GroupID

by imanami | NOW PART OF netwrix

Version 10

GroupID Authenticate

GroupID Automate

GroupID Self-Service

GroupID Synchronize

GroupID Password Center

GroupID Insights

GroupID Mobile App

GroupID Reports

User Guide

Self-Service

This publication applies to GroupID Version 10 and subsequent releases until otherwise indicated in new editions.

Contents

Chapter 1 - Introduction to Self-Service

GroupID Self-Service lets you quickly build and deploy web-based portals for end-users to carry out their own directory and group management tasks.

Using a Self-Service portal, users can:

- Search the directory
- Maintain and update their directory profiles
- Create and update directory objects

You can also use Self-Service to reduce the work required to manage groups. Self-Service allows end-users to create, delete and edit groups, without assistance from an administrator.

When enterprise users maintain and update their own information, data is more accurate and reliable. Yet you still maintain complete control over data integrity, because you determine what users can view and change using the portal.

You can also define workflows for Self-Service portals; these workflows serve as a built-in auditing system to ensure that correct data is entered before applying changes in the directory.

A Self-Service portal can also send notification emails to designated recipients when a user makes any change to an object in the directory.

Role-based security

In GroupID, user roles are defined at the identity store level. Each role is granted a set of permissions, such that role members can perform the operations they have permissions for.

Priority value

Each user role has a priority value in the 1-99 range, where 1 is the highest and 99 is the lowest value. Role priority is unique for each role in an identity store, and determines which role is higher than the other.

Chapter 2 - Creating a Self-Service Portal

A Self-Service portal represents a virtual link with the directory. Using it, users can:

- Create and manage their directory groups
- Join and leave semi-private and public groups
- View and update their own profile information in the directory
- Search the directory and even export the results to a Microsoft Excel file
- Approve or deny workflow requests
- View a log of the actions they have performed through the portal

You do not have to create a different Self-Service portal for each identity store defined in GroupID; rather, a portal can serve multiple identity stores. While creating a portal, you must associate it with one or more identity stores. When logging into the portal, a user must select an identity store to connect to.

Prerequisites for a portal

The following must be defined in GroupID before a Self-Service portal can be created:

- An identity store
  A portal cannot be created unless an identity store is defined in GroupID since a portal must be associated with an identity store to enable users to carry out profile and group management functions for that store.
- An SMTP server and a messaging system
  These must be configured for each identity store you want to associate with your portal, so that notification emails can be sent using the portal.
- Scheduled jobs
  Scheduled jobs must be defined for an identity store, so that different activities in the portal, such as group membership update, group expiry and deletion, and orphan group ownership, are automatically carried out on a scheduled basis.
- Role-based permissions
  A user must belong to at least one user role in the identity store in order to

log into the portal. When logged on, the user will be able to perform the tasks his or her role has permissions for.

- Workflows (optional)
  With workflows defined for an identity store, any changes made to an object are approved by an authorized user before they are committed to the directory.

Role policies

Additionally, the following policies, which are defined for each user role in an identity store, also impact the portal:

- **Group Owners policy**
  This policy applies when a role member creates or modifies a static group or Smart Group. It specifies:
  - Whether the group must have a primary owner
  - The number of additional owners the group must have.
- **Group name prefixes policy**
  Administrators can enforce the use of prefixes in group names.
- **New object policy**
  This policy restricts role members to create new directory objects in specific containers(s).
- **Search policy**
  This policy limits the search scope of the portal to a particular container for role members. The administrator can also designate a criterion to filter specific objects in searches.

Second factor authentication

If the GroupID administrator enables second factor authentication for a user role in an identity store, role members must authenticate their identity store accounts while logging into the portal.

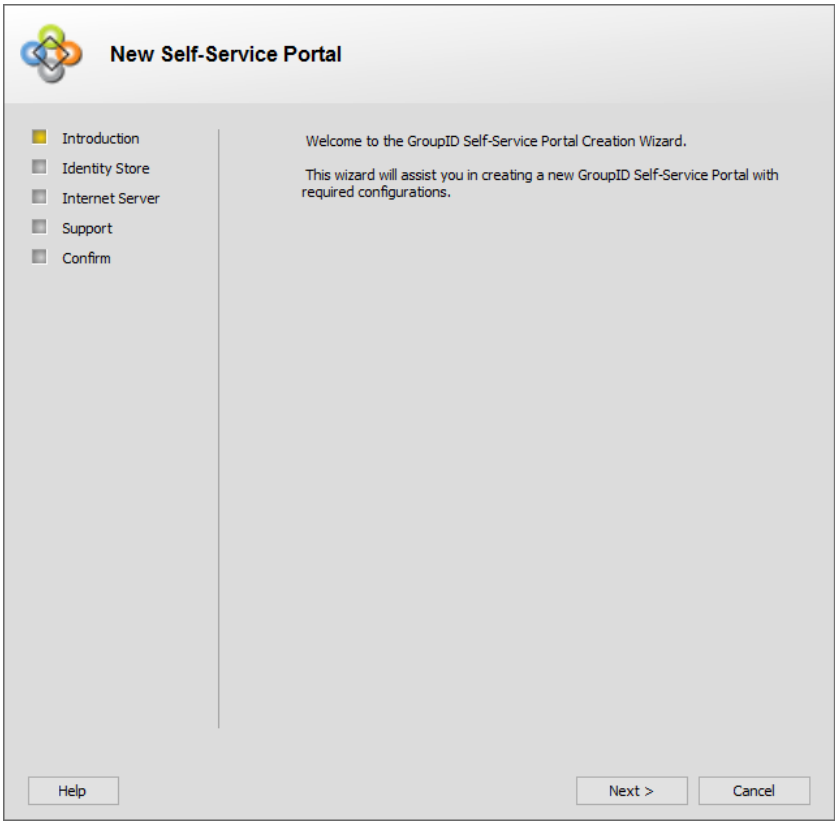
Create a new Self-Service portal

You can create a portal using the portal creation wizard or by copying an existing portal.

Create a portal using the wizard

1. In GroupID Management Console, select the **Self-Service** node.
2. Click the **User Portal** link under **How to create a User Portal** or right-click **Portals** in the left pane and select **Create**.

   The portal creation wizard opens to the **Introduction** page.

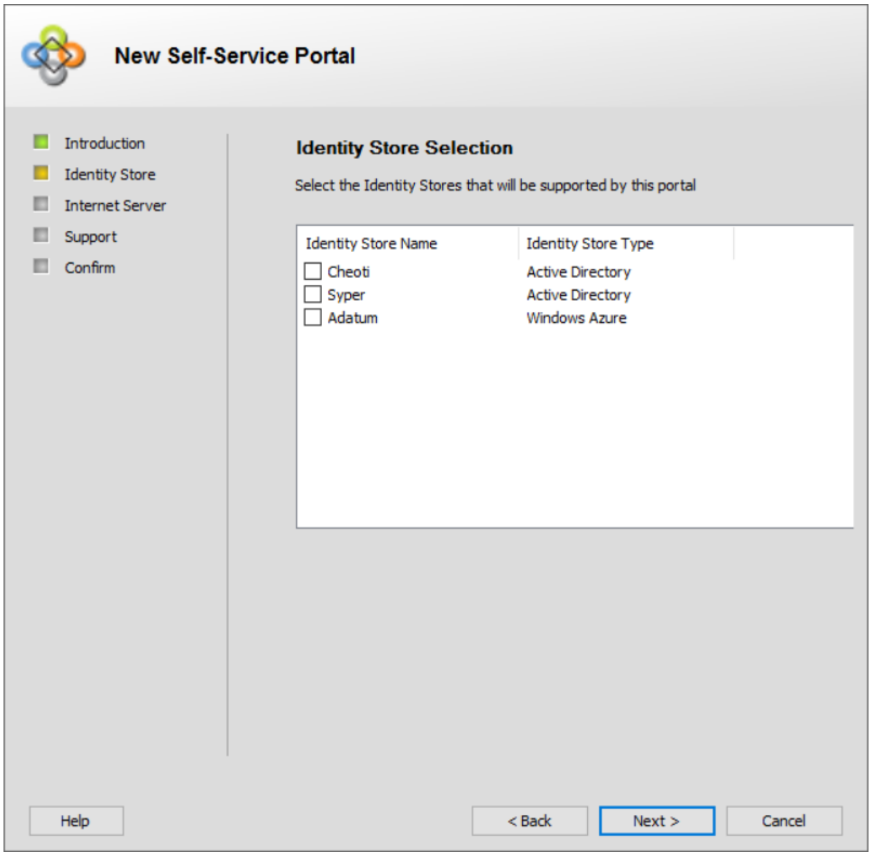
   

   Welcome to the GroupID Self-Service Portal Creation Wizard.

   This wizard will assist you in creating a new GroupID Self-Service Portal with required configurations.

   Figure 1: Introduction page

3. Read the welcome message and click **Next**.



Identity Store Selection

Select the Identity Stores that will be supported by this portal

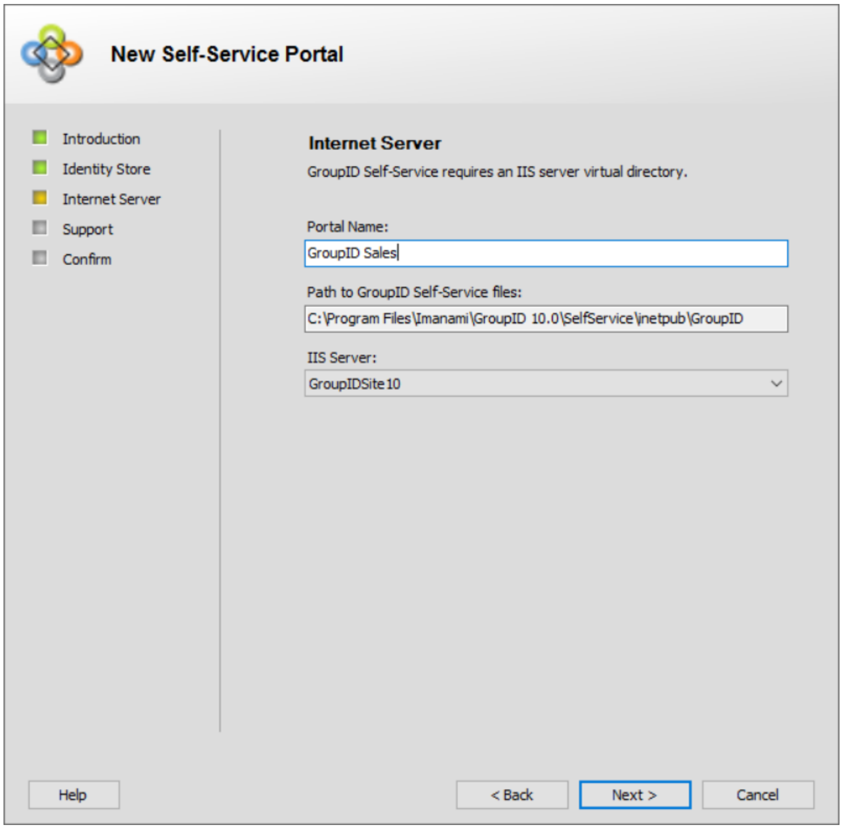
Identity Store Name	Identity Store Type
□ Cheoti	Active Directory
□ Syper	Active Directory
□ Adatum	Windows Azure

Figure 2: Identity Store Selection page

4. On the **Identity Store Selection** page, select the check box for an identity store to associate it with the portal. Users of this identity store can log into the portal to manage directory objects (users, mailboxes, contacts, groups), their directory profiles, and more.

   You can associate multiple identity stores with a portal.

5. Click **Next**.



Internet Server

GroupID Self-Service requires an IIS server virtual directory.

Portal Name: GroupID Sales

Path to GroupID Self-Service files: C:\Program Files\Imanami\GroupID 10.0\SelfService\inetpub\GroupID

IIS Server: GroupIDSite10

Figure 3: Internet Server page

6. The Self-Service portal runs within a virtual directory on Internet Information Server (IIS). On the **Internet Server** page, you can view the location where portal files are physically located on disk, and specify the website on IIS that will host the portal.

   When you create the portal, GroupID creates a directory with the portal’s name at the given path and copies the portal files from its template directory to the file system path. It also creates a virtual directory on the selected IIS website.

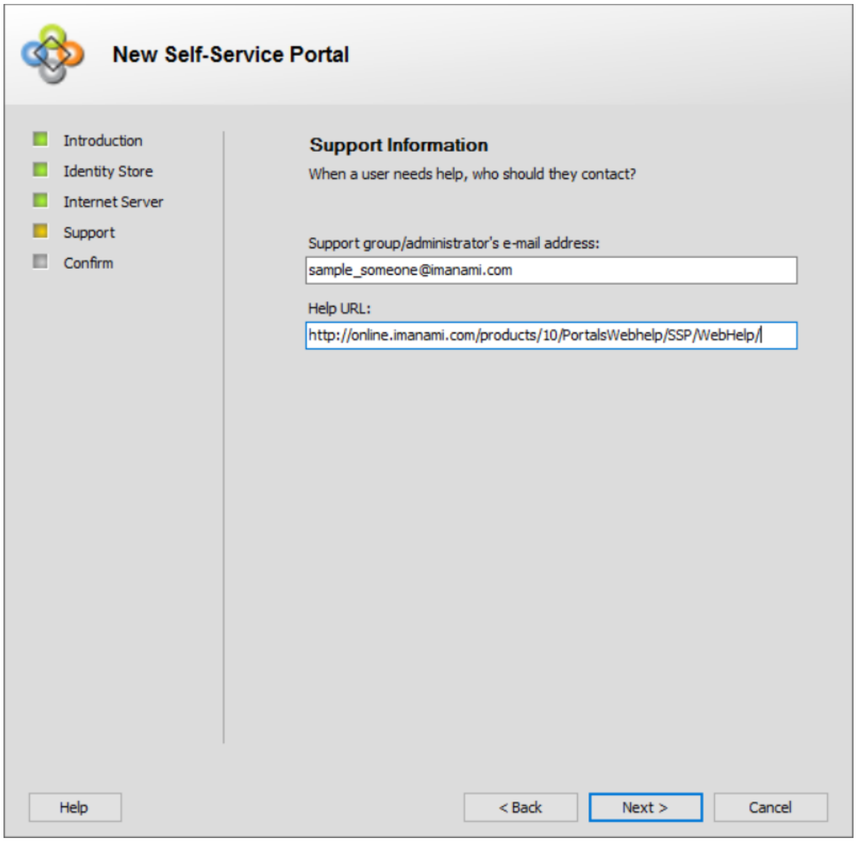
   a. In the **Portal Name** box, change the name of the portal or use the default name.

   b. The **Path to GroupID Self-Service files** field displays the path to the directory where the portal files are located on disk. The path is read-only.

   c. From the **IIS Server** drop-down list, select the website to host the portal files.

      The list displays the websites defined on the local IIS server. **GroupIDSite10** is the default selection.

7. Click **Next**.



Support Information

When a user needs help, who should they contact?

