Domain Local group with Read/Write permissions

       - Global group with Read/Write permissions

   - User accounts are added into the appropriate Global groups.

   - The share path is created.

   - The file share is created on a Windows server.

   - The ACLs are set appropriately on the share.

5. If specified as part of the request, the share is published to the IT Shop making it available to other identities.

6. An email is sent to the requestor with a link to the newly created file share.

7. If a request is denied, it falls back to the requestor to make another request.

Figure 2: QAM Create DGE Managed Resource process chain
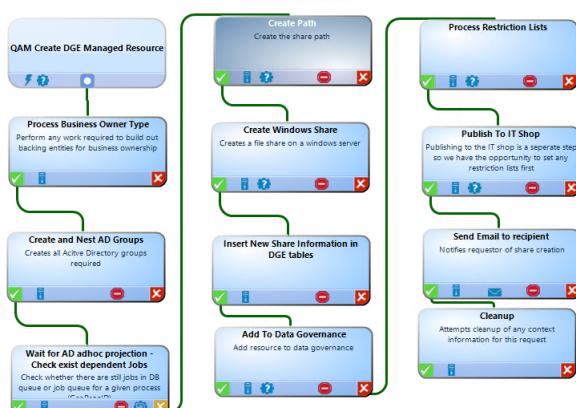
Troubleshooting share creation requests

The following topics explain possible causes and resolutions to the following issues/questions you may encounter when working with self-service share creation requests:

- Error logging

- Access denied error

Error logging

When an error is encountered with a self-service file share creation request, review the following logs:

Job Server logs

Errors encountered with the process chain used to process file share creation requests 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. The default URL for a Job Server log is: http://JobServerHost:1880/Log.

Web Client log

Errors encountered with the web client IT Shop are recorded to the 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 timestamp. The best way to get the proper one is to replicate the issue and take the file with the most recent timestamp.

Data Governance Service log

Errors encountered using the Windows PowerShell cmdlets are recorded to the Data Governance Service Log.txt, which is located in the program folder: %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server.

Access denied error

Access is denied to the new share, even though an email was received stating that the file share requested has been successfully created.

Cause

When configuring the IT Shop, the RecipientAddToGroup property in the QAMManagedResourceType table for the Simple Share managed resource type was not properly set.

That is, if you used the Object Browser and omitted to set the UID_ RecipientAddToGroup (or used the Add-QManagedResourceType PowerShell cmdlet and omitted the -RecipientAddToGroup parameter), the recipient is not added to the appropriate group when it is created and therefore, is denied access to the new file share.

Resolution

Use the IT Shop to request access to the new file share. This will set the property that was originally missing. Log out of the current session and log back in to ensure the change takes effect.

Customizing share creation requests

NOTE: The Resource Access shelf is available through the Identity & Access Lifecycle shop, which is included by default with the One Identity Manager installation. The File system access, SharePoint access and New file system share products are available in the Resource Access shelf by default. In the default installation, several approval policies are assigned to the Identity & Access Lifecycle shop; therefore, requests from this shop are run through predefined approval processes.

You can use the shop to request standard products or you can extend it by adding additional shelves, assigning requestable products, or by setting up your own IT Shop solution. You can also customize the approval processes, including approval policies and approval workflows. For more information on using and customizing the Identity & Access Lifecycle shop, see the *One Identity Manager IT Shop Administration Guide*.

The default configuration and process fulfills self-service share creation requests by creating new file system shares and granting access through group membership based on Microsoft best practices. This release of Data Governance Edition handles the basic fundamentals for creating file system shares which can be modified to meet your file system share creation needs. In addition, you can use the basic configuration provided as a basis for defining additional managed resource types and corresponding processes to fulfill self-service requests to these new managed resources.

Prior to modifying the default configuration for share creation requests or creating new managed resource types, it is very important that you understand the security model currently being used for self-service share creation requests:

- The security model: The default security model defines the groups to be created, parent-child relationships, permissions, and so on for creating new file system shares. The default security model can be modified for self-service share creation

requests or can be used as a basis for defining your own security model for creating additional managed resource types.

Once you fully understand how the security model works, these components can be customized in addition to the security model:

- Group naming patterns: Group naming patterns consist of literal values and variables that are used to dynamically construct a new Active Directory group name. A group naming pattern is specified when building new managed group templates to define the default naming pattern to be used to create new Active Directory groups. Also, as part of the approval process, the Data Governance Administrator can edit the group naming pattern to ensure the groups created by the share creation request are named according to company standards.

- Name pattern resolvers: In addition to allowing you to edit the group naming pattern to be used, you can also create your own name pattern resolver scripts to define additional variables that can then be used in the group naming patterns. Data Governance Edition provides sample name pattern resolver scripts that can be used as a basis for defining your own name pattern resolver scripts.

- Server selection scripts: Data Governance Edition provides a default server selection script that randomly selects a managed host (QAMNode) to host a new file system share. You can, however, write your own server selection scripts to ensure the appropriate managed host is suggested.

- Mail templates: Data Governance Edition provides default email templates that can be modified to meet your company email standards. For information on modifying mail templates, see the *One Identity Manager Configuration Guide*.

- Managed resource functions: Data Governance Edition provides One Identity Manager scripts that can be indirectly invoked to satisfy a predefined extension point in the business logic defined within the managed resource process chain. These scripts allow you to modify the behavior of the function defined in a script instead of modifying or creating the actual process chain used to process and fulfill self-service requests to managed resources.

- Process chain (file system share creation): The share creation request and approval workflows are defined using a specific process chain, similar to other One Identity Manager processes. If necessary, this process can be modified by adding or removing steps in the default chain. In addition, if you create additional managed resource types, you can use this process chain as a basis for defining the process chain to be used to process and fulfill self-service requests to these managed resources. For more detailed information on modifying process chains, see the *One Identity Manager Configuration Guide.*

NOTE: When the Data Governance service first starts up, it writes the default managed resource data into the One Identity Manager database. This behavior is controlled by a registry key, HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Broadway\Server\ResourceTemplateDefaultData.

If you delete the default managed resource components in your Data Governance Edition deployment and replace them with new managed resource components, 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 managed resource data.

If you modify the default managed resource components 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*.

The security model

The default security model defines how and where new file system shares are created, including the Active Directory container where new shares are created, the Active Directory group hierarchy to be used to support ACLs for the new share, the resource type to be created (Simple Share in this release), and the permissions assigned to the Active Directory groups. Therefore, when customizing the security model used to process share creation requests, you must first understand the following objects:

- Managed resource type domain object: As part of the set up process, in each managed domain, you specified the Active Directory container where new groups are to be created and the group to be given full administrative control to the share. For more information, see Updating managed resource type domain object with full-control group and Active Directory container on page 38.

- Managed group templates: Managed group templates define how a hierarchy of Active Directory groups is to be created to support a managed resource (file share). In addition to the hierarchy, these templates define the default group naming pattern to be used to create new Active Directory groups and the type of group to be created. Data Governance Edition uses Microsoft best practices for creating and nesting groups to provide access to newly created file shares; however, you can build your own templates to define this group hierarchy and the group naming pattern to be used. For more information, see Managed group templates on page 55.

- Managed resource types: A managed resource type contains settings that provide a logical distinction that can be used to refine the concept of "file share" into different business specific groupings. More specifically, it points to the managed group templates used to create the groups to be used to grant access and specifies the default server selection script to determine an eligible server to create the file share on. For more information, see Managed resource types on page 57.

  NOTE: The current managed resource type, Simple Share, uses the default configuration and process chain to create file system shares. Therefore, if you add a new managed resource type, you will be required to implement your own IT Shop product and process chain to support that managed resource type.

- Type group permissions object: The last piece of the security model is linking the proper permissions object to the managed resource template for a managed resource type. Data Governance Edition provides default type group permissions objects to support the default managed group templates and Simple Share managed resource type provided. You can, however, create your own type group permissions objects to correlate possible permissions and group hierarchies in your deployment. For more information, see Type group permissions objects on page 58.

Managed group templates

Building the managed group templates to be used to define the Active Directory group hierarchy and default group naming pattern is the first step in customizing the security model to be used for creating managed resources.

By default, Data Governance Edition uses Microsoft best practices for creating and nesting groups to support ACLs for file system shares. By default six groups, three Global groups and three Domain Local groups, are created specially for accessing a new share. The Global groups are nested within the Domain Local groups as defined by the following managed group templates, which are available in the QAMManagedGroupTemplate table in One Identity Manager:

- G-[costcenter]-[random]-FC
- G-[costcenter]-[random]-R
- G-[costcenter]-[random]-RW
- L-[costcenter]-[random]-FC
- L-[costcenter]-[random]-R
- L-[costcenter]-[random]-RW

In addition, by default the Global Read group (created based on the G-[costcenter]-[random]-R template) and Global Read Write group (created based on the G-[costcenter]-[random]-RW template) have the IsSelfServiceGroup flag set to $true. Therefore, these groups will be the only groups returned after Data Governance Edition runs the group membership calculation to determine the "best fit" groups that would provide the requested access to the managed resource.

Before you begin:

- For each managed domain, specify the Active Directory container where new groups are to be created and the group to be given full administrative control to the share for each managed resource type. For more information, see Updating managed resource type domain object with full-control group and Active Directory container on page 38.

- Define any additional name pattern resolvers required to properly name your Active Directory groups. For more information, see Name pattern resolvers on page 60.

- Define your Active Directory group hierarchy, so that you can build the groups top to bottom.

  NOTE: If the default group hierarchy works for your environment, but you want to use different group types or naming patterns, you can edit the existing managed group templates instead of building new ones. To modify an existing managed group template, use the Object Browser (QAMManagedGroupTemplate) or Windows PowerShell (Set-QManagedGroupTemplate).

To build a managed group template (Object Browser)

1. Open the Object Browser.

2. In the Navigation view, locate and select **QAMManagedGroupTemplate**.

3. In the **Managed Group Templates** result list pane, click the **Insert** toolbar button or right-click command.

4. In the new **Managed Group Template** page, specify the following:

   - UID_ParentGroup Template: Use the drop-down menu to specify the template of the parent group this group is to be nested under when it is created.

     NOTE: If this is a top-level (parent) group, do not specify this parameter.

   - Description: (Optional) Enter a brief description for the group.

   - GroupNamingPattern: Enter the group naming pattern to be used when creating the group.