Support group/administrator's e-mail address: sample_someone@imanami.com

Help URL: http://online.imanami.com/products/10/PortalsWebhelp/SSP/WebHelp/

Figure 4: Support Information page

8. On the **Support Information** page, enter internal contact information and resource links for the portal's users to obtain help using the portal.

   A Self-Service portal includes two links, **Contact** and **Help**, on its web interface. The **Contact** link launches an email application to send an email to the administrator or Helpdesk for inquiries or support. The **Help** link launches the online help for the portal in a new browser window. Both links are customizable and their target email address or web address is specified on the **Support Information** page.

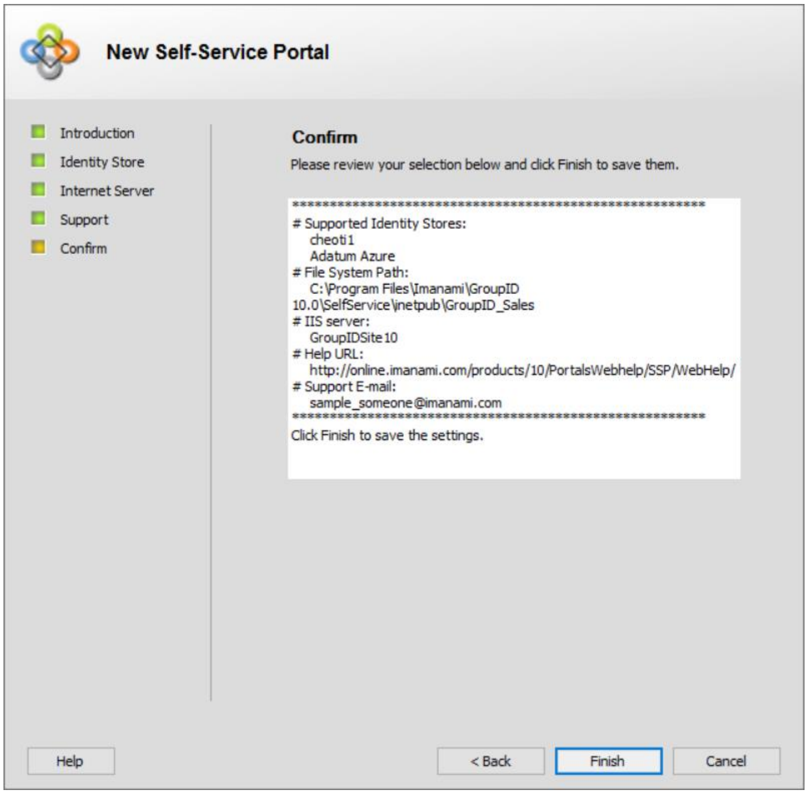
   a. In the **Support group/administrator’s e-mail address** box, type the e-mail address of the group, user or contact to whom the users’ queries will be directed.

      This email address is mapped to the **Contact** link in the portal.

   b. In the **Help URL** box, specify the address of your company's internal support website or the portal’s help page, where portal users can find support material or report their problems. By default, this box displays the URL of the portal’s help page.

This URL is mapped to the **Help** link in the portal.

9. Click **Next**.



Confirm

Please review your selection below and click Finish to save them.

```
************************************************************
# Supported Identity Stores:
    cheoti1
    Adatum Azure
# File System Path:
    C:\Program Files\Imanami\GroupID
10.0\SelfService\inetpub\GroupID_Sales
# IIS server:
    GroupIDSite10
# Help URL:
    http://online.imanami.com/products/10/PortalsWebhelp/SSP/WebHelp/
# Support E-mail:
    sample_someone@imanami.com
************************************************************
Click Finish to save the settings.
```

Figure 5: Confirm page

10. On the **Confirm** page, review the settings that you have entered on the previous pages. Use the **Back** button to access settings that you want to change.

11. After reviewing the information, click **Finish**.

The new portal is now available under the **Self-Service > Portals** node.

Create a portal by copying an existing portal

You can create a new portal by copying an existing portal. All server and design configurations of the copied portal are duplicated to the new portal.

1. In GroupID Management Console, select **Self-Service > Portals**.

2. Right-click the portal you want to copy and select **Copy Portal**.
   The **New Self-Service Portal** wizard is displayed; its pages are populated with the settings of the copied portal.

3. To modify any setting, follow the instructions in the section, Create a portal using the wizard on page 4, beginning at step 3.

Launch a Self-Service portal

1. Click **Self-Service > Portals > [portal name] > Server**. The **General** tab lists the portal URLs for different functionality modes, with the first URL for the default Enterprise mode.
2. Click a URL to launch the portal in the specific functionality mode.

Provide the URL to your users so that they can access the portal.

Notifications in the Self-Service portal

A Self-Service portal can send email notifications to designated recipients when a user makes a change to the identity store, if notifications are configured for that identity store in GroupID Management Console.

The administrator can also specify notification recipients, that can be:

- individual recipients
- the user who makes a change to a directory object
- the directory object being modified.
- group owners and user managers—a practice that does not require updating when role assignments change
- primary owner, additional owners and Exchange additional owners of a public group on membership changes
- an object that is added to the membership of a group
- an object that is removed from the membership of a group

Notification language

By default, notifications are sent to users in the English language. However, a user can opt to receive notifications in a different language by personalizing the language settings from the **User Settings** panel in the Self-Service portal.

Setting a portal’s Functionality Mode

A Self-Service portal can be configured to run in one of the five functionality modes, with each mode exposing a different set of features. Mode-specific URLs determine the mode to launch the Self-Service portal in.

Self-Service supports five functionality modes. These are:

- Enterprise
- My Profile
- Update Wizard
- Groups
- Phonebook

A newly created portal, by default, runs in the Enterprise mode. To change the mode, see Set a portal’s functionality mode on page 16.

Deleting a portal

Deleting a portal removes:

- the portal directory under the following location on disk:
  X:\Program Files\Imanami\GroupID 10.0\SelfService\inetpub\
  (where X represents the GroupID installation drive).
- the portal’s virtual directory from the website in IIS.
  This website was selected for hosting the portal web application on the **Internet Server** page (Figure 3) of the portal creation wizard.

To delete a portal:

1. In GroupID Management Console, select **Self-Service > Portals**.
2. Right-click the portal that you want to delete and select **Delete Portal**.

Chapter 3 - Server Configurations for a Self-Service Portal

You can control these server configurations for a Self-Service portal.

- Change a portal’s name
- Manage settings for the IIS server that hosts the portal
- Set a functionality mode for the portal
- Manage support settings
- Configure Windows logging and File logging for a portal
- Apply advanced settings to a portal
- Link a portal to identity stores

NOTE When any of the above configurations change, the portal’s session ends and all connected users are logged out. When accessed again, the portal runs with the new configurations.

Change a portal’s display name

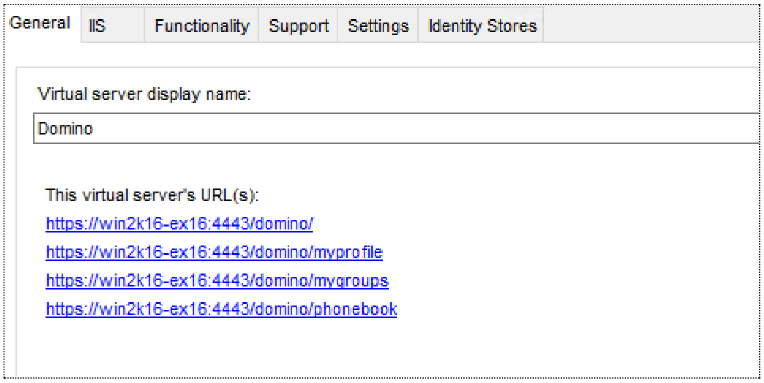
A portal is assigned a display name during creation. This name uniquely identifies the portal and is used to name the portal’s virtual directory in IIS and its physical directory under ***X:\Program Files\Imanami\GroupID 10.0\SelfService\Inetpub*** (where **X** represents the GroupID installation drive).

This name is also appended to the web server address to construct the URL that users click to access the portal. For example:
http://[Web server name]/[portal's display name]

You can change the portal name, but the change propagates only to the IIS directory; the physical directory name remains unchanged.

View a portal's display name

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **General** tab.



Virtual server display name:
Domino

This virtual server's URL(s):
https://win2k16-ex16:4443/domino/
https://win2k16-ex16:4443/domino/myprofile
https://win2k16-ex16:4443/domino/mygroups
https://win2k16-ex16:4443/domino/phonebook

Figure 6: General tab

The **Virtual server display name** box displays the name of the portal.

Change a portal's display name

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **General** tab (Figure 6).
3. In the **Virtual server display name** box, type a new name for the portal.
4. On the toolbar, click Save .

Functionality mode URLs

Depending on the functionality mode selected for the portal on the **Functionality** tab (Figure 8), the **General** tab (Figure 6) displays a URL for launching the portal in that mode. Under the **Enterprise** mode only, the tab displays URLs for all functionality modes.

A functionality mode selected for a portal applies to all users of that portal. However, if you want certain users to access the same portal in a different functionality mode, then provide the URL of the respective mode to those users.

This table shows the addresses (URLs) for all functionality modes:

URL	Description
http://Server/PortalName	Provides access to the Enterprise mode.
http://Server/PortalName/myprofile	Provides access to the My Profile mode.
http://Server/PortalName/update	Provides access to the Update Wizard mode.
http://Server/PortalName/groups	Provides access to the Groups mode.
http://Server/PortalName/phonebook	Provides access to the Phonebook mode.

Table 1: Functionality mode URLs

Here, 'Server' is the name of the web server hosting the portal and 'PortalName' is the name of the Self-Service portal.

Modify web server settings

A Self-Service portal is hosted as a web application on the local IIS server.

Using the IIS tab, you can change:

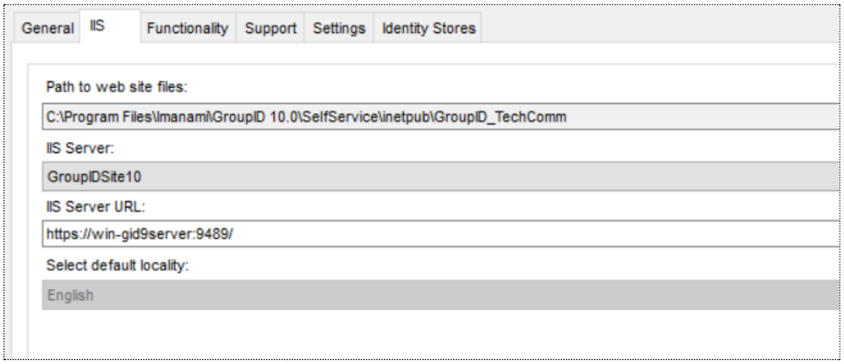
- The IIS website that hosts the portal
- The URL of the IIS server

You can also:

- View the physical path to the portal's folder
- View the default language used for serving the portal's content if the client browser is set to a language that is not supported by the Self-Service portal.

View the physical path to a portal's folder

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **IIS** tab.



Path to web site files:
C:\Program Files\Imanami\GroupID 10.0\SelfService\inetpub\GroupID_TechComm

IIS Server:
GroupIDSite10

IIS Server URL:
https://win-gid9server:9489/

Select default locality:
English

Figure 7: IIS tab

The **Path to web site files** box displays the path to the directory where the portal files are located on disk. This field is read-only.

Change the IIS site for a portal

A Self-Service portal is hosted as a web application in IIS on the GroupID server machine.

On the **IIS** tab, you can change the website in IIS that hosts a portal. In such an instance, the portal's URL(s) also change. You must provide the updated URL to users to enable them to access the portal. The URL(s) are displayed on the **General** tab (Figure 6).

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **IIS** tab (Figure 7).
3. The **IIS Server** list displays the IIS site that hosts the portal. You can select a different site from the list to move the portal's directory under it.

   The list displays the websites defined on the local IIS server.
4. On the toolbar, click Save 💾.

Change the base server URL for a portal

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **IIS** tab (Figure 7).
3. The **IIS Server URL** box displays the URL of the IIS web server. This URL is used in email notifications for linking back to portal pages.

If the name of the IIS web server changes, you can edit the URL in this box.

When you change this URL, the portal’s URL(s) also change. You must provide the updated URL to users to enable them to access the portal. The URL(s) are displayed on the **General** tab (Figure 6).

4. On the toolbar, click Save .

View the default language for a portal

A Self-Service portal detects the language settings of the web browser that is accessing it and attempts to serve the portal’s content in that language.

Supported languages are:

- Danish
- Dutch
- English
- Finnish
- French
- German
- Icelandic
- Italian
- Portuguese
- Spanish
- Swedish
- Turkish

However, if the portal does not support the browser’s language set or if it cannot detect it, the portal is loaded with the default language, which is English.

To view a portal’s default language:

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **IIS** tab (Figure 7).
3. The **Select default locality** box displays English as the default language for serving the portal’s content. This field is read-only.

Set a portal's functionality mode

Self-Service functionality modes allow you to expose only the required functionality in the portal. Mode-specific URLs determine the mode to launch the portal in.

The following table describes the modes in detail.

Functionality	Enterprise mode	Groups mode	My Profile mode
Group Management			
Create Groups	✓	✓	
Modify Group Properties	✓	✓	
Manage Group Membership	✓	✓	
Request to Join a Group	✓	✓	
Group Life Cycle and Attestation	✓	✓	
Expire and Renew Groups	✓	✓	
View My Groups History	✓	✓	
User Management			
Create User and Exchange Recipient	✓		
Modify / Update My Profile	✓		✓
Modify / Update My Direct Reports Profile	✓		
User Life Cycle and Attestation	✓		✓
User Profile Validation	✓		✓
Transfer / Terminate My Direct Reports	✓		✓
Change My Password	✓		✓
Reset other User's Password	✓		
View My History	✓		✓
View My Direct Reports History	✓		
Advanced Search	✓	✓	
Quick Search	✓	✓	
Groups Search	✓	✓	
Search Form and Search Result Customization	✓	✓	
Workflows	✓	✓	✓
Change Notifications	✓	✓	✓

Table 2: Functionality modes

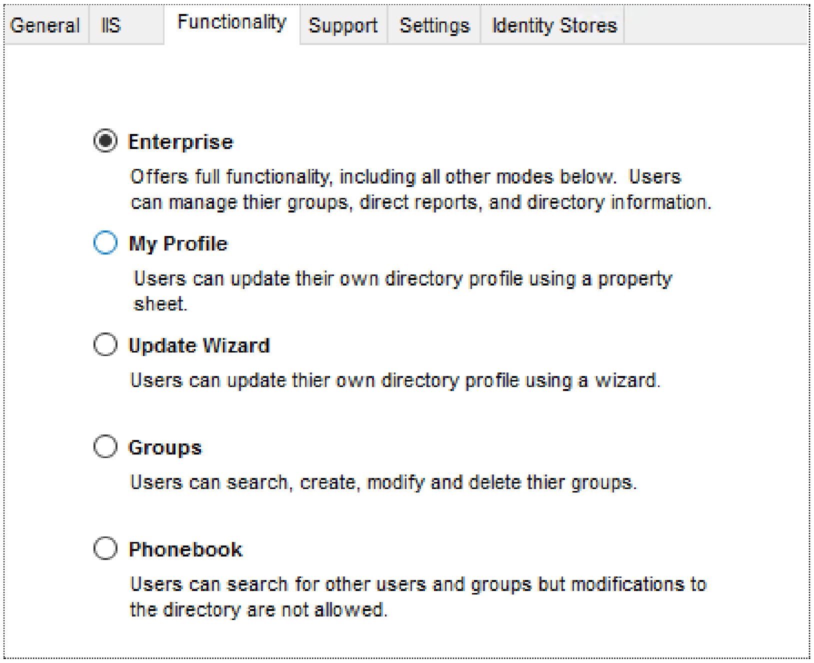
In the **Update Wizard** mode, users can update their directory profiles using a wizard.

In the **Phonebook** mode, users can search Users and Groups; this mode is read-only.

NOTE The available functionality in a mode can be trimmed further at granular level using role-based access. See Prerequisites for a portal.

Change the functionality mode of a portal

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server.**
2. Click the **Functionality** tab.



● **Enterprise**
Offers full functionality, including all other modes below. Users can manage thier groups, direct reports, and directory information.

○ **My Profile**
Users can update their own directory profile using a property sheet.

○ **Update Wizard**
Users can update thier own directory profile using a wizard.

○ **Groups**
Users can search, create, modify and delete thier groups.

○ **Phonebook**
Users can search for other users and groups but modifications to the directory are not allowed.

Figure 8: Functionality tab

3. Select the required functionality mode.
4. On the toolbar, click Save 💾.

NOTE When you change a portal's mode, the IIS session is reset and all users connected to the portal are logged out. When accessed again with the appropriate URL, the portal runs in the newly set mode.

The **General** tab (Figure 6) displays the URL for the functionality mode set on the **Functionality** tab. For the Enterprise mode, however, the **General** tab displays the URLs of all functionality modes.

NOTE You can override the default configurations of a functionality modes by customizing the portal's navigation bar. See Customize the Navigation bar on page 100.

Manage support settings

Portals include a **Contact** link and a **Help** icon on their web interface. The **Contact** link launches an email application to send an email to the administrator or Helpdesk for inquiries or feedback. The **Help** icon launches the online help for the portal in a new browser window. Both links are customizable and their target email address or web address can be changed using the **Support** tab (Figure 11).

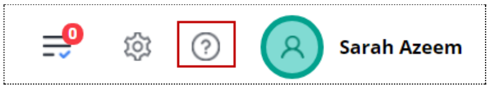
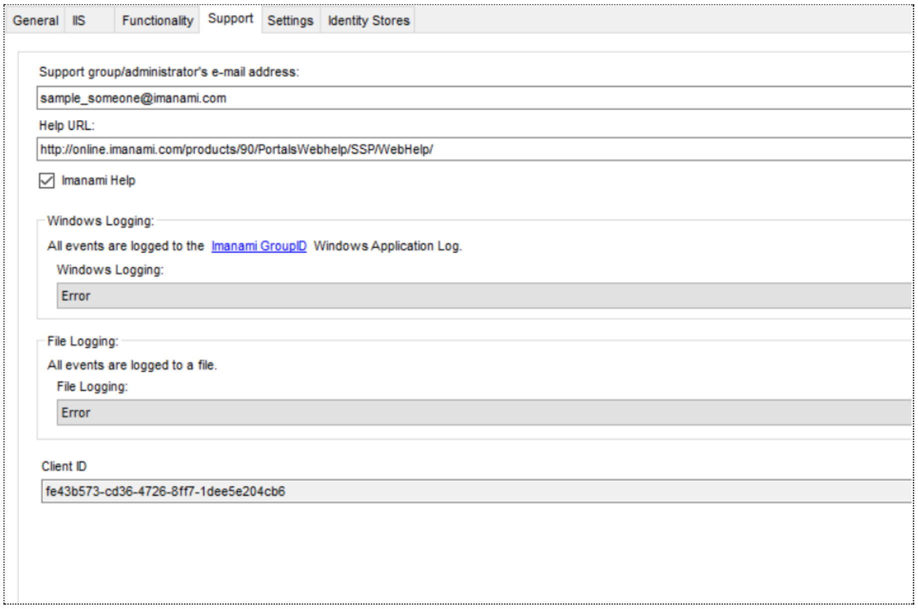


Figure 9: Help icon in the top right corner of the portal

Figure 10: Contact link at the bottom of the portal

Specify a different email address for the support group or administrator

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **Support** tab.



Support group/administrator's e-mail address:
sample_someone@imanami.com

Help URL:
http://online.imanami.com/products/90/PortalsWebhelp/SSP/WebHelp/

☑ Imanami Help

Windows Logging:
All events are logged to the Imanami GroupID Windows Application Log.
Windows Logging:
Error

File Logging:
All events are logged to a file.
File Logging:
Error

Client ID
fe43b573-cd36-4726-8ff7-1dee5e204cb6

Figure 11: Support tab

3. In the **Support group/administrator's email address** box, type the email address for the group, user, or contact that will be responsible for responding to requests or inquiries from portal users.

This box displays the support email address specified during portal creation.

This email address is mapped to the **Contact** link in the portal (Figure 10).

4. On the toolbar, click **Save** 💾.

Change the Help URL for a portal

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server.**
2. Click the **Support** tab (Figure 11).
3. In the **Help URL** box, type the address of the portal's help page or your company's internal support website, where portal users can find support material or report their problems.

   This box displays the help URL specified during portal creation (Figure 4).

   This URL is mapped to the **Help** icon in the portal (Figure 9).
4. Select the **Imanami Help** check box if the help URL points to the portal help. For GroupID 10, this URL is as: http://online.imanami.com/products/100/PortalsWebhelp/SSP/WebHelp/

   Clear this check box if the help URL points to help pages other than Imanami Help, such as when it points to your company's internal help page.
5. On the toolbar, click **Save** 💾.

View the client ID assigned to the portal

Every GroupID client (such as Automate, Management Shell, a Self-Service portal, etc.) is registered with a unique ID in the database, known as client ID.

This client ID is required while integrating a third-party single sign-on solution that support the SAML standard, into GroupID via any of its clients.

To view the portal's client ID:

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server.**
2. On the **Support** tab (Figure 11), the **Client ID** box displays the client ID assigned to the portal. It is read-only and can be copied for use.

Specify log settings

Self-Service uses Windows Logging and File Logging to monitor events from a Self-Service portal. You can specify the kind of information that you want to track for a portal by setting the logging level for each service.

Windows Logging

Windows Logging records Self-Service events in a centralized event log named Imanami GroupID that can be viewed from the Windows Event Viewer.

Windows logging groups events into five levels, depending on the type of information being captured. These levels are:

Level	Information Captured
1 - Failure Audit	Audited security access attempts that fail, such as when a user fails to log on to the portal.
2 - Success Audit	Audited security access attempts that succeed, such as when a user successfully logs on to the portal.
3 - Info	Successful operation of a module or functionality.
4 - Warn	Events that are not necessarily significant, but that could potentially cause a future problem, such as low disk space.
5 - Error	Significant problem, such as loss of data or functionality. Default setting.

Table 3: Windows Logging levels

Change the Windows Logging level

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server.**
2. Click the **Support** tab (Figure 11).
3. From the **Windows Logging** list, select the required logging level for the portal.
4. On the toolbar, click **Save** 💾.

Open Event Viewer from GroupID Management Console

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server.**
2. Click the **Support** tab (Figure 11).
3. In the **Windows Logging** area, click **Imanami GroupID**.

File Logging

File Logging records Self-Service events in log files that are created in a sub-folder within the root directory of each portal:

X:\Program Files\Imanami\GroupID 10.0\Self-Service\Inetpub\[Portal Name]\log\
(where X is the installation drive)

File Logging uses the Rollover Logging mechanism to log events. This mechanism logs events in a text file named **GroupID10-SSP**. When the file size reaches 100 MB, the rollover archives the log file in the same directory by replacing the file extension with the suffix **.Log.X** and then creating a new text file named **GroupID10-SSP**. X in .Log.X is a number from 1 to 10 representing the archiving order; the lower the number, the more recently the file was archived.

File Logging groups events into six levels, depending on the type of information being captured. These levels are:

Level	Information Captured
1 - All	Every event involving the Self-Service portal; this is the highest logging level.
2 - Debug	Fine-grained event information that is most useful for debugging the application.
3 - Info	Successful operations of a module or functionality.
4 - Warn	Events that are not necessarily significant, but that could potentially cause a future problem.
5 - Error	Errors that might still allow the Self-Service portal to continue running. Default level.
6 – Fatal	Severe errors that will presumably cause an operation to abort.
7 - Off	No events captured; turns off file logging.

Table 4: File Logging levels

Change the File Logging level

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server.**
2. Click the **Support** tab (Figure 11).
3. From the **File Logging** list, select the required logging level for the portal.
4. On the toolbar, click **Save** 💾.

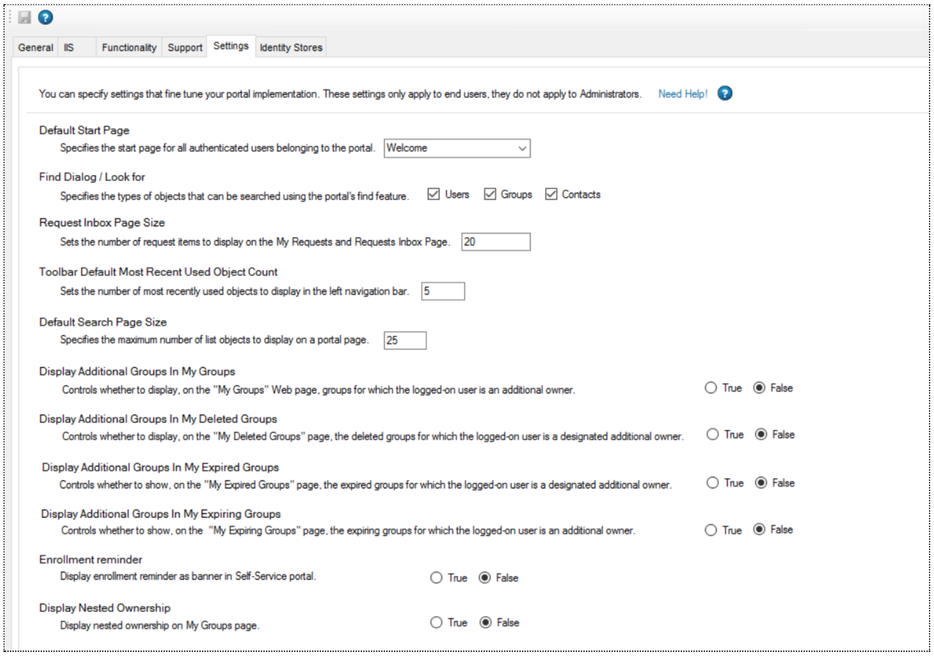
Apply advanced settings to a portal

Self-Service supports advanced settings that allow you to customize the functionality and appearance of a portal.

Using the **Settings** tab, you can specify advanced settings for a Self-Service portal. Some settings are available in all user interfaces of the portal, while others are specific to a particular one.

Modify a setting

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **Settings** tab.



You can specify settings that fine tune your portal implementation. These settings only apply to end users, they do not apply to Administrators.

Default Start Page
Specifies the start page for all authenticated users belonging to the portal. Welcome

Find Dialog / Look for
Specifies the types of objects that can be searched using the portal's find feature. ☑ Users ☑ Groups ☑ Contacts

Request Inbox Page Size
Sets the number of request items to display on the My Requests and Requests Inbox Page. 20

Toolbar Default Most Recent Used Object Count
Sets the number of most recently used objects to display in the left navigation bar. 5

Default Search Page Size
Specifies the maximum number of list objects to display on a portal page. 25

Display Additional Groups In My Groups
Controls whether to display, on the "My Groups" Web page, groups for which the logged-on user is an additional owner. ○ True ● False

Display Additional Groups In My Deleted Groups
Controls whether to display, on the "My Deleted Groups" page, the deleted groups for which the logged-on user is a designated additional owner. ○ True ● False

Display Additional Groups In My Expired Groups
Controls whether to show, on the "My Expired Groups" page, the expired groups for which the logged-on user is a designated additional owner. ○ True ● False

Display Additional Groups In My Expiring Groups
Controls whether to show, on the "My Expiring Groups" page, the expiring groups for which the logged-on user is an additional owner. ○ True ● False

Enrollment reminder
Display enrollment reminder as banner in Self-Service portal. ○ True ● False

Display Nested Ownership
Display nested ownership on My Groups page. ○ True ● False

Figure 12: Settings tab

3. Change the required setting.
4. On the toolbar, click **Save** 💾.

Advanced settings for a Self-Service portal

On the **Settings** tab (Figure 12), you can specify settings that fine-tune your portal implementation. These settings only apply to end users; they do not apply to administrators.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Default Start Page</td><td>
<p>Specify the start page for the functionality mode selected on the <b>Functionality</b> tab (Figure 8). When a user logs into the portal, he or she is redirected to the start page.</p>
<p>Each functionality mode has a default start page that is displayed if you do not specify a value in the <b>Default Start Page</b> list. Knowing the portal’s functionality mode, you can change its start page to the pages listed:</p>
<table>
<tr><th>Functionality Mode</th><th>Page Title</th></tr>
<tr><td><b>Enterprise</b></td><td>Welcome</td></tr>
<tr><td></td><td>Group Search</td></tr>
<tr><td></td><td>My Groups</td></tr>
<tr><td></td><td>My Memberships</td></tr>
<tr><td></td><td>My Expired Groups</td></tr>
<tr><td></td><td>My Expiring Groups</td></tr>
<tr><td></td><td>My Deleted Groups</td></tr>
<tr><td></td><td>Search</td></tr>
<tr><td></td><td>My Profile</td></tr>
<tr><td></td><td>My Direct Reports</td></tr>
<tr><td></td><td>Change My Password</td></tr>
<tr><td></td><td>Reset Password</td></tr>
<tr><td></td><td>Request Inbox</td></tr>
<tr><td></td><td>My Requests</td></tr>
<tr><td></td><td>Organizational Hierarchy</td></tr>
<tr><td><b>Groups</b></td><td>My Groups</td></tr>
<tr><td></td><td>Welcome</td></tr>
<tr><td></td><td>Group Search</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>My Memberships</td></tr>
<tr><td></td><td>My Expired Groups</td></tr>
<tr><td></td><td>My Expiring Groups</td></tr>
<tr><td></td><td>My Deleted Groups</td></tr>
<tr><td></td><td>Request Inbox</td></tr>
<tr><td></td><td>My Requests</td></tr>
<tr><td><b>My Profile</b></td><td>My Profile</td></tr>
<tr><td></td><td>Welcome</td></tr>
<tr><td></td><td>Request Inbox</td></tr>
<tr><td></td><td>My Requests</td></tr>
<tr><td></td><td>Organizational Hierarchy</td></tr>
<tr><td><b>Phonebook</b></td><td>Search</td></tr>
<tr><td><b>Update Wizard</b></td><td>Update Wizard</td></tr>
</table>
<p><b>Tip</b>: If, after changing the start page, the portal does not open to the new start page, check that the functionality mode for the new start page is the same as the portal mode.</p>
<p>NOTE Individual users can personalize this setting through the <i>Settings</i> option in the portal. The value set here applies to users who have not changed it.</p>
</td></tr>
<tr><td>Find Dialog / Look For</td><td>
<p>Select the <b>Users</b>, <b>Contacts</b>, and/or <b>Groups</b> check boxes to specify the type of objects that can be searched using the portal’s <b>Find</b> dialog box.</p>
<p>You can launch the <b>Find</b> dialog box from multiple portal pages to search for objects to designate as owners, managers, additional owners, members, and more.</p>
<p>By default, the <b>Find</b> dialog box searches for all types of objects, including users, contacts, and groups. Use this setting to limit the <i>Find</i> feature to specific object types. For example, select the <b>Users</b> check box to limit users to search for the User object type only.</p>
<p>The <i>contact</i> object type is not supported in a Microsoft Azure based identity store.</p>
</td></tr>
</table>