   - GroupType: Use the drop-down menu to select the type of group to be created: Domain Local (default), Global or Universal.

   - IsSelfServiceGroup: Change this value to **True** if this group is to be available for self-service access requests in the IT Shop. That is, limit the "best fit" calculation to only include groups that have this flag set to $true.

   NOTE: UID_QAMManagedGroupTemplate: This value is automatically generated by One Identity Manager.

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

   The newly created managed group template appears in the **Managed Group Templates** result list pane.

To build a managed group template (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 add a new managed group template:

   Add-QManagedGroupTemplate -GroupNamingPattern <String> [-Description[[<String>]] [-GroupType] [-Int32>]] [-ParentGroupTemplateID] [<String>]] [-IsSelfServiceGroup [<Boolean>]]

   - GroupNamingPattern: Enter the group naming pattern to be used when creating the group.

   - Description: (Optional) Enter a description for the group.

   - GroupType: Specify the type of group to be created based on this template:

     - 0: Domain Local group (Default)

     - 1: Global group

- 2: Universal group
  - ParentGroupTemplateID: Enter the ID of the parent group template for the parent group this group is to be nested under when it is created.

    | NOTE: If this is a top-level (parent) group, do not include this parameter.
  - IsSelfServiceGroup: (Optional) Specify whether the group defined in the template is to be published to the IT Shop. That is, limit the "best fit" calculation to only include groups that have this flag set to $true.

For more information, see Group template management on page 87.

Next step:

- If using a new managed resource type, define the managed resource type. For more information, see Managed resource types on page 57.
- If using the Simple Share managed resource type, assign type group permissions object. For more information, see Type group permissions objects on page 58.

Managed resource types

A managed resource type contains various default settings for a type, which is a logical distinction that can be used to refine the concept of a "file share" into different business specific groupings.

By default, a single managed resource type, Simple Share, is provided with Data Governance Edition. The settings for the Simple Share managed resource type can be found in the QAMManagedResourceType table in One Identity Manager. Take note of the following settings:

- Default server selection script: This setting specifies the default server selection script to be used to determine an eligible server to create the new file share on. Default value: QAM-492C2929FD77ED478EA6BA3EB40774C2

  NOTE: If this parameter is not specified, no script is run and during the approval process, the Data Governance Administrator must manually select a target managed host.
- Full control add to group: This setting points to the managed group template being used to create the Active Directory group where the full control group is to be added to provide administrative access to a new share when it is created. Default value: G-[costcenter]-[random]-FC

  NOTE: If this parameter is not specified, the specified full control group is not added to the Active Directory group that provides administrative control for the new file share when it is created.
- Recipient add to group: This setting points to the managed group template being used to create the Active Directory group where the recipient will be added to provide access to a new share when it is created. Default value: G-[costcenter]-[random]-RW

NOTE: If this parameter is not specified, the recipient will not be added to the group when it is created and will be denied access to the newly created file share. The recipient can use the IT Shop to request access to the new file share, which will also set this value.

NOTE: If you are using the Simple Share managed resource type and need to modify the default settings, use the Object Browser (QAMManagedResourceType) or Windows PowerShell (Set-QManagedResourceType).

The "Simple Share" managed resource type is used in a pre-generation step in the current process chain. Therefore, it is recommended that you do not rename or remove this managed resource type. If you change the name of this managed resource type, you need to modify the process chain, either removing or modifying this pre-generation check step as appropriate.

NOTE: If you are adding a new managed resource type, you must implement your own IT Shop product and process chain. The current configuration and process chain are intended for creating new file shares.

Type group permissions objects

Once you have built your group hierarchies (managed group templates) and defined your managed resource types (Simple Share in default configuration), you must link the required permissions object to define the root level group for creating a managed resource.

By default, Data Governance Edition has defined the following group permission objects, which are available in the QAMTypeGroupPermissions table in One Identity Manager:

- L-[costcenter]-[random]-FC - Simple Share
- L-[costcenter]-[random]-R - Simple Share
- L-[costcenter]-[random]-RW - Simple Share

Group naming patterns

Since organizations have different rules for naming groups, Data Governance Edition allows you to add literal values and variables to the group naming pattern to dynamically construct a new Active Directory group name. Upon creation of the actual group, any variable specified in the pattern is then replaced with actual values to create a unique group name. The default group naming patterns are specified in the Managed group templates used to define the Active Directory groups to be created to fulfill self-service share creation requests. In addition, as part of the approval process, the Data Governance Administrator can edit the group naming pattern for the Active Directory groups to be created.

The default group name patterns provided with Data Governance Edition are:

- Domain Local group (Full Control): L-[costcenter]-[random]-FC
- Global group (Full Control): G-[costcenter]-[random]-FC
- Domain Local group (Read): L-[costcenter]-[random]-R
- Global group (Read): G-[costcenter]-[random]-R
- Domain Local group (Read/Write): L-[costcenter]-[random]-RW
- Global group (Read/Write): G-[costcenter]-[random]-RW

The following variables have been defined allowing you to define a group naming pattern to dynamically construct a new Active Directory group name.

Table 2: Group name pattern variables

Variable	Description
[costcenter]	Sample name pattern resolver that retrieves the short name of the cost center associated with the identity who made the request.
	If the requestor does not have a cost center assigned, this variable resolves to a blank.
[dept]	Sample name pattern resolver that retrieves the short name of the department associated with the identity who made the request.
	If the requestor does not have a department assigned, this variable resolves to a blank.
[random]	Sample name pattern resolver that generates a random number, between 1 and 999999.
[ShareName]	A variable that retrieves the name assigned to the file share.

NOTE: To add additional group name pattern resolvers, use the Object Browser (QAMNamePatternResolver) or Windows PowerShell (Add-QNamePatternResolver). For more information, see Name pattern resolvers on page 60. For more information on adding and testing scripts, see the *One Identity Manager Configuration Guide*.

To add a variable to a group naming pattern during the approval process:

1. On the **Permissions** page of the **New File Share** dialog, click **Edit** to the right of the group name to be changed.

2. In the **Group Name** dialog, use the **Group name pattern** field to construct your naming pattern, which can consist of literal values and variables.

   NOTE: Variables are enclosed in square brackets [ ] in the **Group name pattern** field. If you enter a variable that does not exist as a name pattern resolver, it will show as a literal in your group name.

3. To add a variable, place your cursor within the naming pattern where the variable is to be inserted and enter the variable enclosed in square brackets (for example, [dept]).

NOTE: Clicking a variable in the Macro list appends the selected variable to the end of the group naming pattern, regardless of where your cursor is located in the string.

4. Once you have constructed the naming pattern, click the **Resolve** button to view the unique Active Directory group name created.

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

   Both the group naming pattern and the resolved group name appear on the **Permissions** page of the **New File Share** dialog.

Name pattern resolvers

Data Governance Edition allows you to define your own name pattern resolver scripts, which define the variables that can be added to a group naming pattern. These variables can then be used when building or modifying managed group templates. In addition, during the approval process, available variables are listed on the **Group Name** dialog when editing the group naming pattern to dynamically construct unique Active Directory group names for the new managed resource.

By default, the following sample name pattern resolver scripts are provided with Data Governance Edition and are available in the QAMNamePatternResolver table:

- costcenter
- dept
- random

Server selection scripts

Defining where new resources get created can be very complicated and specific to your organization. The Data Governance server allows you to select a managed host or use a server selection script to select the QAMNode to host a new file system share. Creating customized server selection scripts allows you to define the server selection process to be used for selecting the appropriate QAMNode. Available server selection scripts appear on the **Server Selection Scripts** dialog when the Data Governance Administrator selects to assign a file share host using the script option on the **File Share** page of the **New File Share** dialog.

By default, Data Governance Edition provides the following server selection script, which is available in the QAMServerSelectionScript table in One Identity Manager:

- QAM_RandomNode: Randomly selects a managed host from those that have been specified as target machines (that is, managed hosts that have the **IsManagedResourceHost** flag set to **True**).

Managed resource functions

A managed resource function is a One Identity Manager script that can be invoked indirectly by some arbitrary name to satisfy a pre-defined extension point in the business logic. Data Governance Edition provides sample managed resource function records that contain the necessary mappings to perform the following functions which are used in the default process chain (QAM Create DGE Managed Resource) to fulfill self-service requests to managed resources:

- Locate a job server that can process new shares and file paths when creating a new managed resource.
- Locate the Active Directory container ID to be used when creating the new managed resource groups.
- Set a restriction list for managed resource creation.

You can override the default functionality, by mapping a custom script to a predefined managed resource function record. However, each custom script must match the function signature and return the expected object. By doing this, you eliminate the need to modify the existing process chain. If you create a new managed resource function, you are required to create a custom process chain to call the custom managed resource function record.

Before you begin

- If you are writing a custom script, use the Designer to write and compile the managed resource function script and commit it to the One Identity Manager database.

  NOTE: Managed resource function scripts must have a particular signature or they will fail at run time. These scripts are functions that take one parameter, the UID of the PersonWantsOrg record for this request, as a string and returns an object or null. The type of object returned varies based upon the expectations of the consuming code. It is highly recommended that you look at the sample implementations to see what is expected from the script.

  Currently all data needed to rune the function must be resolvable directly or indirectly using the PersonWantsOrg record specified.

Table 3: Supported managed resource functions

Script name	Signature	Returns	Description
LocateFileOperationsJobServer	`Public Function Func(ByVal UID_PWO As String) As String`	The UID_ QBMServer value identifying an appropriate entry in the QBMServer	Processor for locating a job server that can process new shares

Script name	Signature	Returns	Description
		table.	and file paths when creating a new managed resource.
ResolveADContainer	`Public Function Func(ByVal UID_PWO As String) As String`	The UID_ ADSContainer value identifying an appropriate entry in the ADSContainer table.	Processor for locating an Active Directory container ID to be used when creating the new managed resource groups.
SetRestrictionList	`Public Sub X (ByVal UID_ PWO As String)`	N/A	Subroutine used to set a restriction list for managed resource creation.

To point an existing managed resource function record to a custom script (Object Browser)

The ManagedResourceFunction table contains a mapping between the function name and the script to be run. By overriding the functionality in this manner you do not need to modify the process chain.

1. Open the Object Browser.

2. In the Navigation view, locate and select **QAMManagedResourceFunction**.

3. From the **Managed Resource Function** result list, select the managed resource function record to be mapped to the new script. For example, select **Simple Share – SetRestrictionList**.

4. In the **Managed Resource Function** page (right pane), specify the following:

   - UID_DialogScript: Use the drop-down menu to select your custom script.

   - UID_QAMManagedResourceType: Do not modify this setting. The function name is unique by ManagedResourceType.

   - Description: (Optional) Enter a new description for the managed resource function record.

   - Name: Do not modify this setting.

NOTE: UID_QAMManagedResourceFunction: This value is automatically generated by One Identity Manager and cannot be modified.

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

To point an existing managed resource function record to a custom script (PowerShell)

1. If necessary, run the following cmdlet to 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 map a custom script:

   Set-QManagedResourceFunction -Id <String> [-Description [<String>]] - DialogScriptID <String>

   - Id: Enter the value (GUID) assigned to the managed resource function (UID_ QAMManagedResourceFunction) to be changed.

   - Description: (Optional) Enter a different description.

   - DialogScriptID: Enter the ID (GUID) assigned to the custom script when it was created in One Identity Manager.

For more information, see Managed resource function management on page 109.

ONE IDENTITY
by Quest

Process chain (file system share creation)

One Identity Manager uses process steps (also known as process chains) to represent company workflows. A default process chain is provided to fulfill self-service share creation requests; however, if the workflow defined in the default process does not meet your company's procedures, you can use the Process Editor in the Designer to create a new process or modify the default process chains. In order to fulfill self-service share creation requests, the following process chain is provided:

- QAM Create DGE Managed Resource: Defines the process steps for validating the creation parameters, and creating the groups and file share once the request has been approved.

To modify the file share creation process chain

1. Use the Process Editor to copy the default process.

   a. From the navigation pane, select **Process Orchestration** and expand **Processes** to locate target process.

      - **PersonWantsOrg | QAM Create DGE Managed Resource**

   b. Right-click and select **Navigation | Process Editor | Edit process** or click the **Edit process** task in the far right pane.

      The current process is loaded and displayed in the process editor.

2. Use the **Process | Copy** menu command to make a copy of the original process chain.

   The Copy process wizard appears. Ensure the following copy options are selected on the first page:

   - Rename process steps
   - Copy events
   - Disable source process

   Enter the requested information (for example, name of the new process and names for the process steps).

3. Modify the process chain as required and save your selections.

For more information on modifying process chains, see the *One Identity Manager Configuration Guide*.

PowerShell commands

Data Governance Edition provides Windows PowerShell cmdlets to manually manage resources used in the file system share creation feature.

- Adding the PowerShell snap-ins
- Self-service request information
- Managed resource information
- Managed resource type management
- Managed resource type domain object management
- Group template management
- Name pattern resolver management
- Server selection script management
- Share root path management
- Type group permissions object management
- Managed resource function management

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`

Self-service request information

These PowerShell commands allow you to view information about the self-service request configuration.

For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 4: Self-service request information commands

Use this command	If you want to
Get-QSelfServiceClientConfiguration	View the options available for self-service requests within the IT Shop.
Set-QSelfServiceClientConfiguration	Set the options available for self-service requests within the IT Shop.
Get-QSelfServiceMethodsToSatisfyRequest	View the group membership that is required to satisfy an access request.

Get-QSelfServiceClientConfiguration

Returns the options available for self-service requests within the IT Shop.

Syntax:

Get-QSelfServiceClientConfiguration [<CommonParameters>]

Examples:

Table 5: Examples

Example	Description
Get-QSelfServiceClientConfiguration	Returns the self-service client configuration information.

Details retrieved:

Table 6: Details retrieved

Detail	Description
AllowNonPublishedGroups	Indicates whether groups that have not been published to the IT Shop are allowed for self-service access requests.
AllowUnsynchronizedGroups	Indicates whether groups that have not been synchronized with One Identity Manager are allowed for self-service access requests.
MaximumMethodsCount	The maximum number of groups returned from a call to the Get-QSelfServiceMethodsToSatisfyRequest, which returns the groups that satisfy a resource access request.

Detail	Description
EnableSelfServiceAccessRequest	Indicates whether self-service access requests are enabled in the IT Shop.

Set-QSelfServiceClientConfiguration

Sets the options available for self-service requests within the IT Shop.

Syntax:

Set-QSelfServiceClientConfiguration [-MaximumMethodsCount] <Int32> [-EnableSelfServiceAccessRequest] <Boolean> [-AllowNonPublishedGroups] <Boolean> [-AllowUnsynchronizedGroups] <Boolean> [<CommonParameters>]

Table 7: Parameters

Parameter	Description
MaximumMethodsCount	Specify the maximum number of groups that are to be returned from a call to the GetMethodsToSatisfyRequest.
EnableSelfServiceAccessRequest	Specify whether self-service access requests are to be enabled in the IT Shop. Valid values are: • 0: Disable self-service access requests • 1: Enable self-service access requests
AllowNonPublishedGroups	Specify whether groups that have not been published to the IT Shop are to be included in self-service access requests. Valid values are: • 0: Unpublished groups will not be available for self-service access requests in the IT Shop. • 1: Unpublished groups will be available for self-service access requests in the IT Shop.
AllowUnsynchronizedGroups	Specify whether groups that have not been synchronized with One Identity Manager are to be included in self-service requests. Valid values are: • 0: Unsynchronized groups will not be available for self-service access requests in the IT Shop.

Parameter	Description
	• 1: Unsynchronized groups will be available for self-service access requests in the IT Shop.

Examples:

Table 8: Examples

Example	Description
Set-QSelfServiceClientConfiguration -MaximumMethodsCount 1 -EnableSelfServiceAccessRequest 1 -AllowNonPublishedGroups 1 -AllowUnsynchronizedGroups 1	Sets the self-service client configuration information: • Enabling self-service access requests • Making unpublished groups available for self-service access requests in the IT Shop • Making unsynchronized groups available for self-service access requests in the IT Shop

Get-QSelfServiceMethodsToSatisfyRequest

Returns the group membership that satisfies a resource access request. Use this command to simulate the "best fit" calculation to see what groups are returned if you request read or read and write access to a specific resource.

NOTE: This PowerShell cmdlet does not support NFS or Cloud resources (since these types of resources cannot be published to the IT Shop).

Syntax:

Get-QSelfServiceMethodsToSatisfyRequest [-Path] <String> [-DomainName] <String> [-ActionIdentifier] <String> [[-ClientCulture] [<String>]] [[-ResourceTypeString] [<String>]] [<CommonParameters>]

Table 9: Parameters

Parameter	Description
Path	Specify the path of the resource.
DomainName	Specify the name of the domain where the resource is located.
ActionIdentifier	Specify the type of self-service action: • RequestReadAccess: Use this option if you want read

Parameter	Description
	access to items within a folder.
	• RequestChangeAccess: Use this option if you want read and write access to items within a folder.
ClientCulture	(Optional) Set the client culture.
ResourceTypeString	(Optional) Specify the type of resource for which to request access:
	• NTFS\Folder
	• NTFS\File
	• Windows\Computer\Share
	• SharePoint\Site
	• SharePoint\Folder
	• SharePoint\List
	• SharePoint\ListItem
	• SharePoint\ResourceItem

Examples:

Table 10: Examples

Example	Description
Get-QSelfServiceMethodsToSatisfyRequest -Path "\\2K8RDJSQL\CS\Test Data\Email_ Addresses.txt" -DomainName VMSET6 - ActionIdentifier "RequestReadAccess" - ResourceTypeString NTFS\File	Returns the groups that satisfy the "RequestReadAccess" request for a NTFS/File.

Managed resource information

These commands are available to retrieve the following information about a managed resource.

- Managed group: A managed group is an Active Directory group created by the Data Governance Edition deployment in order to control access to a managed resource, such as a file share.

- Managed resource: A managed resource is a type of resource, such as a file share, that was created by the Data Governance deployment.

- Managed resource/DuG mapping: A managed resource/DuG mapping object correlates a managed resource to any QAMDuG object it links to.

For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 11: Managed resource information commands

Use this command	If you want to
Get-QManagedGroup	Retrieve a managed group from the Data Governance Edition deployment. You can retrieve a specific managed group or a list of all managed groups in the database.
Get-QManagedResource	Retrieve a managed resource from the Data Governance Edition deployment. You can retrieve a specific managed resource or a list of all managed resources in the database.
Get-QManagedRe-sourceDuG	Retrieve a managed resource/DuG mapping object from the Data Governance Edition deployment. You can retrieve a specific managed resource/DuG mapping object or a list of all managed resource/DuG mapping objects in the database.

Get-QManagedGroup

Retrieves details about a managed group from the Data Governance Edition deployment.

Syntax:

Get-QManagedGroup [-Id [<String>]] [<CommonParameters>]

Table 12: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of the managed group to be retrieved. If this parameter is not specified, all managed groups in the database are returned.

Examples:

Table 13: Examples

Example	Description
Get-QManagedGroup	Returns all managed groups in the database.
Get-QManagedGroup -Id fe59f287-8177-46e8-9cae-71b3b455ee3e	Returns information on the specified managed group.

Details retrieved:

Table 14: Details retrieved

Detail	Description (Associated key or property in QAMManagedGroup table)
GroupName	The name assigned to the group when it was created (OriginalGroupName).
ADSGroupID	The value (GUID) assigned to the ADS group (UID_ADSGroup).
ManagedGroupTemplateID	The value (GUID) assigned to the managed group template (UID_QAMManagedGroupTemplate).
ManagedResourceID	The value (GUID) assigned to the managed resource (UID_QAMManagedResource).
Id	The value (GUID) assigned to the managed group (UID_QAMManagedGroup).

Get-QManagedResource

Retrieves details about a managed resource that was created by Data Governance Edition.

Syntax:

Get-QManagedResource [-Id [<String>]] [<CommonParameters>]

Table 15: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of the managed resource to be retrieved. If this parameter is not specified, all managed resources in the database are returned.

Examples:

Table 16: Examples

Example	Description
Get-QManagedResource	Returns a list of all managed resources in the database.
Get-QManagedResource -Id c0bc3da4-f660-4e18-8b14-a945c7a6be69	Returns information on the specified managed resource.

Details retrieved:

Table 17: Details retrieved

Detail	Description (Associated key or parameter in QAMManagedResource table)
Name	The name assigned to the managed resource (Name).
BusinessOwnerIDObjectKey	The value assigned to the business owner (ObjectKeyBusinessOwner).
ManagedResourceTypeID	The value (GUID) assigned to the managed resource type (UID_QAMManagedResourceType).
QAMNodeID	The value (GUID) assigned to the QAMNode (UID_QAMNode).
Id	The value (GUID) assigned to the managed resource (UID_QAMManagedResource).