Setting	Description
Request Inbox Page Size	In the **Request Inbox Page Size** box, specify a value in the range, 1 to 99999, to set the number of workflow request items to display on the **My Requests** and **Request Inbox** pages of the portal. Users access the **My Requests** and **Request Inbox** pages through the portal’s left navigation bar. By default, both pages display 20 request items at a time. You can use any value from 1 to 99999. Setting zero or a negative number displays all workflow requests. When setting the page size, consider the volume of request traffic generated by your users. Showing all or a large number of workflow requests increases page-load time and response times.
Toolbar Default Most Recent Used Object Count	In the **Toolbar Default Most Recent Used Object Count** box, specify a value in the range, 1 to 9, to set the number of most recently used objects to display in the left navigation bar of the portal. The left navigation bar has a **Recent** section that shows objects that are recently viewed by the logged-on user. Clicking an object shows the properties of that object. By default, the portal shows five of the most recently viewed objects. Using this setting, you can change it to a number from 1 to 9. NOTE Individual users can personalize this setting through the *Settings* option in the portal. The value set here applies to users who have not changed it.
Default Search Page Size	In the **Default Search Page Size** box, specify a value in the range, 1 to 999, to set the maximum number of list objects to display on a portal page. Many Self-Service portal pages display lists of objects. Examples are the **My Groups** and **My Memberships** pages. By default, all list views display 25 objects per page. For the remaining objects, the page numbers are given at the bottom of each page using which users can move through the other objects. When setting the page size, consider available network bandwidth and server resources, as the greater the number,

Setting	Description
	the higher the potential for increased page load time and slow response time. NOTE Individual users can personalize this setting through the *Settings* option in the portal. The value set here applies to users who have not changed it.
Display Additional Groups In My Groups	This setting controls whether to display, on the portal’s **My Groups** page, groups for which the logged-on user is an additional owner. • Select the **True** option button to display groups for which the logged-on user is a primary or additional owner. • Select the **False** option button to display groups for which the logged-on user is the primary owner. Additional ownership is not displayed. NOTE Individual users can personalize this setting through the *Settings* option in the portal. The value set here applies to users who have not changed it.
Display Additional Groups In My Deleted Groups	This setting controls whether to display, on the portal’s **My Deleted Groups** page, the deleted groups for which the logged-on user is an additional owner. • Select the **True** option button to display deleted groups for which the logged-on user is a primary or additional owner. • Select the **False** option button to display deleted groups for which the logged-on user is the primary owner. Additional ownership is not displayed. NOTE Individual users can personalize this setting through the *Settings* option in the portal. The value set here applies to users who have not changed it.
Display Additional Groups In My Expired Groups	This setting controls whether to show, on the porta’s **My Expired Groups** page, the expired groups for which the logged-on user is an additional owner.

Setting	Description
	• Select the **True** option button to display expired groups for which the logged-on user is a primary or additional owner. • Select the **False** option button to display expired groups for which the logged-on user is the primary owner. Additional ownership is not displayed. NOTE Individual users can personalize this setting through the *Settings* option in the portal. The value set here applies to users who have not changed it.
Display Additional Groups In My Expiring Groups	This setting controls whether to display, on the portal’s **My Expiring Groups** page, the expiring groups for which the logged-on user is an additional owner. • Select the **True** option button to display expiring groups for which the logged-on user is a primary or additional owner. • Select the **False** option button to display expiring groups for which the logged-on user is the primary owner. Additional ownership is not displayed. NOTE Individual users can personalize this setting through the *Settings* option in the portal. The value set here applies to users who have not changed it.
Enrollment reminder	This setting controls whether to display a reminder with redirect to the **Enroll My Account** page, when an unenrolled user logs on to the Self-Service portal. • Selecting the **True** option button initiates these events whenever a user who has not enrolled their account in GroupID logs on to the Self-Service portal: i. The Self-Service Welcome page displays an information bar requesting that the user enroll their account. (The user can ignore the request.) ii. Clicking the bar redirects the user to the **Enroll My Account** page, where the user can enroll their account. • Selecting the **False** option button does not display the information bar for account enrollment.

Setting	Description
Display Nested Ownership	This setting controls whether to display nested ownership on the portal's **My Groups** page. • With the **False** option button selected, the **My Groups** page will display groups that have the logged-in user set as the primary owner, additional owner or Exchange additional owner. • With the **True** option button selected, the **My Groups** page will display groups with nested ownership as well. Suppose the logged-in user is a member of Group C, and Group C is an owner of Group B. With the **True** option button selected, the **My Groups** page also shows Group B since the logged-in user is its nested owner.
Use Contains Filter	Specify the filter that search pages should use while searching objects. • By default, the **False** option button is selected, which implies that when a search parameter is entered on any of the search pages of the portal, it searches the directory on the "starts with" basis. For example, if the user enters "Sam" in the **First Name** box of the **Advanced Search** page, the portal searches the directory for all objects whose first name starts with "Sam". • When you select the **True** option button, it changes the filter to "Contains", which returns objects with the string "Sam" anywhere in the first name.
Auto Complete Quick Search	Specify whether to turn on search predictions for the portal's Quick search. Search predictions are possible search terms that are related to the term that the user is typing as search string. • Select the **True** option button to turn on search predictions for Quick search in the portal. This will show matched items as the user types the search string for Quick search. • Select the **False** option button to turn off search predictions.
Hide Help Link	This setting controls whether to display the **Help** link in the portal.

Setting	Description
	A Self-Service portal displays the **Help** link on its web interface. This link opens the online help for the portal in a new browser window, where portal users can find support material or report their problems. • Select the **True** option button to display the **Help** link in the portal. • Select the **False** option button to hide the **Help** link in the portal. In this case, users will not be able to access the portal's help pages.
Suggest Owner/Manager	Set the Self-Service portal to suggest owners for orphan groups and managers for users without managers. • Select the **True** option button to allow GroupID to suggest a primary owner for an orphan group (on the **Owner** tab in group properties) and a primary manager for a user without one (on the **Organization** tab in user properties). • The manager is suggested with respect to the user's department; if the department is not specified, the manager suggestion does not work. • The owner is suggested with respect to the group's membership; GroupID checks the managers of group members and the user who shows up most as a manager is suggested as the group owner. This user may or may not be a member of the group. For example, when 40 members of Group A have User A as their manager and 38 members have User B as a manager, User A is suggested as Group A's primary owner. User A may not necessarily be a member of Group A. • Select the **False** option button to turn off the owner/manager suggestion feature.
Search Default	Set the default selection in the Search list box. The Search list box is available on the toolbar of all Search pages and a few other pages of the portal.

Setting	Description
	From the **Search Default** drop-down list, select one of the following options to set the search scope for the Search list box: - **Global Catalog**: Selecting this option shows "Entire Directory" selected in the Search list box. Also, expanding the list displays the Entire Directory check box selected instead of the logged-on domain. - **Domain**: The Search list box shows the domain of the connected identity store. The user can expand the list to select any other option. Select the **Global Catalog** option when most of the searches that portal users perform are based on the global catalog.
Sort Search	Set the field name (column header) by which the search results should be sorted. The *Sort Search* setting applies to all search result pages in the portal, such as the Default Search, Group Search and Find dialog box searches. In the **Sort Search** field, specify an attribute by which the search results should be sorted. By default, the displayName attribute is specified, indicating that objects on all pages are sorted by the displayName attribute in ascending order.
Portal Logo	Use the default Self-Service logo or a logo of your choice for display in the portal. - Use **Browse** to select and upload a logo of your choice for display in the portal. - Use **Reset** to revert to the default logo.

Table 5: Advanced settings for a Self-Service portal

Link a portal to identity stores

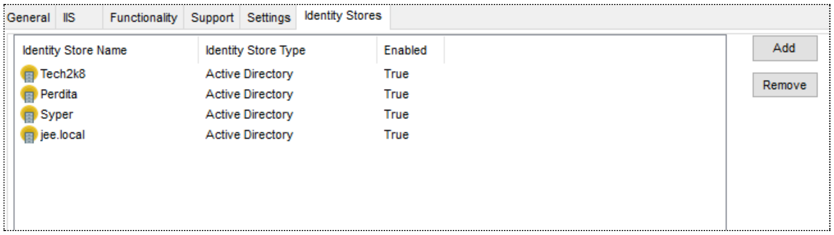
You must associate a Self-Service portal with one or more identity stores. When logging into the portal, a user must select an identity store to connect to, so that he or she can perform group and identity management operations for that identity store.

On the **Identity Stores** tab, you can:

- View the identity stores associated with the portal. You can also view the data store type the identity store is created for, and whether the identity store is enabled.
- Associate another identity store with the portal.
- Dissociate an identity store from the portal, so that the portal cannot connect to it.

Associate an identity store with a portal

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **Identity Stores** tab.



Identity Store Name	Identity Store Type	Enabled
Tech2k8	Active Directory	True
Perdita	Active Directory	True
Syper	Active Directory	True
jee.local	Active Directory	True

Figure 13: Identity Stores tab

3. Click **Add**.
4. On the **Add Identity Stores** dialog box, select the check box for an identity store to associate it with the portal.
5. Click **OK** to close the **Add Identity Stores** dialog box.
6. On the toolbar, click **Save** .

Users can connect the portal only to an enabled identity store. An identity store is enabled if the **Enabled** column displays **True** as its value.

Dissociate an identity store from a porta

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Server**.
2. Click the **Identity Stores** tab (Figure 13).
3. Select an identity store to dissociate it from the portal and click **Remove**.
4. On the toolbar, click **Save** .

Chapter 4 - Working with Display Types

The Self-Service portal offers an intuitive front-end to users for adding and updating values for schema attributes. Using display types, you can specify data input fields on this front-end and hook up each field to the appropriate schema attribute.

Each schema attribute requires a value of a certain type. Some attributes require a single string value (such as the Active Directory attributes, **name** and **sAMAccountName**) while others can accept multiple values (such as the Active Directory attribute, **proxyAddress**). Some can accept only (one or more) distinguished names (DN) (such as the Active Directory attributes, **members** and **memberOf**) while others allow only Boolean values (true or false), (such as the Active Directory attributes, **hideDLMembership** and **isDeleted**).

To ensure that portal users update these attributes in the same manner as supported by the directory, display types play an important role.

A display type enables you to define: the user interface element to be used for an attribute in the portal (for example, text box, drop-down list, check box, etc.). This user interface element must support the type of data that can be entered as the attribute value, so that users enter proper data through the portal.

Display Type Categories

Self-Service display types support almost all types of schema attributes (single-valued, multi-valued, Boolean, distinguished name, and more). Based on their characteristics and customization options, display types are divided into two categories:

Basic types

You can link a basic display type to a schema attribute straight away. Basic display types are:

- Text box
- Password
- Multi-value
- Check box

- DN
- DNs

Custom types

Some display types cannot be linked to schema attributes straight away; they must be customized before you can apply them to an attribute.

Display types that require customization are:

- Text box - this display type can be used directly with an attribute, but if you want to apply data validation checks to it, you must convert it to a custom display type.
- Drop-down list
- Linked-field drop-down list
- Image
- Grid
- Radio
- Multiline text box
- Linked combo

For example, you can define a simple text box type for a telephone number field and apply a validation rule so that it accepts phone numbers in US format only. Another example is defining a drop-down list display type containing a list of the departments in your organization or creating a linked field drop-down list type where selecting the office address populates its phone number and fax number.

The default portal template uses several predefined custom display types. See Defining and using custom display types on page 36 to add more display types as needed.

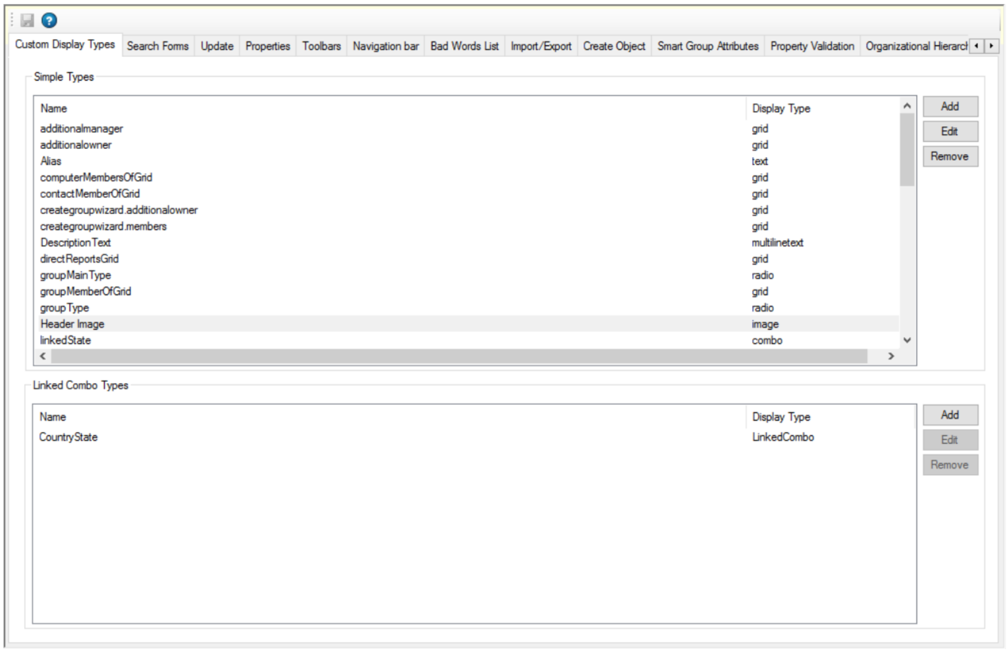
How to implement display types

On the **Search Forms**, **Properties**, **Update**, **Create Object,** and **Property Validation** tabs of the **Designs** node, you can select a schema attribute and a display type to link them.

On linking, the display type is rendered on the portal page; through it, users can view or specify a value for the linked attribute.

A Self-Service portal comes with a default design template, where a few data input fields are available in the portal. These fields involve the use of both basic and custom display types. You can use these predefined display types to add new fields to the portal or define your own custom display types.