Get-QManagedResourceDuG

Retrieves details about a managed resource/DuG mapping from the Data Governance Edition deployment.

Syntax:

Get-QManagedResourceDuG [-ManagedResourceId [<String>]] [-QAMDuGId [String]] [<CommonParameters>]

Table 18: Parameters

Parameter	Description
ManagedResourceId	(Optional) Specify the ID (GUID format) of the managed resource to be retrieved.

Parameter	Description
	If no parameters are specified, all managed resource/DuG mapping objects are returned.
	NOTE: If this parameter is included, the QAMDuGId parameter must also be specified; otherwise, all objects are returned.
QAMDuGId	(Optional) Specify the ID (GUID format) of the QAM DuG object to be retrieved.
	If no parameters are specified, all managed resource/DuG mapping objects are returned.
	NOTE: If this parameter is included, the ManagedResourceId must also be specified; otherwise, all objects are returned.

Examples:

Table 19: Examples

Example	Description
Get-QManagedResourceDuG	Returns a list of all managed resource/DuG mapping objects in the database.
Get-QManagedResourceDuG -ManagedResourceId c0bc3da4-f660-4e18-8b14-a945c7a6be69 -QAMDuGId db9d52d9-8ef1-44b4-8941-47bd5223388c	Returns the mapping information for the specified managed resource and QAM DuG object.

Details retrieved:

Table 20: Details retrieved

Detail	Description (Associated key in QAMManagedResourceDuG table)
ManagedResourceID	The value (GUID) assigned to the managed resource (UID_QAMManagedResource).
QAMDuGID	The value (GUID) assigned to the governed data (UID_QAMDuG).

Managed resource type management

A managed resource type contains various default settings for a type, which is a logical distinction that can be used to refine the concept of a "file share" into different business specific groupings.

The following commands are available to manage your resource types, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 21: Managed resource type management commands

Use this command	If you want to
Add-QManagedRe-sourceType	Add a managed resource type to the Data Governance deployment.
Get-QManagedRe-sourceType	Retrieve a managed resource type from the Data Governance Edition deployment. You can retrieve a specific managed resource type or a list of all managed resource types in the database.
Remove-QManagedRe-sourceType	Remove a managed resource type from the Data Governance Edition deployment.
Set-QManagedRe-sourceType	Update an existing managed resource type in the Data Governance Edition deployment.

Add-QManagedResourceType

Adds a managed resource type to the Data Governance Edition deployment.

A managed resource type contains settings that provide a logical distinction that can be used to refine the concept of "file share" into different business specific groupings. The default managed resource type available is "Simple Share".

NOTE: The current managed resource type, Simple Share, uses the default configuration and process chain to create file system shares. Therefore, if you add a new managed resource type, you will be required to implement your own IT Shop product and process chain to support that managed resource type.

Syntax:

Add-QManagedResourceType -Name <String> [-Description [<String>]] [-FullControlAddToGroupID [<String>]] [-RecipientAddToGroupID [<String>]] [-PublishToITShop <Boolean>]] [-SetRestrictionList [<Boolean>]] [-ServerSelectionScriptID [<String>]] [-ContainerAERole [<String>]] [-BusinessOwnerType [<Int32>]] [<CommonParameters>]

Table 22: Parameters

Parameter	Description
Name	Specify the name of the managed resource type.
Description	(Optional) Specify a description for the managed resource

Parameter	Description
	type.
FullControlAddToGroupID	Specify the ID (GUID format) of the managed group template being used to build the domain-specific full control group for this managed resource type.
	If this parameter is not specified, the full control group specified by the Managed resource type domain object (UID_FullControlGroup) for this resource type will not be added when the resource (file share) is created.
RecipientAddToGroupID	Specify the ID (GUID format) of the managed group template being used to build the group where the recipient is to be added.
	If this parameter is not specified, the recipient will not be added to the group when it is created and will be denied access to the newly created file share. The recipient can use the IT Shop to request access to the new file share, which will also set this value.
PublishToITShop	(Optional) Specify whether a managed resource associated with this resource type should be published to the IT Shop after it is created. $true (Default) $false If this parameter is not specified, the default value of true is used and any managed resource associated with this resource type will be published to the IT Shop after it is created.
SetRestrictionList	(Optional). Indicates if the managed resource associated with this resource type should have automatically have a restriction list set when the resource is created. $true: Run the SetRestrictionList subroutine to set a restriction list for this resource type. By default, the SetRestrictionList subroutine creates a restriction list based on the department, location and cost center properties defined in the requester's Identity record. $false: (Default) No restriction list applies to this resource type.
ServerSelectionScriptID	(Optional) Specify the default server selection script to be run to determine an eligible server to create the share on.
	If this parameter is not specified, no server selection script is run. During the approval process, the Data Governance

Parameter	Description
	Administrator must manually select the managed host server to be used to host the managed resource.
	Run the Get-QServerSelectionScript cmdlet to retrieve a list of available server selection scripts, including their IDs.
ContainerAERole	(Optional) Specify the parent role under which new roles are to be created. That is, if the business owner type is set to role-based ownership (value of 0), then any roles created will have this container AERole set as the parent role.
	If this parameter is not provided, no parent role is created. When no parent container is specified, all roles created are placed under the "Data Governance" role.
	The default configuration has a parent role called "Managed Resources" set as the default.
BusinessOwnerType	(Optional) Specify the type of business ownership to be assigned to newly created managed resources of this type. Valid values are:
	• 0: (Default) Role-based ownership. A new role will be created to own the resource.
	• 1: Identity-based ownership. This is equivalent to the behavior in version 7.0.1.
	NOTE: If you used the managed resource functionality to create simple shares in Data Governance Edition version 7.0.1, the default is set to Identity.
	The Role default setting is only used for new Data Governance Edition version 7.0.2 (or higher) installations and for upgraded installations if the managed resource functionality was never used.

Examples:

Table 23: Examples

Example	Description
Add QManagedResourceType -Name "Test Share"-FullControlAddToGroupID c61303ea-6d70-4d75-beb6-ef06d79d92aa - RecipientAddToGroupID 6d5e4f5b-a3bb-4882-b82d-1139313517f8 -PublishToITShop $false	Adds a new managed resource type, named "Test Share", indicating that managed resources associated with this resource type should not be published to the IT shop after the resource is created.

Get-QManagedResourceType

Retrieves details about a managed resource type from the Data Governance Edition deployment.

Syntax:

Get-QManagedResourceType [-Id [<String>]] [<CommonParameters>]

Table 24: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of the managed resource type to be retrieved. If this parameter is not specified, all managed resource types in the database are returned.

Examples:

Table 25: Examples

Example	Description
Get-QManagedResourceType	Returns a list of all managed resource types available in the database.
Get-QManagedResourceType -Id a816fe83-6d49-4f43-9c0a-b37589e1058d	Returns information on the specified managed resource type.

Details retrieved:

Table 26: Details retrieved

Detail	Description (Associated key or parameter in QAMManagedResourceType table)
Name	The name assigned to the managed resource type (Name).
Description	The description for the managed resource type (Description)
PublishedToITShop	Indicates whether a resource is to be published to the IT Shop when it is created. (PublishToITShop)
RecipientAddToGroupID	The value (GUID) assigned to template-generated group where recipients are added when creating new resources (UID_RecipientAddToGroup)
SetRestrictionList	Indicates whether the resource is to have a restriction list when it is created. (SetRestrictionList).

Detail	Description (Associated key or parameter in QAMManagedResourceType table)
FullControlAddToGroup	The value (GUID) assigned to the template-generated group where the Active Directory full control group is added when creating new resources (UID_FullCtrlAddToGroup).
ServerSelectionScriptID	The value (GUID) assigned to the default sever selection script being used for this type of resource (UID_DefaultSelectionScript).
ContainerAERole	The name of the parent role where newly created roles are created when the business owner type is set to role-based ownership (UID_ContainerAERole).
BusinessOwnerType	Indicates the type of business ownership associated with the managed resource type (BusinessOwnerType): • 0: Role-based ownership • 1: Identity-based ownership
Id	The value (GUID) assigned to the managed resource type (UID_QAMManagedResourceType).

Remove-QManagedResourceType

Removes a managed resource type from the Data Governance Edition deployment.

Syntax:

> Remove-QManagedResourceType -Id <String> [<CommonParameters>]

Table 27: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the managed resource type to be removed. Run the Get-QManagedResourceType cmdlet without any parameters to retrieve a list of available managed resource types and associated IDs.

Examples:

Table 28: Examples

Example	Description
Remove-QManagedResourceType -Id	Removes the specified managed resource

Example	Description
a816fe83-6d49-4f43-9c0a-b37589e1058d	type from the Data Governance Edition deployment.

Set-QManagedResourceType

Updates an existing managed resource type in the Data Governance Edition deployment.

Syntax:

Set-QManagedResourceType -Id <String> [-Name [<String>]] [-Description [<String>]] [-FullControlAddToGroupID [<String>]] [-RecipientAddToGroupID [<String>]] [-PublishToITShop <Boolean>] [-SetRestrictionList [<Boolean>]] [-ServerSelectionScriptID [<String>]] [-ContainerAERole [<String>]] [-BusinessOwnerType [<Int32>]] [<CommonParameters>]

Table 29: Parameters

Parameter	Description
Id	Specify the ID of the managed resource type to be updated.
Name	(Optional) Specify this parameter to change the name of the managed resource type.
Description	(Optional) Specify this parameter to add or change the description of the managed resource type.
FullControlAddToGroupID	(Optional) Specify this parameter to change the managed group template being used to build the domain-specific full control group for this managed resource type.
RecipientAddToGroupID	(Optional) Specify this parameter to change the managed group template being used to build the group where the recipient is to be added when the resource is created.
PublishToITShop	(Optional) Specify this parameter to change the flag that indicates whether a managed resource associated with this resource type should be published to the IT Shop after it is created.
SetRestrictionList	(Optional) Specify this parameter to change the flag that indicates whether to set a restriction list for a managed resource associated with this resource type after it is created. • $true: Run the SetRestrictionList subroutine to set a restriction list for this resource type. By default, the SetRestrictionList subroutine creates a restriction list

Parameter	Description
	based on the department, location and cost center properties defined in the requester's Identity record.
	• $false: (Default) No restriction list applies to this resource type.
ServerSelectionScriptID	(Optional) Specify this parameter to change the default server selection script to be run to determine an eligible server to create the share on.
	Run the Get-QServerSelectionScript cmdlet without any parameters to retrieve a list of available server selection scripts and their IDs.
ContainerAERole	(Optional) Specify this parameter to change the parent role under which new roles are to be created. That is, if the business owner type is set to role-based ownership (value of 0), then any roles created will have this container AERole set as the parent role.
BusinessOwnerType	(Optional) Specify this parameter to change the business ownership to be assigned to newly created managed resources of this type. Valid values are:
	• 0: (Default) Role-based ownership. A new role will be created to own the resource.
	• 1: Identity-based ownership. This is equivalent to the behavior in version 7.0.1.

Examples:

Table 30: Examples

Example	Description
Set QManagedResourceType -Id a816fe83-6d49-4f43-9c0a-b37589e1058d -PublishToITShop $false	Updates the specified managed resource type, indicating that a resource associated with this resource type should not be published to the IT shop after the resource is created.

Managed resource type domain object management

A managed resource type domain object contains various Active Directory specific settings for a managed resource type.

NOTE: In this release, the basic configuration includes only one managed resource type, Simple Share; therefore, for each managed domain, the managed resource type object specifies the Active Directory container where new groups are to be created and the group to be given full administrative control to the share.

The following commands are available to manage your group containers, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 31: Managed resource type domain object management commands

Use this command	If you want to
Add-QManagedResourceTypeDomain	Add a managed resource type domain object to the Data Governance Edition deployment.
Get-QManagedResourceTypeDomain	Retrieve a managed resource type domain object from the Data Governance Edition deployment.
	You can retrieve a specific object based on resource type or Active Directory domain or you can retrieve all managed resource type domain objects in the database.
Remove-QManagedResourceTypeDomain	Remove a managed resource type domain object from the Data Governance Edition deployment.
Set-QManagedResourceTypeDomain	Update the settings in an existing managed resource type domain object.

Add-QManagedResourceTypeDomain

Adds Active Directory domain specific settings for a managed resource type.

Syntax:

Add-QManagedResourceTypeDomain -ManagedResourceTypeID <String> -DomainID <String> [-ContainerID [<String>]] [-FullControlGroupID [<String>]] [-FileOperationsServerTagID [<String>]] [<CommonParameters>]

Table 32: Parameters

Parameter	Description
ManagedResourceTypeID	Specify the ID (GUID format) of the managed resource type to add.
DomainID	Specify the ID (GUID format) of the Active Directory domain this object applies to.
	NOTE: The ID can be located in the ADSDomain table in

Parameter	Description
	One Identity Manager after Active Directory synchronization is complete (UID_ADSDomain).
ContainerID	Specify the ID (GUID format) of the Active Directory container to use for managed group creation for a given managed resource type and Active Directory domain. NOTE: The ID can be located in the ADSContainer table in One Identity Manager after Active Directory synchronization is complete (UID_ADSContainer).
FullControlGroupID	(Optional) Specify the ID (GUID format) of the Active Directory group to give full control access. NOTE: Only groups that have been previously synchronized with One Identity Manager are available.
FileOperationsServerTagID	(Optional) Specify the value of the Server tag (Server Function) that identifies which job servers can fulfill functions involving file operations. That is, operations involving the creation of folders and shares on managed hosts. Enter the value assigned to the server tag when it was created, which may be an ID, such as QAM-Connector-DGE, for predefined server tags or a GUID for custom server tags. If this parameter is not specified, the Data Governance Connector (QAM-Connector-DGE server function) is used.

Examples:

Table 33: Examples

Example	Description
Add-QManagedResourceTypeDomain –ManagedResourceTypeID 7ade8b8d-a400-4fb1-ab82-6d424feeb63e –DomainID 50905871-5379-455d-8b65-c4bd02360bdb –ContainerID 5d3b3e7b-926b-429c-961b-d4bbe1611cac -FullControlGroupID 6de1fc3d-795f-41a4-b1cb-b0e1192ca547	Adds the necessary Active Directory domain settings for a managed resource type.

Get-QManagedResourceTypeDomain

Retrieves details about a managed resource type domain object from the Data Governance Edition deployment.

Syntax:

Get-QManagedResourceTypeDomain [-ManagedResourceID [<String>]] [-DomainID [<String>]] [<CommonParameters>]

Table 34: Parameters

Parameter	Description
ManagedResourceTypeID	(Optional) Specify the ID (GUID format) of the managed resource type to retrieve.
	If no parameters are specified, all objects in the database are returned.
	NOTE: If this parameter is included, the DomainID parameter must also be specified; otherwise, all objects are returned.
DomainID	(Optional) Specify the ID (GUID format) of the Active Directory domain to retrieve.
	If no parameters are specified, all objects in the database are returned.
	NOTE: If this parameter is included, the ManagedResourceTypeID must also be specified; otherwise, all objects are returned.

Examples:

Table 35: Examples

Example	Description
Get-QManagedResourceTypeDomain	Returns all managed resource type domain objects in the database.
Get-QManagedResourceTypeDomain -ManagedResourceTypeID 7ade8b8d-a400-4fb1-ab82-6d424feeb63e -DomainID 50905871-5379-455d-8b65-c4bd02360bdb	Returns the managed resource type domain object defined for the specified resource type and domain.

Details retrieved:

Table 36: Details retrieved

Detail	Description (Associated key or property in QAMManagedResourceTypeDomain table)
ManagedResourceTypeID	The value (GUID) assigned to the managed resource type (UID_QAMManagedResourceType).

Detail	Description (Associated key or property in QAMManagedResourceTypeDomain table)
ADSDomainID	The value (GUID) assigned to the ADS domain (UID_ADSDomain).
ADSContainerID	The value (GUID) assigned to the ADS group container (UID_ADSContainer).
FullControlGroup	The value (GUID) assigned to the full control group (UID_FullControlGroup).
FileOperationsServerTagID	The value (ID or GUID) assigned to the Server tag (Server Function) that identifies which job servers can fulfill functions involving file operations (UID_FileOperationsServerTag).

Remove-QManagedResourceTypeDomain

Removes a managed resource type domain object from the Data Governance Edition deployment.

Syntax:

Remove-QManagedResourceTypeDomain -ManagedResourceTypeID <String> -DomainID <String> [<CommonParameters>]

Table 37: Parameters

Parameter	Description
ManagedResourceTypeID	Specify the ID (GUID format) of the managed resource type associated with the managed resource type domain object to be removed.
	Run the Get-QManagedResourceTypeDomain cmdlet without any parameters to retrieve a list of available managed resource types and associated IDs.
DomainID	Specify the ID (GUID format) of the Active Directory domain associated with the managed resource type domain object to be removed.

Examples:

Table 38: Examples

Example	Description
Remove-QManagedResourceTypeDomain -ManagedResourceID 7ade8b8d-a400-4fb1-ab82-6d424feeb63e -DomainID 50905871-5379-455d-8b65-c4bd02360bdb	Removes the specified managed resource type domain object from the Data Governance Edition deployment.

Set-QManagedResourceTypeDomain

Updates the settings for an existing managed resource type domain object in the Data Governance Edition deployment.

Syntax:

Set-QManagedResourceTypeDomain -ManagedResourceTypeID <String> -DomainID <String> [-ContainerID [<String>]] [-FullControlGroupID [<String>]] [-FileOperationsServerTagID [<String>]] [<CommonParameters>]

Table 39: Parameters

Parameter	Description
ManagedResourceTypeID	Specify the ID (GUID format) of the managed resource type associated with the managed resource type domain object to be updated. Run the Get-QManagedResourceTypeDomain cmdlet without any parameters to retrieve a list of available managed group containers and associated IDs.
DomainID	Specify the ID (GUID format) of the Active Directory domain this object applies to. TIP: The ID can be located in the ADSDomain table in One Identity Manager after Active Directory synchronization is complete (UID_ADSDomain)..
ContainerID	(Optional) Specify this parameter to change the Active Directory container to use for managed group creation for a given Active Directory domain. Enter the ID (GUID format) of the Active Directory container. TIP: The ID can be located in the ADSContainer table in One Identity Manager after Active Directory synchronization is complete(UID_ADSContainer).

Parameter	Description
FullControlGroupID	(Optional) Specify this parameter to change the Active Directory group to give full control access. Enter the ID (GUID format) of the Active Directory group.
	TIP: Only groups that have been previously synchronized with One Identity Manager are available.
FileOperationsServerTagID	(Optional) Specify this parameter to change the Server tag (Server Function) that identifies which job servers can fulfill functions involving file operations. That is, operations involving the creation of folders and shares on managed hosts. Enter the value assigned to the server tag when it was created, which may be an ID, such as QAM-Connector-DGE, for predefined server tags or a GUID for custom server tags.

Examples:

Table 40: Examples

Example	Description
Set-QManagedResourceTypeDomain -ManagedResourceTypID 7ade8b8d-a400-4fb1-ab82-6d424feeb63e -DomainID 50905871-5379-455d-8b65-c4bd02360bdb -FullControlGroupID 6a402082-0be9-4815-9910-b69241ce6d6a	Updates the full control group associated with the specified managed resource type domain object.

Group template management

A managed group template defines how a hierarchy of Active Directory groups is to be created and nested to support ACLs for managed resources.

TIP: Prior to adding or modifying a managed group template, see The security model on page 54.

The following commands are available to manage your group templates, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 41: Group template management commands

Use this command	If you want to
Add-QManagedGroupTem-	Add a managed group template to the Data Governance

Use this command	If you want to
plate	Edition deployment.
Get-QManagedGroupTem-plate	Retrieve a managed group template from the Data Governance Edition deployment.
	You can retrieve a specific group template or a list of all group templates in the database.
Remove-QManagedGroupTemplate	Remove a managed group template from the Data Governance Edition deployment.
Set-QManagedGroupTem-plate	Update an existing managed group template in the Data Governance Edition deployment.

Add-QManagedGroupTemplate

Adds a managed group template to the Data Governance Edition deployment to define the hierarchy of Active Directory groups to be created to support ACLs for managed resources.