Use the **Custom Display Types** tab in the **Designs** node to view a list of all predefined custom display types. You can also define new custom display types.



Simple Types

Name	Display Type
additionalmanager	grid
additionalowner	grid
Alias	text
computerMembersOfGrid	grid
contactMemberOfGrid	grid
creategroupwizard.additionalowner	grid
creategroupwizard.members	grid
DescriptionText	multilinetext
directReportsGrid	grid
groupMainType	radio
groupMemberOfGrid	grid
groupType	radio
Header Image	image
linkedState	combo

Linked Combo Types

Name	Display Type
CountryState	LinkedCombo

Figure 14: Design node – Custom Display Types tab

Basic display types

Basic display types encompass six basic controls:

- Text box
- Password
- Multi-value
- Check box
- DN
- DNs

You can link these basic display type directly to a schema attribute; they require no customization.

Text box

Use a text box to collect and display a single value for an attribute. You can link it directly to a schema attribute. However, if you want to apply additional rules to it, such as assigning a default value or implementing a regular expression to validate the data entered, you must create a custom display type from this basic type. See Define a Text box display type on page 37.

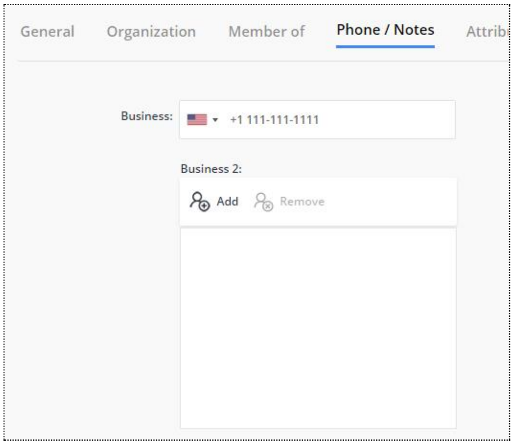
Password

Use the password display type with schema attributes containing confidential information. The user interface element is displayed as a text box on the portal with bullets or asterisks in place of text.

Multi-value

Use the multi-value display type for schema attributes that can accept multiple string values.

The user interface elements set to multi-value type appear on the portal as:



Business: +1 111-111-1111

Business 2:

Figure 15: Multi-value display type applied on the Business 2 field

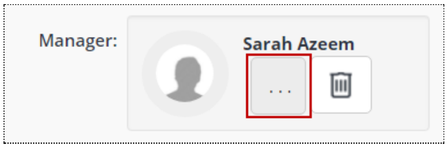
Clicking Add launches a dialog box where you can add new values.

Check box

Use a check box for schema attributes that can only accept true or false values, such as the Active Directory attributes, reportToOwner, reportToOriginator, and oOFReplyToOriginator.

DN

Use the DN type for schema attributes that accept a single distinguished name for their value, such as the Active Directory attributes, **Assistant** and **altRecipient**. The user interface element for this display type appears as a button that launches the **Find** dialog box where users can add or remove the desired object. It is as shown below:



Manager: Sarah Azeem

Figure 16: DN display type applied on the Manager field

DNs

Use the DNs display type for schema attributes that can accept multiple distinguished names, for example, the Active Directory attributes, member and memberOf. The user interface element for this display type is the same as for a multi-value display type (Figure 15).

Clicking Add launches the **Find** dialog box where you can search and select the desired objects.

Defining and using custom display types

Self-Service, by default, provides several predefined custom display types, that are already used in the default portal template.

To customize the default template, you can use the predefined display types or define new custom display types. Custom display types can then be linked to different fields (schema attributes) on the **Search Forms**, **Update**, **Properties**, **Create Object** and **Property Validation** tabs.

Display types that require customization are:

- Text box - this display type can be used directly with an attribute, but if you want to apply data validation checks to it, you must convert it to a custom display type.
- Drop-down list
- Linked-field drop-down list
- Image

- Grid
- Radio
- Multiline text box
- Linked combo

Define a Text box display type

A text box display type can be used without customization, but you must customize it in the following cases:

- When you want to specify a default value for it.
- When you want to place a check to validate the data entered in the text box. This can be done by defining a regular expression for the text box.

  A regular expression is a pattern of text that consists of ordinary characters (for example, letters a through z) and special characters, known as metacharacters. You can use regular expressions to ensure that users enter data in an input field according to a standard pattern. For example, the regular expression for a US phone number of the pattern: (555) 123-4567 will be: ^\(\d\d\d\) \d\d\d-\d\d\d\d.

  Use the links below to find additional information about regular expressions and their syntax:

  - ✓ Introduction to Regular Expressions
  - ✓ Regular Expression Syntax Reference
- When you want to enforce the user to enter a unique value for the field.

A few text box types predefined in the default portal template are:

	Display Type Name	Default Value	Regular Expression	Regular Expression Example
1.	maskPhoneUSwithExt	None	^\(\d\d\d\) \d\d\d-\d\d\d\d x\d\d\d$	(555) 123-4567 x890
2.	SmtpEmail	None	([^A-Za-z0-9!#$%&'*+-/=?.^_`{\|}~\u00A1-\u00FF])\|([.]{2})\|(^(\.))\|((\.)$)	someone@imanami.com

3.	maskPhoneUS	None	^\(\d\d\d\) \d\d\d-\d\d\d\d$	(555) 123-4567
4.	maskEmailAddress	None	^([a-zA-Z0-9_\-\.]+)@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.)|(([a-zA-Z0-9\-]+\.)+))([a-zA-Z]{2,4}|[0-9]{1,3})(\]?)$	user@domain.com
5.	maskZipCode	None	\d{5}(-\d{4})?	NNNNN-NNNN

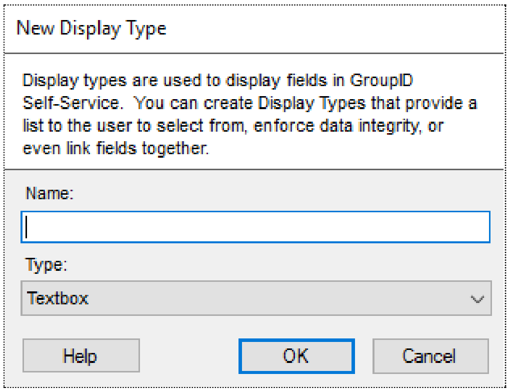
Table 6: Some predefined text box display types

You can define more custom text box display types, if required.

Define a text box display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. On the **Custom Display Types** tab (Figure 14), click **Add** in the **Simple Types** area.



New Display Type

Display types are used to display fields in GroupID Self-Service. You can create Display Types that provide a list to the user to select from, enforce data integrity, or even link fields together.

Name:

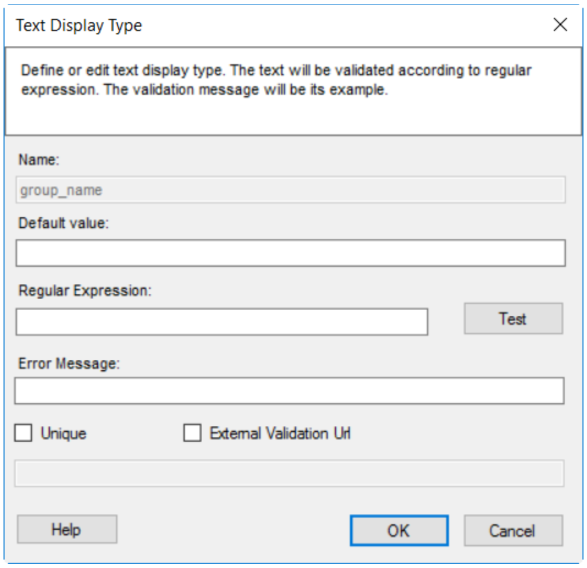
Type: Textbox

Figure 17: New Display Type dialog box

4. Enter a name for the display type in the **Name** box.

   You cannot change the name of a custom display type once you have created it.

5. From the **Type** list, select *Textbox* and click **OK**.



Define or edit text display type. The text will be validated according to regular expression. The validation message will be its example.

Name: group_name

Figure 18: Text Display Type dialog box

6. Specify a value in the **Default Value** box to set it as the default value for the text box.

   Users can modify this value in the portal.

7. In the **Regular Expression** box, type a regular expression to use for validating data that would be entered in the text box using the portal. For example, for Social Security number validation, type the expression **^\d{3}-\d{2}-\d{4}$**.

   Leave this box blank if you do not want to apply any validation rule to the data.

   a. Click **Test** to check if the regular expression is valid.

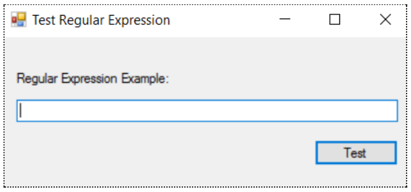


Figure 19: Test Regular Expression dialog box

   In the **Regular Expression Example** box, type an example that satisfies the regular expression and click **Test**.

   For example, you can type **111-22-3333** for a regular expression that is meant to validate the Social Security number.

b. In the **Error Message** box, type the text that would be displayed as an error message when a portal user enters data in the text box that does not conform to the regular expression.

8. You can place a real-time validation check to ensure that users enter a unique value for the field. GroupID can look up the value for uniqueness in the directory or an external data source.

   The portal would prevent the user from proceeding unless a unique value is provided.

   - Select the **Unique** check box to enforce the user to enter a value that is unique for the field (attribute) in the directory.

   OR

   - You can also use an external data source, such as an Excel file, to validate the uniqueness of the value in real time. An API is provided to link to that data source.

     Select the **External Validation URL** check box and enter the URL of the API in the box below.

   Suppose you apply this text box display type to the *group name* field on the *group creation* wizard. When a user enters a name while creating a group, the portal will look up this name for uniqueness in the directory/external data source in real time and display an error message if it is not unique.

9. Click **OK** to close the **Text Display Type** dialog box.

10. On the toolbar, click **Save** 💾.

You can now link this customized text box display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which it is displayed on the relevant portal page.

External API reference

The external API for real-time validation should receive the following parameters:

Parameter	Description
objectType	The type of object the user is creating or updating (for example, group, user).
attributeName	The name of the attribute the user is updating (for example, name, first name, logon name).

attributeValue	The attribute value that needs to be validated.
objectID	If an existing user is being updated, the ID of that user is sent; else it is an empty string.

Table 7: Input parameters

The API returns the following parameters:

Parameter	Description
status	Should be ‘true’ (when the attribute value is unique) or ‘false’ (when the attribute value is not unique).
message	(Optional) For the ‘false’ status, you can return an error message in this parameter, that is displayed to the user.
data	Not in use.

Table 8: Output parameters

NOTE Data should be in JSON format.

Define a Drop-down List display type

Use the drop-down list display type to give users a list of options to select from.

To create a drop-down list, you must create a custom type for it where you specify the values (options) to display in the list. This custom type can then be linked to a schema attribute.

The options in the list are the different values that can be selected for the schema attribute you associate with this display type.

A few drop-down list display types are predefined in the default portal template. The following table lists some of these along with the list values.

	Display Type Name	Default Value	Values
1.	lstSecurity	Private: Closed Membership	• Public • Semi-Private: Owner Must Approve • Private: Closed Membership
2.	lstGroupScope	Universal Group	• Domain Local • Global Group • Universal Group
3.	lstGroupType	None	• Security • Distribution
4.	membershipeditlist	None	• Perpetual

	Display Type Name	Default Value	Values
			• Temporary Member • Addition Pending • Temporary Removed • Removal Pending
5.	lstCountry	None	The list of all countries.
6.	lstState	None	The list of all states in the US.
7.	lstStateProvince	None	The list of all states and provinces in the US.
8.	lstProvince	None	The list of all provinces in the US.
9.	linkedState	None	None

Table 9: Some predefined drop-down list display types

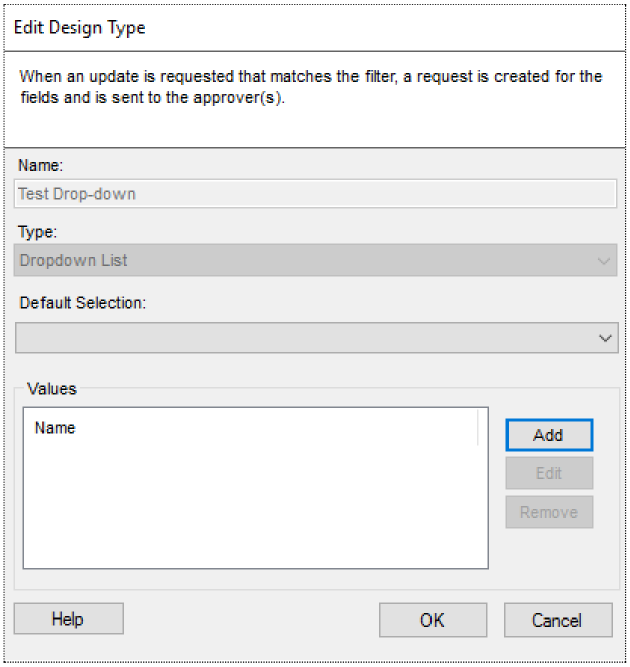
You can define more custom drop-down display types, if required.

Define a drop-down list display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. On the **Custom Display Types** tab (Figure 14), click **Add** in the **Simple Types** area. The **New Display Type** dialog box is displayed (Figure 17).
4. Enter a name for the display type and select **Dropdown List** from the **Type** list.

   You cannot change the name of a custom display type once you have created it.
5. Click **OK**.
   The **Edit Design Type** dialog box is displayed:



Edit Design Type

When an update is requested that matches the filter, a request is created for the fields and is sent to the approver(s).

Name:
Test Drop-down

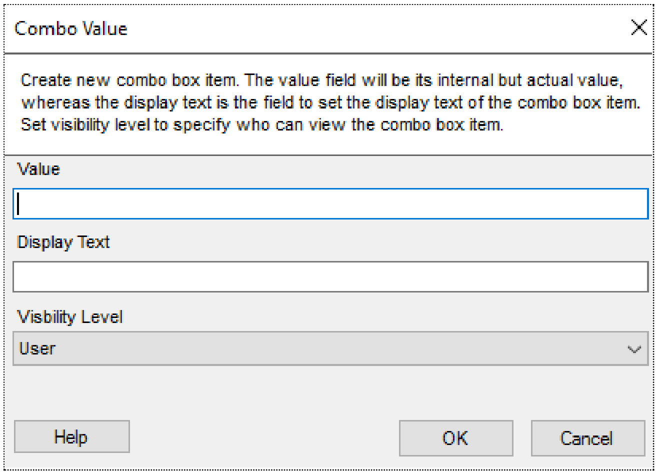
Type:
Dropdown List

Default Selection:

Figure 20: Edit Design Type dialog box

6. Use the **Values** area to specify the values to be displayed in the drop-down list.

   To add a value, click **Add**.



Combo Value

Create new combo box item. The value field will be its internal but actual value, whereas the display text is the field to set the display text of the combo box item. Set visibility level to specify who can view the combo box item.