Syntax:

Add-QManagedGroupTemplate -GroupNamingPattern <String> [-Description [<String>]] [-GroupType [<Int32>]] [-ParentGroupTemplateID [<String>]] [-IsSelfServiceGroup [<Boolean>]] [<CommonParameters>]

Table 42: Parameters

Parameter	Description
GroupNamingPattern	Specify the default naming pattern to be used to name the group defined in the managed group template.
	A naming pattern is a series of literals and embedded variables that allows a group name to be dynamically generated at run time.
	Run the Get-QNamePatternResolver cmdlet to retrieve a list of available variables that can be used in the group naming pattern.
Description	(Optional) Specify a description for the managed group template.
GroupType	(Optional) Specify the type of Active Directory group to be created as defined in the managed group template:
	• 0: Domain Local group (Default)
	• 1: Global group

ONE IDENTITY by Quest

Parameter	Description
	• 2: Universal group
ParentGroupTemplateID	(Optional) Specify the ID (GUID format) of a parent group template under which the group defined in this managed group template is to be created. When created, child groups are nested as members of their parent group. When no parent group template is specified, a top-level (parent) group is created.
IsSelfServiceGroup	(Optional) Specify whether the group defined in the template is to be published to the IT Shop: • $true: Is available in the IT Shop • $false: Is not available in the IT Shop (Default) Setting this flag limits the "best fit" calculation to only include groups that have this flag set to $true.

Examples:

Table 43: Examples

Example	Description
Add-QManagedGroupTemplate -GroupNamingPattern L-[ShareName]-FC -GroupType 0	Adds a new top-level managed group template for a Domain Local group with a naming pattern of L-[ShareName]-FC.
Add-QManagedGroupTemplate -GroupNamingPattern G-[random]-FC -GroupType 1 -ParentGroupTemplateID b119eac0-7a92-45c3-b7af-6c97c8dc34f2	Adds a new managed group template for a Global group with a naming pattern of G-[random]-FC, nested under the specified Domain Local group.

Get-QManagedGroupTemplate

Retrieves a managed group template from the Data Governance Edition deployment.

Syntax:

Get-QManagedGroupTemplate [-Id [<String>]] [<CommonParameters>]

Table 44: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of the managed group template

Parameter	Description
	to be retrieved.
	If this parameter is not specified, all managed group templates in the database are returned.

Examples:

Table 45: Examples

Example	Description
Get-QManagedGroupTemplate	Returns a list of all managed group templates in the database.
Get-QManagedGroupTemplate -Id b119eac0-7a92-45c3-b7af-6c97c8dc34f2	Returns information on the specified managed group template.

Details retrieved:

Table 46: Details retrieved

Detail	Description (Associated key or property in QAMManagedGroupTemplate table)
GroupNamePattern	The pattern used to dynamically build the group name (GroupNamingPattern).
Description	The description for the managed group template (Description).
GroupType	Indicates the type of group to be created: Domain Local, Global or Universal (GroupType).
ParentGroupTemplateID	The value (GUID) assigned to the parent group template used for building nested groups (UID_ParentGroupTemplate).
IsSelfServiceGroup	Indicates whether this is a self-service group that is available in the IT Shop (IsSelfServiceGroup).
Id	The value (GUID) assigned to the managed group template (UID_QAMManagedGroupTemplate).

Remove-QManagedGroupTemplate

Removes a managed group template from the Data Governance Edition deployment.

Syntax:

Remove-QManagedGroupTemplate -Id <String> [<CommonParameters>]

Parameter	Description
Id	Specify the ID (GUID format) of the managed group template to be removed. Run the Get-QManagedGroupTemplate cmdlet without any parameters to retrieve a list of available managed group templates and associated IDs.

Examples:

Table 48: Examples

Example	Description
Remove-QManagedGroupTemplate -Id b119eac0-7a92-45c3-b7af-6c97c8d-c34f2	Removes the specified managed group template from the Data Governance Edition deployment.

Set-QManagedGroupTemplate

Updates an existing managed group template in the Data Governance Edition deployment.

Syntax:

Set-QManagedGroupTemplate -Id <String> -GroupNamingPattern <String> [-Description [<String>]] [-ParentGroupTemplateID [<String>]] [-GroupType [<Int32>]] [-IsSelfServiceGroup [<Boolean>]] [<CommonParameters>]

Table 49: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the managed group template to be updated.
GroupNamingPattern	(Optional) Specify this parameter to update the group naming pattern used for the group defined in the template. A group naming pattern is a series of literals and embedded variables that allows a group name to be dynamically generated at run time. Run the -Get-QNamePatternResolver cmdlet without any parameters to retrieve a list of available variables.
Description	(Optional) Specify this parameter to add or change the description of the managed group template.

Parameter	Description
ParentGroupTemplateID	(Optional) Specify this parameter to change the parent group template for this managed group template. When created, child groups are nested as members of their parent group.
GroupType	(Optional) Specify this parameter to change the type of Active Directory group defined in the template: • 0: Domain Local group • 1: Global group • 2: Universal group
IsSelfServiceGroup	(Optional) Specify this parameter to change the self-service setting for the group defined in the template: • $true: Is available in the IT Shop • $false: Is not available in the IT Shop

Examples:

Table 50: Examples

Example	Description
Set-QManagedGroupTemplate -Id b119eac0-7a92-45c3-b7af-6c97c8dc34f2 -GroupNamingPattern G-[rnd]-FC -GroupType 1	Changes the group type to a Global group in the specified managed group template.

Name pattern resolver management

A name pattern resolver is a variable that is resolved at run time in the context of the request to create a new managed resource during the Data Governance Administrator's approval process. These variables are listed on the **Group Name** dialog and can be added to the group naming pattern to dynamically construct unique Active Directory group names for the new managed resources.

TIP: Prior to adding or modifying a name pattern resolver, see Name pattern resolvers on page 60 for an overview of this feature.

The following commands are available to manage your name pattern resolvers, which are used in file system share creation requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 51: Name pattern resolver management commands

Use this command	If you want to
Add-QNamePatternResolver	Add a name pattern resolver to the Data Governance Edition deployment.
Get-QNamePatternResolver	Retrieve a name pattern resolver from the Data Governance Edition deployment. You can retrieve a specific name pattern resolver or a list of all name pattern resolvers (variables) in the database.
Remove-QNamePatternResolver	Remove a name pattern resolver (variable) from the Data Governance Edition deployment.
Set-QNamePatternResolver	Update an existing name pattern resolver in the Data Governance Edition deployment.

Add-QNamePatternResolver

Adds a name pattern resolver to the Data Governance Edition deployment.

A name pattern resolver is a variable that is resolved at run time in the context of the request to create a new managed resource. These variables can be added to the group naming pattern to dynamically construct unique Active Directory group names for the new managed resources.

Syntax:

Add-QNamePatternResolver -NamePatternVariable <String> -DialogScriptID <String> [<CommonParameters>]

Table 52: Parameters

Parameter	Description
NamePatternVariable	Specify the variable to be specified in the group naming pattern. For the "random number" variable, this is "random".
DialogScriptID	Specify the value assigned to the script that will be run to resolve the variable. For the "random number" variable, this is "QAM-6F86A9F78B1A0144A01EACEE3B4F54B3".

Examples:

Table 53: Examples

Example	Description
Add -QNamePatternResolver -NamePatternVariable "CurrentDate" -DialogScriptID "QAM-5E75A8E58B0A00FABDD2A3E43A2"	Adds a new name pattern resolver, CurrentDate, to the Data Governance Edition deployment.

Get-QNamePatternResolver

Retrieves a name pattern resolver from the Data Governance Edition deployment.

Syntax:

Get-QNamePatternResolver [-Id [<String>]] [<CommonParameters>]

Table 54: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of a name pattern resolver to retrieve.
	If this parameter is not specified, all name pattern resolvers in the database are returned.

Examples:

Table 55: Examples

Example	Description
Get-QNamePatternResolver	Returns a list of all name pattern resolvers in the database.
Get-QNamePatternResolver -Id 3b2a26da-a024-430f-adaa-3dbe5265cf5b	Returns information on the specified name pattern resolver.

Details retrieved:

Table 56: Details retrieved

Detail	Description (Associated key or property in QAMNamePatternResolver table)
Variable	The variable to be specified in a group naming pattern (NamePat-

Detail	Description (Associated key or property in QAMNamePat- ternResolver table)
	ternVariable).
DialogScriptID	The value assigned to the name pattern resolver script when it is created (UID_DialogScript).
Id	The value (GUID) assigned to the name pattern resolver (UID_ QAMNamePatternResolver).

Remove-QNamePatternResolver

Removes a name pattern resolver from the Data Governance Edition deployment.

Syntax:

> Remove-QNamePatternResolver -Id <String> [<CommonParameters>]

Table 57: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the name pattern resolver to be removed.
	Run the Get-QNamePatternResolver cmdlet without any parameters to retrieve a list of available name pattern resolvers and associated IDs.

Examples:

Table 58: Examples

Example	Description
Remove -QNamePatternResolver -Id 7c8dd75a-c42e-43f8-8c60-72c1a9050b6c	Removes the specified name pattern resolver from the database.

Set-QNamePatternResolver

Updates an existing name pattern resolver in the Data Governance Edition deployment.

Syntax:

> Set-QNamePatternResolver -Id <String> [-VariableName [<String>]] [-DialogScriptID [<String>]] [<CommonParameters>]

Table 59: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the name pattern resolver script to be updated.
VariableName	(Optional) Specify this parameter to change the variable to be specified in the group naming pattern.
DialogScriptID	(Optional) Specify this parameter to change the script to be used to resolve the variable. Enter the value assigned to a pre-defined script.

Examples:

Table 60: Examples

Example	Description
Set -QNamePatternResolver -Id b4626325-1b4e-4f28-9276-4723d2655d77 -VariableName "DeptName"	Updates the variable name assigned to the "QAM_GetDepartmentShortName" name pattern resolver.

Server selection script management

A server selection script can be used to select a QAMNode to host a new file share. Available server selection scripts appear on the **Sever Selection Scripts** dialog when the Data Governance Administrator selects to assign a file share host using the script option on the **File Share** page of the **New File Share** dialog.

TIP: Prior to adding or modifying a server selection script, see Server selection scripts on page 60 for an overview of this feature.

The following commands are available to manage your server selection scripts, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 61: Server selection script management commands

Use this command	If you want to
Add-QServer-SelectionScript	Add a server selection script to the Data Governance Edition deployment.
Get-QServer-SelectionScript	Retrieve a server selection script from the Data Governance Edition deployment. You can retrieve a specific server selection script or a list of all server selection scripts in the database.

Use this command	If you want to
Remove-QServer-SelectionScript	Remove a server selection script from the Data Governance Edition deployment.
Set-QServer-SelectionScript	Update an existing server selection script in the Data Governance Edition deployment.

Add-QServerSelectionScript

Adds a server selection script to the Data Governance Edition deployment, which can be used to select a managed host server to host a managed resource.

Syntax:

Add-QServerSelectionScript -DialogScriptID <String> [<CommonParameters>]

Table 62: Parameters

Parameter	Description
DialogScriptID	Specify the ID of an existing script to be run to determine an eligible server to create the share on.

Examples:

Table 63: Examples

Example	Description
Add-QServerSelectionScript -DialogScriptID "QAM-381B1818DC66DC367DA5AA2DA30663B1"	Adds a new server selection script to the database.

Get-QServerSelectionScript

Retrieves details about a server selection script from the Data Governance Edition deployment.

Syntax:

Get-QServerSelectionScript [-Id [<String>]] [<CommonParameters>]

Table 64: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of the server selection script to be retrieved. If this parameter is not specified, all server selection scripts in the database are returned.

Examples:

Table 65: Examples

Example	Description
Get-QServerSelectionScript	Returns a list of all the server selection scripts in the database.
Get-QServerSelectionScript -Id 2196674d-e227-4ce9-af29-1bb9f69a7718	Returns information on the specified server selection script.

Details retrieved:

Table 66: Details retrieved

Detail	Description (Associated key or property in QAMServerSelectionScript table)
DialogScriptID	The value assigned to the server selection script when it was created (UID_DialogScript).
Id	The value (GUID) assigned to the server selection script (UID_QAMServerSelectionScript).

Remove-QServerSelectionScript

Removes a server selection script from the Data Governance Edition deployment.

Syntax:

Remove-QServerSelectionScript -Id <String> [<CommonParameters>]

Table 67: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the server selection script to be removed.

Parameter	Description
	Run the Get-QServerSelectionScript cmdlet without any parameters to retrieve a list of available server selection scripts and associated IDs.

Examples:

Table 68: Examples

Example	Description
Remove-QServerSelectionScript 2196674d-e227-4ce9-af29-1bb9f69a7718	Removes the random node server selection script from the database.

Set-QServerSelectionScript

Updates an existing server selection script in the Data Governance Edition deployment.

Syntax:

Set-QServerSelectionScript -Id <String> [-DialogScriptID [<String>]] -Name <String> [<CommonParameters>]

Table 69: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the server selection script to be updated.
	Run the Get-QServerSelectionScript cmdlet without any parameters to retrieve a list of available server selection scripts and associated IDs.
DialogScriptID	(Optional) Specify this parameter to change the script to be run to determine an eligible server to create the share on. Enter the value assigned to a pre-defined script.

Examples:

Table 70: Examples

Example	Description
Set-QServerSelectionScript -Id "2196674d-e227-4ce9-af29-1bb9f69a7718" -DialogScriptID "QAM-381B1818DC66DC367DA5AA2DA30663B1"	Updates the specified server selection script.

Share root path management

A managed share root path defines root paths that a share could be created under for a given local managed host (QAMNode). Available managed share root paths appear on the **Managed Share Root Path** dialog when the Data Governance Administrator selects to assign a root path on the **File Share** page of the **New File Share** dialog.

NOTE: Only local managed hosts are supported at this time.

NOTE: You must add a share root path prior to creating a file system share request in the IT Shop. For more information, see Setting up share creation requests on page 36.

The following commands are available to manage your group containers, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 71: Share root path management commands

Use this command	If you want to
Add-QManagedShareRootPath	Add a managed share root path to the Data Governance Edition deployment.
Get-QManagedShareRootPath	Retrieve a managed share root path from the Data Governance Edition deployment.
	You can retrieve a specific share root path or a list of all managed share root paths in the database.
Remove-QManagedShareRootPath	Remove a managed share root path from the Data Governance Edition deployment.
Set-QManagedShareRootPath	Update an existing managed share root path in the Data Governance Edition deployment.

Add-QManagedShareRootPath

Adds a new managed share root path in the Data Governance Edition deployment to define where a share for the specified managed host (QAMNode) is to be created under.

Syntax:

Add-QManagedShareRootPath -QAMNodeID <String> -RootPath <String> [-Description [<String>]] [<CommonParameters>]

Table 72: Parameters

Parameter	Description
QAMNodeID	Specify the ID (GUID format) of the managed host (QAMNode) to which the path applies.
RootPath	Specify the root path to be used for new file shares, for example D$\ShareRoot1. NOTE: Only local managed hosts are supported at this time. Do not include the machine name as part of the path.
Description	(Optional) Specify a description for the shared root path.

Examples:

Table 73: Examples

Example	Description
Add-QManagedShareRootPath -QAMNode db9d52d9-8ef1-44b4-8941-47bd5223388c -RootPath D$\ShareRoot4	Adds a new share root path, D$\ShareRoot4 to the managed host with the GUID db9d52d9-8ef1-44b4-8941-47bd5223388c.

Get-QManagedShareRootPath

Retrieves details about a managed shared root path that defines where a share is to be created under for a given QAMNode.

Syntax:

Get-QManagedShareRootPath [-Id [<String>]] [<CommonParameters>]

Table 74: Parameters

Parameter	Description
Id	(Optional) Specify the ID (GUID format) of the managed share root path to be retrieved. If this parameter is not specified, all managed share root paths in the database are returned.

Examples:

Table 75: Examples

Example	Description
Get-QManagedShareRootPath	Returns a list of all managed share root paths in the database.
Get-QManagedShareRootPath -Id ca65709c-5d80-43e6-a56f-de6468ca6b51	Returns information on the specified managed share root path.

Details retrieved:

Table 76: Details retrieved

Detail	Description (Associated key or property in QAMManagedShareRootPath table)
RootPath	The value assigned to the managed share root path (RootPath).
Description	The description of the managed share root path (Description).
QAMNodeID	The value (GUID) assigned to the QAMNode where this root path resides (UID_QAMNode).
Id	The value (GUID) assigned to the managed share root path (UID_QAMManagedShareRootPath).

Remove-QManagedShareRootPath

Removes an existing managed shared root path from the Data Governance Edition deployment.

Syntax:

Remove-QManagedShareRootPath -Id <String> [<CommonParameters>]

Table 77: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the managed share root path to be removed. Run the Get-QManagedShareRootPath cmdlet without any parameters to retrieve a list of available managed share root paths and associated IDs.

ONE IDENTITY
by Quest

Data Governance Edition 9.2 IT Shop Resource Access Requests
User Guide

102

Appendix: PowerShell commands

Examples:

Table 78: Examples

Example	Description
Remove-QManagedShareRootPath -Id ca65709c-5d80-43e6-a56f-de6468ca6b51	Removes the specified managed share root path from the database.

Set-QManagedShareRootPath

Updates a managed shared root path in the Data Governance Edition deployment.

Syntax:

Set-QManagedShareRootPath -Id <String> [-RootPath [<String>]] [-Description [<String>]] [-QAMNodeID [<String>]] [<CommonParameters>]

Table 79: Parameters

Parameter	Description
Id	Specify the ID of the managed share root path to be updated.
	Run the Get-QManagedShareRootPath cmdlet without any parameters to retrieve a list of available managed share root paths and associated IDs.
RootPath	(Optional) Specify this parameter to change the share root path.
	Only local managed hosts are supported at this time. Do not include the machine name as part of the path.
Description	(Optional) Specify this parameter to add or change the description of the shared root path.
QAMNodeID	(Optional) Specify this parameter to change the managed host (QAMNode) to which the path applies.

Examples:

Table 80: Examples

Example	Description
Set-QManagedShareRootPath -Id ca65709c-5d80-43e6-a56f-de6468ca6b51 -RootPath C$\ShareRoot1	Updates the specified managed share root path in the database.

Type group permissions object management

A type group permissions object correlates possible permissions and group hierarchies within a managed resource type.

The default managed resource types defined include:

- L-[costcenter]-[random]-FC - Simple Share
- L-[costcenter]-[random]-R - Simple Share
- L-[costcenter]-[random]-RW - Simple Share

TIP: Prior to adding or modifying a type group permission object, see The security model on page 54 for an overview of this feature.

The following commands are available to manage your type group permissions objects, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 81: Type group permissions object management commands

Use this command	If you want to
Add-QTypeGroupPer-missions	Add a new type group permissions object to the Data Governance Edition deployment.
Get-QTypeGroupPer-missions	Retrieve a type group permissions object from the Data Governance Edition deployment.
	You can retrieve a specific type group permissions object or a list of all type group permissions in the database.
Remove-QTypeGroupPer-missions	Remove a type group permissions object from the Data Governance Edition deployment.
Set-QTypeGroupPer-missions	Update an existing type group permissions object in the Data Governance Edition deployment.

Add-QTypeGroupPermissions

Adds a type group permissions object to the Data Governance Edition deployment.

A type group permissions object correlates possible permissions and group hierarchies within a managed resource type.

ONE IDENTITY
by Quest

Syntax:

Add-QTypeGroupPermissions -ManagedResourceTypeID <String> -
ManagedGroupTemplateID <String> [-Permissions [<Int32>]]
[<CommonParameters>]

Table 82: Parameters

Parameter	Description
ManagedResourceTypeID	Specify the ID (GUID format) of a managed resource type to be associated with the new type group permissions object.
	Run the Get-QManagedResourceType cmdlet to retrieve a list of available resource types and their IDs.
ManagedGroupTemplateID	Specify the ID (GUID format) of a managed group template to be associated with the new type group permissions object.
	Run the Get-QManagedGroupTemplate cmdlet to retrieve a list of available group templates and their IDs.
Permissions	(Optional) Specify the type of permissions to use for the new type group permissions object:
	• 0: Read (Default)
	• 1: Read Write
	• 2: Full Control
	If this parameter is not specified, Read permissions is used for the type group permissions object.