Value

Display Text

Visbility Level
User

Figure 21: Combo Value dialog box

7. On the **Combo Value** dialog box, specify a value and a display text for that value in the respective boxes.

   The display text would be displayed in the drop-down list, while the value will be saved in the directory or database when a user selects the display text from the drop-down list in the portal.

(The value would be saved in the directory or database depending on whether the drop-down list display type is mapped to a directory attribute or a database attribute respectively.)

8. From the **Visibility Level** drop-down list, select a security role. The value would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   Select *Never* to hide the value from all users.

   The visibility level determines the security role(s) whose members can view the value in the drop-down list. The **Visibility Level** list contains all security roles defined for the identity store.

9. Click **OK**. The new value is listed in the **Values** area (Figure 20), represented by its display text.

10. Repeat steps 7 to 10 to define a new value in the list.

    - To edit a value, select it and click **Edit**.
    - To remove a value from the lost, select it and click **Remove**.

11. Select a value from the **Default Selection** list to set it as the default value to be displayed in the drop-down list on the portal.

    The **Default Selection** list contains all values you have defined in the **Values** area.

12. Click **OK** to close the **Edit Design Type** dialog box.

13. On the toolbar, click **Save** 💾.

You can now link this customized drop-down list display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which it is displayed on the relevant portal page.

Define a Linked Field Drop-down List display type

A linked field drop-down list is displayed on the portal as a drop-down list with multiple values. When a user selects a value, all fields linked to that value are auto-populated. However, these fields remain isolated, and are not displayed on the portal.

Use a linked field drop-down list, for example, when you want the Office Address, Business Phone Number, Fax Number and Email fields to be auto-populated when a user selects his or her office name from a drop-down list. Here, <office name> is the key value while Office Address, Business Phone Number, Fax Number and Email are its (isolated) linked fields.

To define a linked field drop-down list,

- Specify a value, called a key value.
- Link schema attributes (fields) with this key value. For each attribute that you link, you must also provide a value.

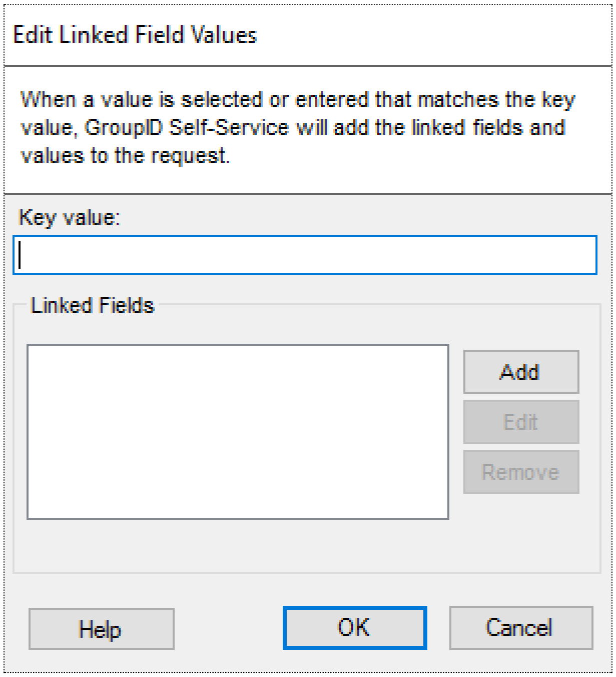
: Define a linked field drop-down list display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Custom Display Types** tab (Figure 14).
4. In the **Simple Types** area, click **Add**.
   The **New Display Type** dialog box is displayed (Figure 17).
5. Enter a name for the display type and select **Linked Field Dropdown List** from the **Type** list.

   You cannot change the name of a custom display type once you have created it.
6. Click **OK**.
   The **Edit Design Type** dialog box (Figure 20) is displayed.
7. Use the **Values** area to specify the key values to appear in the drop-down list.

   To add a key value, click **Add**.


Edit Linked Field Values

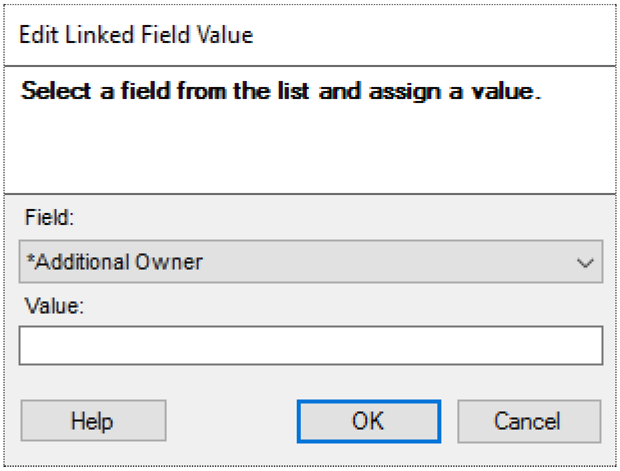
When a value is selected or entered that matches the key value, GroupID Self-Service will add the linked fields and values to the request.

Figure 22: Linked Field Values dialog box

8. In the **Key value** box, type a key value
   A key value is one that is displayed in the drop-down list on the portal, and when selected, auto populates the isolated linked fields.

9. The **Linked Fields** area is for specifying the fields to link with this key value. Simply select a schema attribute (field) and specify a value for it.

   Click **Add**; the **Edit Linked Field Value** dialog box is displayed.


Edit Linked Field Value

Select a field from the list and assign a value.

Field: *Additional Owner

Figure 23: Edit Linked Field Value dialog box

a. From the **Field** drop-down list, select a schema attribute that you want to create as a linked field for the key value.

b. In the **Value** box, type a value for the attribute.

c. Click **OK**.

   The linked field gets listed in the **Linked Fields** area on the **Linked Field Values** dialog box (Figure 22).

10. After defining the linked fields as required, click **OK** on the **Linked Field Values** dialog box (Figure 22).

    The key value is displayed in the **Values** area on the **Edit Design Type** dialog box (Figure 20).

11. Repeat steps 7 to 10 to define a new key value in the list.

    - To edit a key value, select it and click **Edit**.
    - To remove a key value from the lost, select it and click **Remove**.

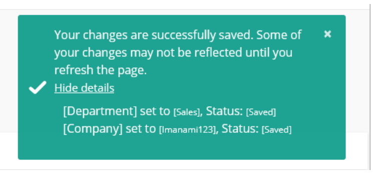
12. Select a key value from the **Default Selection** list to set it as the default value to be displayed in the drop-down list on the portal.

    The **Default Selection** list contains all key values you have defined in the **Values** area.

13. Click **OK** to close the **Edit Design Type** dialog box.

14. On the toolbar, click **Save** .

You can now link this customized linked field drop-down display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which it is displayed on the relevant portal page. On selecting a value from this list and saving the information, the isolated linked fields are auto-populated with the predefined values and a message, similar to the following, is displayed.



Your changes are successfully saved. Some of your changes may not be reflected until you refresh the page.

Hide details

[Department] set to [Sales], Status: [Saved]
[Company] set to [Imanami123], Status: [Saved]

Figure 24: Linked field drop-down list save message

Here, **Department** is the key value. Selecting it from the drop-down list populates the **Company** field with the predefined value.

Define an Image display type

Use the image display type for schema attributes of the User object type that can store image data. The following table lists the attributes for Active Directory.

Active Directory Attribute	CN	Description	Max. Image Size (in KB)
jpegPhoto	JpegPhoto	Stores one or more images of a user in JPEG File Interchange Format (JFIF). The image saved in this attribute is mainly used by SharePoint.	10240
Photo	Photo	An object encoded in G3 fax as explained in recommendation T.4, with an ASN.1 wrapper to make it compatible with an X.400 BodyPart as defined in X.420.	N.A.
thumbnailPhoto	Picture	An image of the user for display in Outlook. A space-efficient format like JPEG or GIF is recommended.	100
thumbnailLogo	Logo	A small-sized image; the user's logo.	32

Table 10: Active Directory attributes for the Image display type

To define an image display type, you have to specify the image's display dimensions (height and width), that would be used to display the image on the portal. You also have to specify the maximum image size that can be uploaded for this display type.

The following figure shows an example of the custom image type rendered on a portal page.

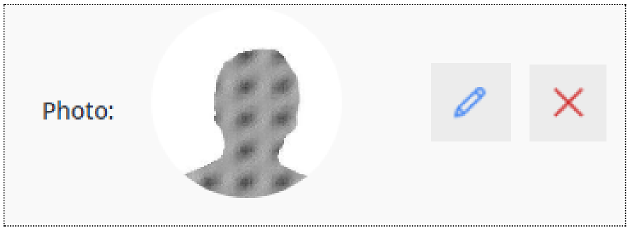


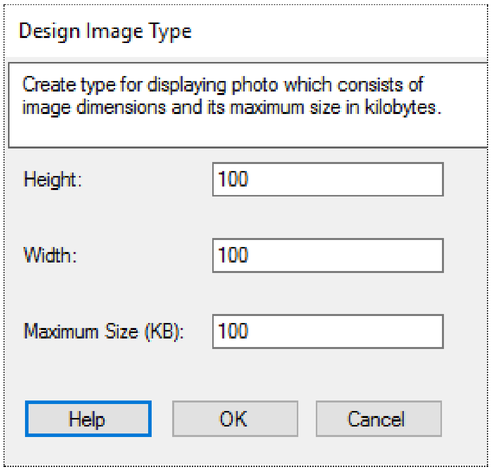
Figure 25: Custom image type as applied to the Photo field

Click ✎ to launch the **Manage Photo** dialog box for uploading a photo. The dialog box also provides many image editing options, including rotate, crop, flip, and re-size.

: Define an image display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Custom Display Types** tab (Figure 14).
4. In the **Simple Types** area, click **Add**.
   The **New Display Type** dialog box is displayed (Figure 17).
5. Enter a name for the display type and select **Image** from the **Type** list.
   You cannot change the name of a custom display type once you have created it.
6. Click **OK**.
   The **Design Image Type** dialog box is displayed.



Design Image Type

Create type for displaying photo which consists of image dimensions and its maximum size in kilobytes.

Height: 100

Width: 100

Maximum Size (KB): 100

Figure 26: Design Image Type dialog box

7. In the **Height** and **Width** boxes, type the dimensions (in pixels) of the image. The image would be displayed in the portal with these dimensions.

   The default dimension is 100 x 100 pixels.
8. In the **Maximum Size (KB)** box, type the maximum image size (in kilobytes) that can be uploaded for this display type.
9. Click **OK**.
10. On the toolbar, click **Save** 💾.

You can now link this customized image display type to a schema attribute (such as these Active Directory attributes – jpegPhoto, Photo, thumbnailPhoto, and thumbnailLogo) on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which the image placeholder is displayed on the relevant portal page. Users can use it to upload their photos.

Define a Grid display type

Use a grid display type to display data on the portal in tabular form. This is especially helpful when you want to group together multiple attributes of an object.

For example, use a grid display type to capture information about a group's members and additional owners. This information may include a member's display name, department, email, and more. Add a column to the grid for each attribute required. For each group member, portal users can view or enter values in each column (attribute) of the grid.

To create a grid, simply define its columns. Each column is mapped to a schema attribute, so each column represents the value of the attribute it is mapped to.

After creating the custom grid display type, link it to an appropriate schema attribute to render it on a portal page. This attribute must support multi-valued distinguished names. Examples of such attributes from Active Directory are; member, memberof, etc.

A few grid display types are predefined in the default portal template. The following table lists some of these along with the column names:

Display Type Name	Column Names	Description
membersgrid	• Display_Name • Membership • Beginning • Ending	Used to display the members in a group, with the display name, membership type, and membership start and end dates for each member.
groupMemberOfGrid	• Display_Name • Email • Description	Used to display the groups an object is a member of, with the display name, email address and description shown for each group.
directReportsGrid	• Display_Name • Status	Used to display the direct reports of a user, with the

		display name and status of each direct report.

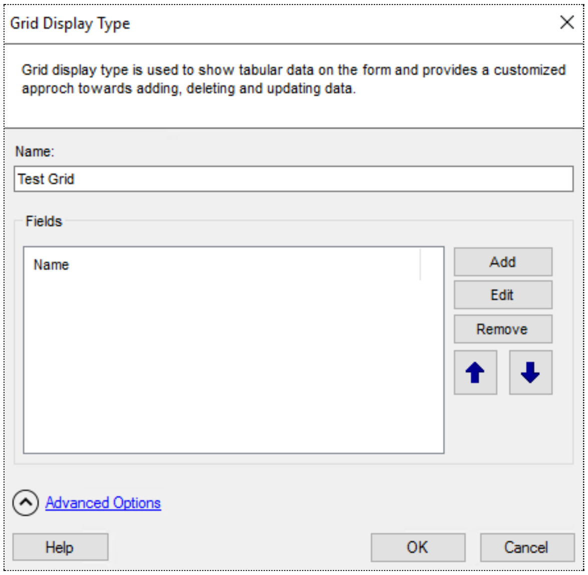
Table 11: Some predefined grid display types

You can define more custom grid display types, if required.

Define a grid display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Custom Display Types** tab (Figure 14).
4. In the **Simple Types** area, click **Add**.
   The **New Display Type** dialog box is displayed (Figure 17).
5. Enter a name for the display type and select **Grid** from the **Type** list.
   You cannot change the name of a custom display type once you have created it.
6. Click **OK**.



Grid Display Type

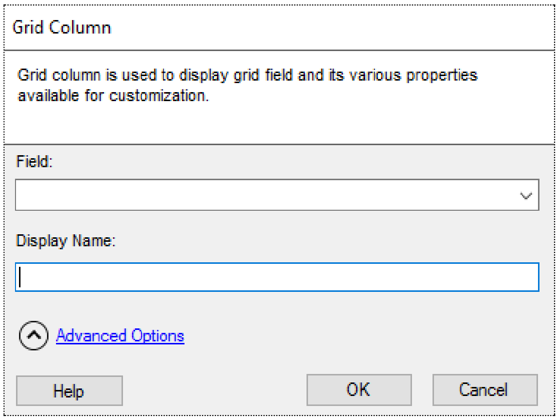
Grid display type is used to show tabular data on the form and provides a customized approch towards adding, deleting and updating data.

Name: Test Grid

Figure 27: Grid Display Type dialog box

7. On the **Grid Display Type** dialog box, specify the columns of the grid, along with the grid properties.

Click **Add** to define a column for the grid.



Grid Column

Grid column is used to display grid field and its various properties available for customization.

Figure 28: Grid Column dialog box

8. On the **Grid Column** dialog box, select a schema attribute from the **Field** list. This attribute would serve as a column in the grid.

9. Enter a name for the column in the **Display name** box. This display name would be displayed as the column name in the portal.

10. Click the **Advanced Options** link to specify additional details for the column.

11. From the **Edit Type** drop-down list, select a display type (for example, a text box or a drop-down list). In edit mode, the fields in the column would be displayed in the portal using the display type you select here.

12. From the **Search Type** drop-down list, select a display type (for example, a text box or a drop-down list). The search filter for the column would be displayed in the portal using the display type you select here, provided that:

    - search is enabled for the grid (the **Show Search Filters** check box is selected on the **Grid Display Type** dialog box - Figure 27), and

    - search is also enabled for the column (the **Searchable** check box is selected on the **Grid Column** dialog box - Figure 28).

13. Select the **Searchable** check box to enable search for the column.

14. Select the **Sortable** check box to enable the column to be sorted by clicking on its header.

15. Click **OK** to close the **Grid Column** dialog box.

    The column name is displayed in the **Fields** list on the **Grid Display Type** dialog box (Figure 27).

16. Repeat steps 7 to 15 to add a new column to the grid.

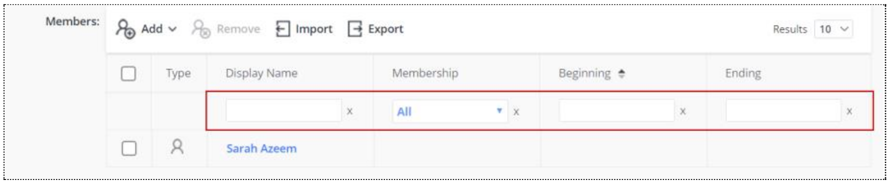
- To edit the details of a column, select it in the **Fields** area and click **Edit**.
- To remove a column from the grid, select it and click **Remove**.
- To change the order of columns in the grid, select a column and use the **Up** and **Down** arrows.

17. Click the **Advanced Options** link to specify additional details for the grid.
18. Specify a height and width for the grid by entering values in the **Height** and **Width** boxes.

    From the drop-down list next to each box, select a unit for the height and width.

    - **%**, to specify the height and width of the grid in terms of a percentage of the page's height and width.
    - **px**, to specify the height and width of the grid in pixels.
19. In the **Page Size** box, type or select a value. This value represents the number of records to show on a page.
20. Select the **Show Search Filters** check box to add a row to the grid that serves as a search bar.

    This row appears in the grid, as shown in Figure 29.



□	Type	Display Name	Membership	Beginning	Ending
		x	All x	x	x
□		Sarah Azeem			

Figure 29: Search row in a grid

21. Select the **Editable** check box to make the rows in the grid available for editing. Else, the grid would be read-only.
22. Click **OK** to close the **Grid Display Type** dialog box.
23. On the toolbar, click **Save** .

You can now link this customized grid display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which it is displayed on the relevant portal page.

Define a Radio Button display type

Use a radio display type to present the users with a predefined set of mutually exclusive options, of which they can choose only one. Usually radio buttons in a set are grouped together under a label.

In the default portal template, the following custom radio display types are predefined:

Display Type Name	Values	Description
groupMain Type	• Static Group • Smart Group	Enables users to specify whether they want to create a static group or a Smart Group.
reportTo	• Report To Originator • Report To Owner • Don’t Send Delivery Reports	Enables users to set delivery report recipients when a message sent to a group or user is not delivered.
group Type	• Security Group • Distribution List	Enables users to specify whether they want to create a security group or a distribution list.

Table 12: Predefined radio display types

You can define more radio display types, if required.

To create a radio display type, provide a label for the set of radio buttons and then add at least two radio buttons to the set.

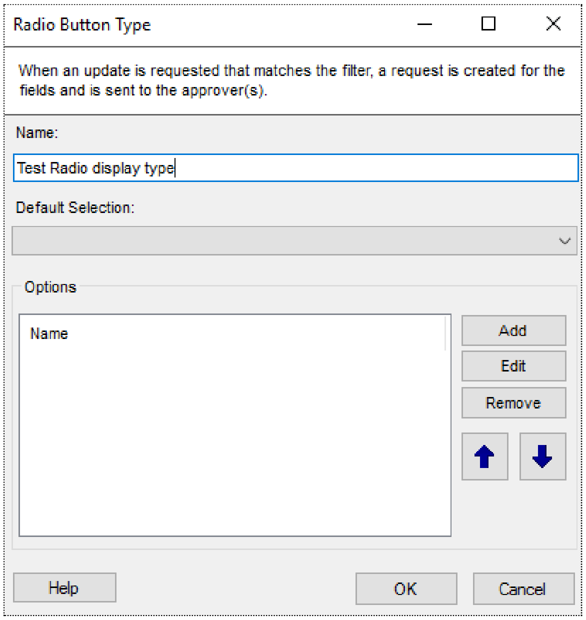
Define a radio display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Custom Display Types** tab (Figure 14).
4. In the **Simple Types** area, click **Add**.
   The **New Display Type** dialog box is displayed (Figure 17).

5. Enter a name for the display type and select **Radio** from the **Type** list. You cannot change the name of a custom display type once you have created it.

6. Click **OK**.



Radio Button Type

When an update is requested that matches the filter, a request is created for the fields and is sent to the approver(s).

Name: Test Radio display type

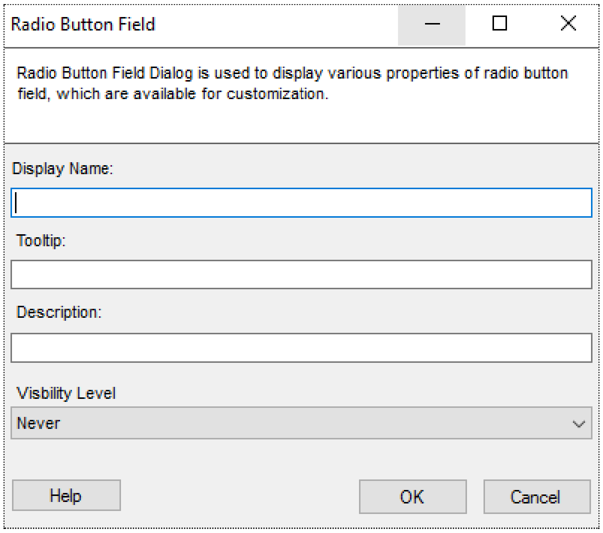
Default Selection:

Figure 30: Radio Button Type dialog box

7. On the **Radio Button Type** dialog box, use the **Options** area to define a set of radio buttons, that would be displayed in the portal under the label displayed in the **Name** box.

   You must individually define each radio button in the set.

   Click **Add** to define a radio button. The **Radio Button Field** dialog box is displayed.


Radio Button Field

Radio Button Field Dialog is used to display various properties of radio button field, which are available for customization.

Display Name:

Tooltip:

Description:

Visbility Level

Never

Figure 31: Radio Button Field dialog box

8. In the **Display Name** box, type a name for the radio button. This name is the radio button's label in the portal, so it should represent the value of the radio button.
9. In the **Tooltip** box, type the text to appear when a user hovers the pointer over the radio button.
10. Enter a description for the radio button in the **Description** box.
11. From the **Visibility Level** drop-down list, select a security role. The radio button would be visible to users of the selected role and to roles with a priority value higher than the selected role.

    Select **Never** to hide the radio button from all users.

    The visibility level determines the security role(s) whose members can view the radio button. The **Visibility Level** list contains all security roles defined for the identity store.
12. Click **OK** to close the **Radio Button Field** dialog box.

    The radio button is listed in the **Options** area on the **Radio Button Type** dialog box.
13. To define another radio buttons in the set, repeat steps 7 to 12.
    - To modify the details of a radio button, select it and click **Edit**.
    - To remove a radio button from the set, select it and click **Remove**.
    - To change the order by which radio buttons are displayed on the portal, select a radio button and use the **Up** and **Down** arrows.

14. From the **Default Selection** drop-down list, select a radio button. On the portal, this radio button would be the default selection in the radio button set.

    The **Default Selection** list contains all radio buttons defined in the **Options** area.

15. Click **OK** to close the **Radio Button Type** dialog box.

16. On the toolbar, click **Save** 🖫.

You can now link this customized radio display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which it is displayed on the relevant portal page.

Define a Multiline Textbox display type

A multiline textbox allows users to type information into a box that supports wordwrapping and vertical scrolling.

Like a textbox, use a multiline textbox display type to collect and display a single value for an attribute.

The multiline textbox display type is especially useful for fields that require a lengthy value, such as the Description field. Moreover, as it can have multiple rows, users can view more characters of the entered value on screen as compared to a textbox.

In the portal's default template, the Description field on the Create New Group wizard uses the multiline textbox display type. It is as:

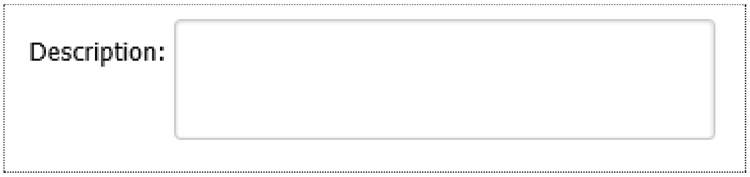


Figure 32: Multiline textbox display type applied on the Description field

To define a multiline textbox display type, provide a name for it and specify the on-screen width by giving the number of rows to be displayed for it. Portal uses can use the Enter key to add as many rows as required while entering data.

Define a multiline textbox display type

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.

2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.

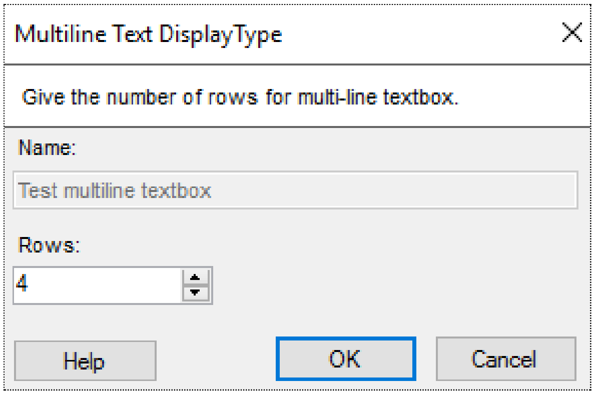
3. Click the **Custom Display Types** tab (Figure 14).

4. In the **Simple Types** area, click **Add**.
   The **New Display Type** dialog box is displayed (Figure 17).

5. Enter a name for the display type and select **Multiline Textbox** from the **Type** list.

   You cannot change the name of a custom display type once you have created it.

6. Click **OK**.



Multiline Text DisplayType

Give the number of rows for multi-line textbox.

Name: Test multiline textbox

Rows: 4

Figure 33: Multiline Text Display Type dialog box

7. In the **Rows** box, type or select a value to specify the number of rows the textbox display type should have. These rows make up the on-screen length of the textbox; however, portal uses can use the Enter key to add as many rows as required while entering data.

8. Click **OK**.

9. On the toolbar, click **Save** .

You can now link this customized radio display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14), after which it is displayed on the relevant portal page.

Define a Linked Combo display type

The linked combo is a custom display type that you can link to other display types on a portal page. When a user selects a value from the linked combo, the values for the display types linked to it are populated accordingly. A common application of the linked combo is the country, state, and city fields. When a user selects a country, the State field changes to display states specific to it. On selecting a state, the City field displays the cities specific to the selected state.

In the default portal template, only one linked combo display type, CountryState, is defined, that establishes a relationship between the country and state fields. Selecting a country populates the State list with the corresponding states.

The linked combo display type also allows for more complex linking between fields, such as would be needed to link the office, city, state and country fields. Relationships can be extended to any level. However, this requires you to create and maintain an external data file containing the data and relationships for the required fields.

NOTE While defining a linked combo, consider the following:

- You can define multiple linked combos for an object on different pages of the portal, or even on the same page, provided that different attributes are used for the combos.

  Suppose you define a linked combo for the user properties page using the department, title, last name, description, country and address attributes. Next, when you define another linked combo for the user object on the user properties page or on any other page, such as the Profile Validation page, you cannot use any of the attributes used in the first combo.

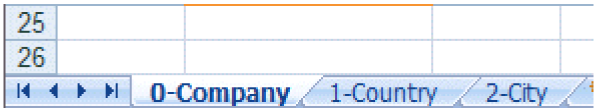
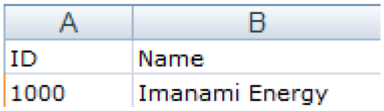
- For two different objects, you can use the same attributes in different linked combos that are rendered on the same page.

Linked Combo data file

The linked combo requires an XML file that contains the data for the display type itself and the other display types that will be linked to it. GroupID also supports the Microsoft Excel file format (.xls or .xlsx), which it automatically converts to XML. The data in the Excel file must be in a specific format for GroupID to process it.

Excel data file format

The following table explains the rules for the Microsoft Excel workbook to use for the linked combo display type, so that Self-Service can identify field values and their relationships.

No.	Rule for	Description
1.	Worksheet names	The worksheet names should be in the format: Number-Name Where: ▪ *Number* is the serial number based on the order of the worksheet and it should start from zero. This means that the number for the first worksheet should be 0, the second worksheet should be 1, the third worksheet should be 2, and so on. ▪ *Name* is the name of the worksheet that identifies the data it contains. It can be anything you want.  Figure 34: Worksheet names set for the data file
2.	Identity column	Each worksheet should have an identity (*ID*) column, which will contain a unique value for every record entered in the sheet. A B ID Name 1000 Imanami Energy Figure 35: ID column for the 0-Company worksheet
3.	Name column	Each worksheet should have a *Name* column. This column contains the values that will be displayed in the linked combo. For example, the *Name* column on the 0-Company worksheet (Figure 35) will contain the company name for every record on the sheet.
4.	Foreign Key column	Each worksheet that contains data related to that on a previous sheet, should have a foreign key identity column (*FK*). This column contains the ID of the record (from the immediately previous sheet) to which the current record is related.