Examples:

Table 83: Examples

Example	Description
Add-QTypeGroupPermissions -ManagedResourceTypeID a816fe83-6d49-4f43-9c0a-b37589e1058d -ManagedGroupTemplateID 0381aced-2aa7-4cc0-bbe2-b400a9c9ea9e	Creates a type group permissions object with Read permissions.
Add-QTypeGroupPermissions -ManagedResourceTypeID a816fe83-6d49-4f43-9c0a-b37589e1058d -ManagedGroupTemplateID 381aced-2aa7-4cc0-bbe2-b400a9c9ea9e -Permissions 1	Creates a type group permissions object with Read Write permissions.

Get-QTypeGroupPermissions

Retrieves information about a type group permissions object from the Data Governance Edition deployment.

Syntax:

Get-QTypeGroupPermissions [-ManagedResourceTypeID [<String>]] [-ManagedGroupTemplateID [<String>]] [<CommonParameters>]

Table 84: Parameters

Parameter	Description
ManagedResourceTypeID	(Optional) Specify the ID (GUID format) of a managed resource type to retrieve associated managed group templates and assigned permissions.
	If either the ManagedResourceTypeID or ManagedGroupTemplateID are not specified, then all type group permission objects in the database are returned.
ManagedGroupTemplateID	(Optional) Specify the ID (GUID format) of a managed group template to retrieve the associated managed resource type.
	If either the ManagedResourceTypeID or ManagedGroupTemplateID are not specified, then all type group permission objects in the database are returned.

Examples:

Table 85: Examples

Example	Description
Get-QTypeGroupPermissions	Returns a list of all the type group permissions objects in the database.
Get-QTypeGroupPermissions -ManagedResourceTypeID a816fe83-6d49-4f43-9c0a-b37589e1058d -ManagedGroupTemplateID b119eac0-7a92-45c3-b7af-6c97c8dc34f2	Returns type group permission information for the specified managed resource type (simple share) and managed group template.

Details retrieved:

Table 86: Details retrieved

Detail	Description (Associated key or property in QAMTypeGroupPermissions table)
ManagedGroupTemplateID	The value (GUID) assigned to the managed group template associated with this managed resource type (UID_QAMManagedGroupTemplate).
ManagedResourceTypeID	The value (GUID) assigned to a managed resource type (UID_QAMManagedResourceType).
Permissions	The permission assigned to the object (Permission): • 0: Read • 1: Read Write • 2: Full Control

Remove-QTypeGroupPermissions

Removes a type group permissions object from the Data Governance Edition deployment.

Syntax:

Remove-QTypeGroupPermissions -ManagedResourceTypeID <String> -ManagedGroupTemplateID <String> [<CommonParameters>]

Table 87: Parameters

Parameter	Description
ManagedResourceTypeID	Specify the ID (GUID format) of a managed resource type for the type group permissions object to be removed.
ManagedGroupTemplateID	Specify the ID (GUID format) of a managed group template for the type group permissions object to be removed.

Examples:

Table 88: Examples

Example	Description
Remove-QTypeGroupPermissions -ManagedResourceTypeID a816fe83-6d49-	Removes the specified type group permissions object from the database.

ONE IDENTITY by Quest

Example	Description
4f43-9c0a-b37589e1058d -ManagedGroupTemplateID b119eac0- 7a92-45c3-b7af-6c97c8dc34f2	

Set-QTypeGroupPermissions

Updates the permissions assigned to an existing type group permissions object in the Data Governance Edition deployment.

Syntax:

Set-QTypeGroupPermissions -ManagedResourceTypeID <String> -
ManagedGroupTemplateID <String> [-Permissions [<Int32>]]
[<CommonParameters>]

Table 89: Parameters

Parameter	Description
ManagedResourceTypeID	Specify the ID (GUID format) of the managed resource type linked to the type group permissions object to be updated. Run the Get-QManagedResourceType cmdlet without any parameters to retrieve a list of available managed resource types and associated IDs.
ManagedGroupTemplateID	Specify the ID (GUID format) of the managed group template linked to the type group permissions object to be updated. Run the Get-QManagedGroupTemplate cmdlet without any parameters to retrieve a list of available managed group templates and associated IDs.
Permissions	(Optional) Specify this parameter to add or change the permissions assigned to the type group permissions object. • 0: Read • 1: Read Write • 2: Full Control

Examples:

Table 90: Examples

Example	Description
Set-QTypeGroupPermissions -ManagedRe-sourceTypeID a816fe83-6d49-4f43-9c0a-b37589e1058d -ManagedGroupTemplateID b119eac0-7a92-45c3-b7af-6c97c8dc34f2 -Permissions 0	Changes the permissions on the selected type group permissions object to "Read".

Managed resource function management

A managed resource function contains mappings between arbitrary logical functions and the scripts that implement them. These functions can be used by the approval and creation process for a managed resource.

The default managed resource functions provided include:

- LocateFileOperationsJobServer: Default processor for locating a job server that can process new shares and file paths when creating a new managed resource.

- ResolveADContainer: Default processor for locating an Active Directory container ID for use when creating new managed resource groups.

- SetRestrictionList: Restriction list processing subroutine for managed resource creation.

TIP: Prior to adding, removing or modifying a managed resource function, see Managed resource functions on page 61 for an overview of this feature.

The following commands are available to manage your managed resource functions, which are used in file system share requests in the IT Shop. For full parameter details and examples, click a command in the table or see the command help, using the **Get-Help** command.

Table 91: Managed resource function management commands

Use this command	If you want to
Add-QManagedRe-sourceFunction	Add a new managed resource function to the Data Governance Edition deployment.
Get-QManagedRe-sourceFunction	Retrieve a specific or all managed resource function records from the Data Governance Edition deployment. You can retrieve a specific managed resource function or a list of all managed resource function records in the

Use this command	If you want to
	database.
Remove-QManagedResourceFunction	Remove a managed resource function from the Data Governance Edition deployment.
Set-QManagedResourceFunction	Update an existing managed resource function in the Data Governance Edition deployment.

Add-QManagedResourceFunction

Adds a new managed resource function to the Data Governance Edition deployment.

NOTE: Adding a new managed resource function will not change how the current default process works. To use a newly created managed resource function requires you to create a new process chain to call the new function or subroutine.

Syntax:

Add-QManagedResourceFunction -Name <String> [-Description [<String>]] -ManagedResourceTypeID <String> -DialogScriptID <String> [<CommonParameters>]

Table 92: Parameters

Parameter	Description
Name	Specify the name of the new managed resource function.
Description	(Optional) Enter a brief description for the new managed resource function.
ManagedResourceTypeID	Specify the value (GUID) assigned to the managed resource type associated with the new managed resource function.
DialogScriptID	Specify the value assigned to the predefined script associated with the new managed resource function.

Examples

Table 93: Examples

Example	Description
Add-QManagedResourceFunction -Name "MyFunction" -ManagedResourceTypeID 7ade8b8d-a400-4fb1-ab826d424feeb63e -DialogScriptID "QAM-	Adds a new managed resource function named "MyFunction" for the managed resource type with the GUID 7ade8b8d-a400-4fb1-ab826d424feeb63e, and associ-

ONE IDENTITY by Quest

Example	Description
2B2A19808659A444B94932679D601234"	ates it with the QAM-2B2A19808659A444B94932679D601234 script.

Get-QManagedResourceFunction

Retrieves a specific or all managed resource function records found in the Data Governance Edition deployment.

Syntax:

Get-QManagedResourceFunction [-Id [<String>]] [<CommonParameters>]

Table 94: Parameters

Parameter	Description
Id	(Optional) Specify the value (GUID format) of the managed resource function to retrieve. If this parameter is not specified, all managed resource function records in the database are returned.

Examples:

Table 95: Examples

Example	Description
Get-QManagedResourceFunction	Retrieves a list of all managed resource function records found in the database.

Details retrieved:

Table 96: Details retrieved

Detail	Description (Associated key or property in QAMManagedResourceFunction table)
Name	The name of the managed resource function.
Description	The description entered when the managed resource function was created.
ManagedResourceTypeID	The value (GUID) assigned to the resource type associated with the managed resource function (UID_QAMMan-

Detail	Description (Associated key or property in QAMMan- agedResourceFunction table)
	agedResourceType).
DialogScriptID	The value assigned to the script called by the managed resource function (UID_DialogScript).
Id	The value (GUID) assigned to the managed resource function (UID_QAMManagedResourceFunction).

Remove-QManagedResourceFunction

Removes a managed resource function record from the Data Governance Edition deployment.

NOTE: Do NOT remove the predefined managed resource functions provided. Removing any of these managed resource functions prevents the existing process chain from working.

Syntax:

Remove-QManagedResourceFunction -Id <String> [<CommonParameters>]

Table 97: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the managed resource function to be removed.

Examples

Table 98: Examples

Example	Description
Remove-QManagedResourceFunction -Id e39946d5-1397-43a7-972a-7557c5511234	Removes the specified managed resource function from the database,

Set-QManagedResourceFunction

Updates an existing managed resource function in the Data Governance Edition deployment.

NOTE: In order to use the existing process chain, only modify the Description or DialogScriptID parameters of a sample managed resource function record. Changing any

of the other optional parameters requires you to create a custom process chain to call the updated function.

Syntax:

Set-QManagedResourceFunction -Id <String> [-Name [<String>]] [-Description [<String>]] [-ManagedResourceTypeID [<String>]] [-DialogScriptID [<String>]] [<CommonParameters>]

Table 99: Parameters

Parameter	Description
Id	Specify the ID (GUID format) of the managed resource function to be updated.
Name	(Optional) Specify this parameter to change the name assigned to the managed resource function.
Description	(Optional) Specify this parameter to change the description of the managed resource function.
ManagedResourceTypeID	(Optional) Specify this parameter to change the managed resource type associated with the managed resource function. Enter the value (GUID format) of the managed resource type.
DialogScriptID	(Optional) Specify this parameter to change the script associated with the managed resource function. Enter the value (GUID format) assigned to a predefined script when it was created in One Identity Manager.

Examples:

Table 100: Examples

Example	Description
Set-QManagedResourceFunction -Id e39946d5-1397-43a7-972a-7557c55182a8 -Description "Custom Restriction List" -DialogScriptID "CCC-EF1751D37DCE4F43B1361E3CDB47F49F"	Changes the description and the script called by the Simple Share-SetRestrictionList function record.

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 Ticket
- 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

Data Governance Edition 9.2 IT Shop Resource Access Requests
User Guide

114

About us

Index

ONE IDENTITY
by Quest

Data Governance Edition 9.2 IT Shop Resource Access Requests
User Guide

117

Index