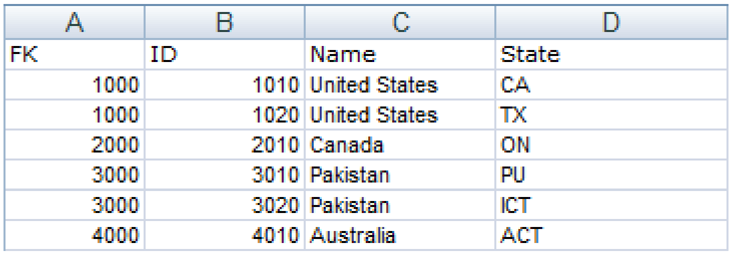
<table>
<tr><th>No.</th><th>Rule for</th><th>Description</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th></th><th>A</th><th>B</th><th>C</th><th>D</th></tr>
<tr><td></td><td>FK</td><td>ID</td><td>Name</td><td>State</td></tr>
<tr><td></td><td>1000</td><td>1010</td><td>United States</td><td>CA</td></tr>
<tr><td></td><td>1000</td><td>1020</td><td>United States</td><td>TX</td></tr>
<tr><td></td><td>2000</td><td>2010</td><td>Canada</td><td>ON</td></tr>
<tr><td></td><td>3000</td><td>3010</td><td>Pakistan</td><td>PU</td></tr>
<tr><td></td><td>3000</td><td>3020</td><td>Pakistan</td><td>ICT</td></tr>
<tr><td></td><td>4000</td><td>4010</td><td>Australia</td><td>ACT</td></tr>
</table>
Figure 36: FK column containing the company ID</td></tr>
</table>

Table 13: Excel data file format for a linked combo

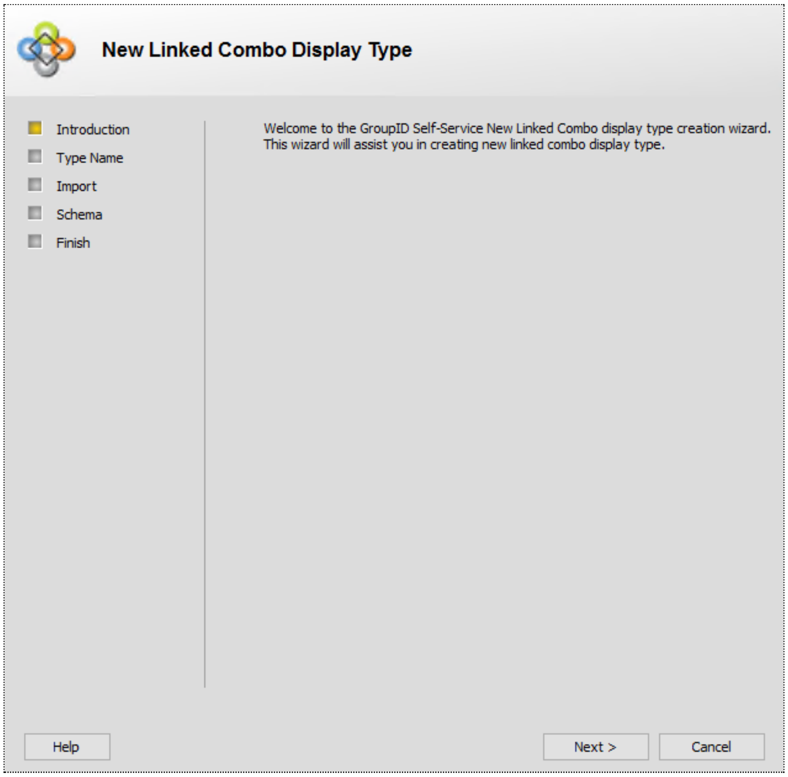
Defining a Linked Combo display type

Before creating a linked combo, you should have the data file ready. The data file is used to populate the linked combo and other fields that will be linked to it.

1. In GroupID Management Console, select **Self-Service** > **Portals** > **[Required portal]** > **Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Custom Display Types** tab (Figure 14).
4. In the **Linked Combo Types** area, click **Add**.

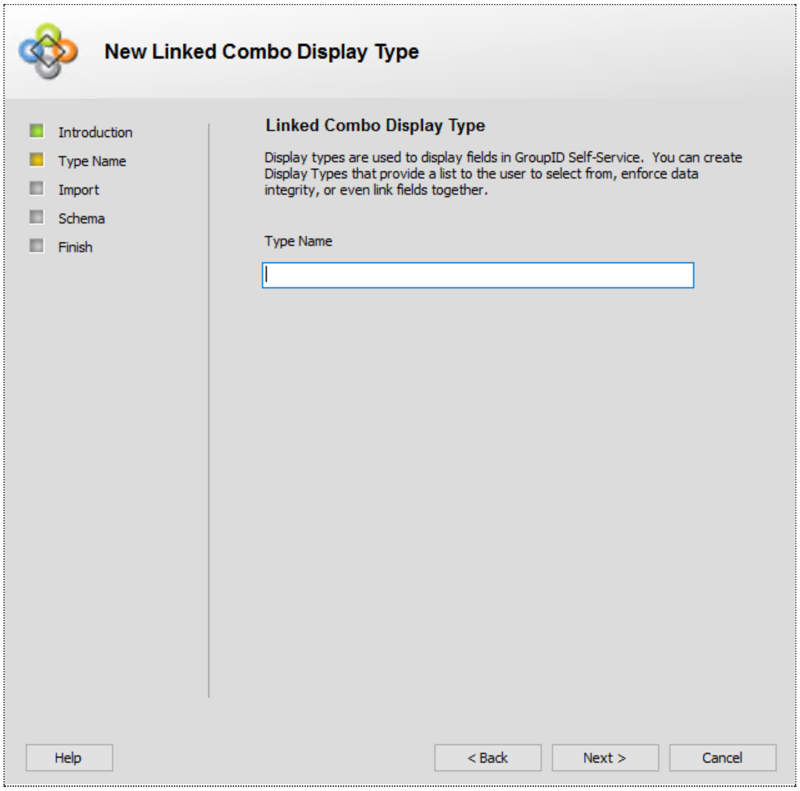
   The **New Linked Combo Display Type** wizard opens to the **Introduction** page.



Welcome to the GroupID Self-Service New Linked Combo display type creation wizard.
This wizard will assist you in creating new linked combo display type.

Figure 37: Introduction page

5. Read the welcome message and click **Next**.



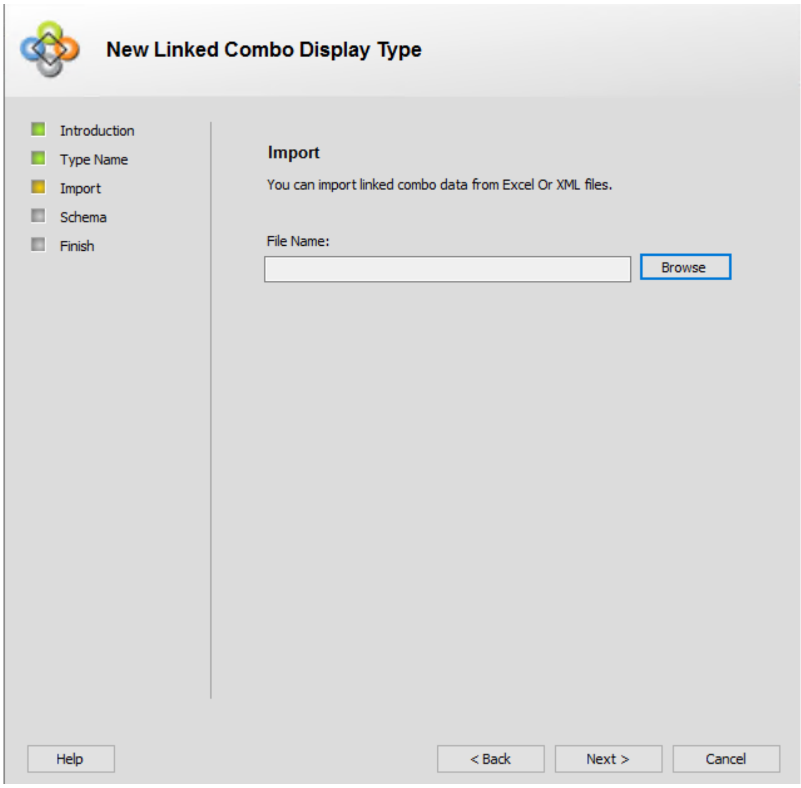
Linked Combo Display Type

Display types are used to display fields in GroupID Self-Service. You can create Display Types that provide a list to the user to select from, enforce data integrity, or even link fields together.

Type Name

Figure 38: Type Name page

6. Type a name for the linked combo in the **Type Name** box and click **Next**.



Import

You can import linked combo data from Excel Or XML files.

File Name:

Figure 39: Import page

On the **Import** page, specify the data source for the linked combo.

7. Click **Browse** and select the XML or Microsoft Excel file containing the data to populate the linked combo and the other display types linked to it.

   - The Excel workbook can be located anywhere on your hard disk or on any shared location on the network.
   - The XML file must be placed at the location, X:\Program Files\Imanami\GroupID 10.0\SelfService\Inetpub\<portal name>\Web\LinkedCombo\
     (where X represents the GroupID installation drive).

   If the input file is a Microsoft Excel (.xls or .xlsx) file, the wizard automatically creates its XML version and uses this XML file for further processing.

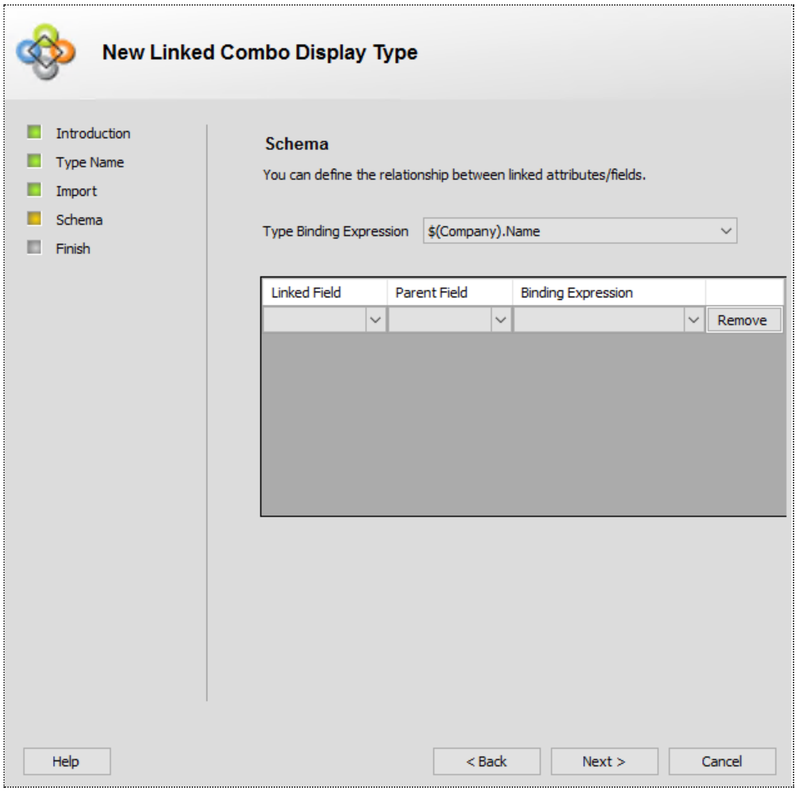
   The format of the Excel file is discussed in the Excel data file format section.

NOTE

If data in the source file is updated, the updates will not be displayed in the linked combo or its linked display types until the linked combo is edited and the source file is again selected on the **Import** page. You must perform this update every time you make changes to the data.

See Updating the source data file on page 72 for details.

8. Click **Next**.



New Linked Combo Display Type

Schema

You can define the relationship between linked attributes/fields.

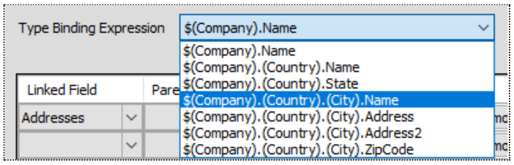
Type Binding Expression: $(Company).Name

Figure 40: Schema page

On the **Schema** page, specify the different linked fields for the combo and the data that each field should contain. This linking must be in accordance with how the data has been defined in the source file.

9. Map the **Type Binding Expression** list to the first worksheet (0-<worksheet name>) of the source Excel workbook. The portal fields use the binding expression to obtain reference to the worksheet in the source file from where they should retrieve and display data.

   Expressions in the **Type Binding Expression** list are auto-generated on the basis of the number of sheets in the source Excel workbook and the number of columns in a sheet. It is as:



Type Binding Expression: $(Company).Name

$(Company).Name
$(Company).(Country).Name
$(Company).(Country).State
$(Company).(Country).(City).Name
$(Company).(Country).(City).Address
$(Company).(Country).(City).Address2
$(Company).(Country).(City).ZipCode

Figure 41: Binding expression examples

In an expression, the worksheet names are enclosed in brackets while the names of the data columns in the worksheets are without brackets. The expressions shown in Figure 41 indicate that the Excel workbook has three worksheets; Country, Company, and City.

- The Company worksheet has one data column; Name.
- The Country worksheet has two data columns; Name and Sate.
- The City worksheet has four data columns; Name, Address, Address2, and ZipCode.

10. Use the grid on the **Schema** page to link and relate the data from the sheets of the Excel workbook to the portal fields.

    a. From the **Linked Field** drop-down list, select a field (for example, Country). This field would be linked to the data column represented by the binding expression you select from the **Binding Expression** drop-down list.

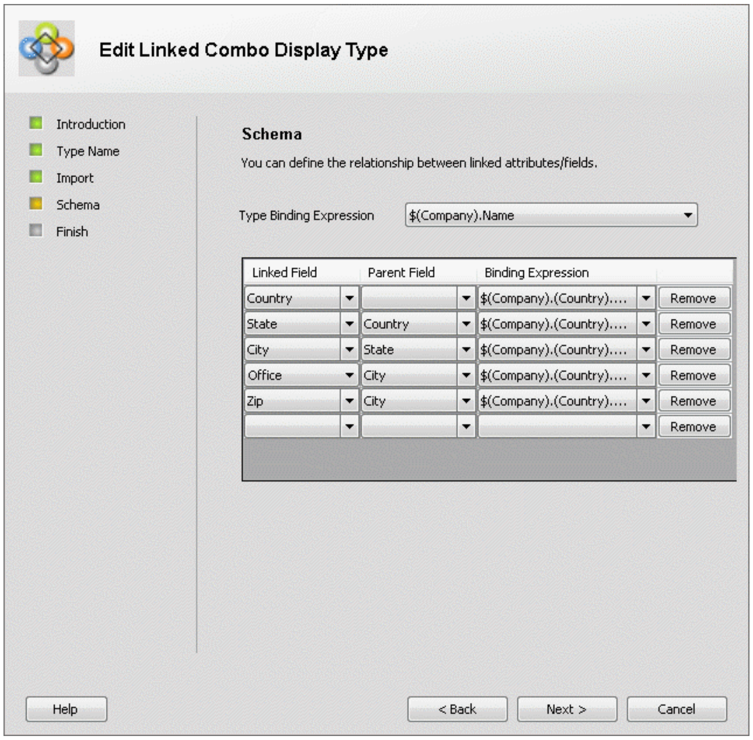
    The **Linked Field** list contains pre-defined, hard coded fields, where each field is already mapped to a schema attribute. These fields can possibly be used in a linked combo. When you map a field to a binding expression, the values in the selected worksheet's data column would be available in the field on the portal. When a portal user selects a value, it is set as the attribute's value for the field.

    b. The **Parent Field** list does not apply to the first row. For all other rows, use it to select the name of the parent field for the selected linked field. For example, when *State* is selected in the *Linked Field* list, you should select *Country* as the parent field.

    c. From the **Binding Expression** list, select an expression that represents the data column you want to link to the field selected in the **Linked Field** list.

    Binding expressions are auto-generated on the basis of the number of sheets in the source Excel workbook and the number of columns in a sheet. It is as shown in Figure 41.

The following example shows the relationship given on the **Schema** page for an Excel workbook with three worksheets; 0-Company, 1-Country, and 2-City.



Edit Linked Combo Display Type

Schema

You can define the relationship between linked attributes/fields.

Type Binding Expression: $(Company).Name

Linked Field	Parent Field	Binding Expression	
Country		$(Company).(Country)....	Remove
State	Country	$(Company).(Country)....	Remove
City	State	$(Company).(Country)....	Remove
Office	City	$(Company).(Country)....	Remove
Zip	City	$(Company).(Country)....	Remove
			Remove

Figure 42: Schema page with field mapping

The binding expressions created with reference to the workbook are as shown in Figure 41. The relationship formed between fields can be explained as:

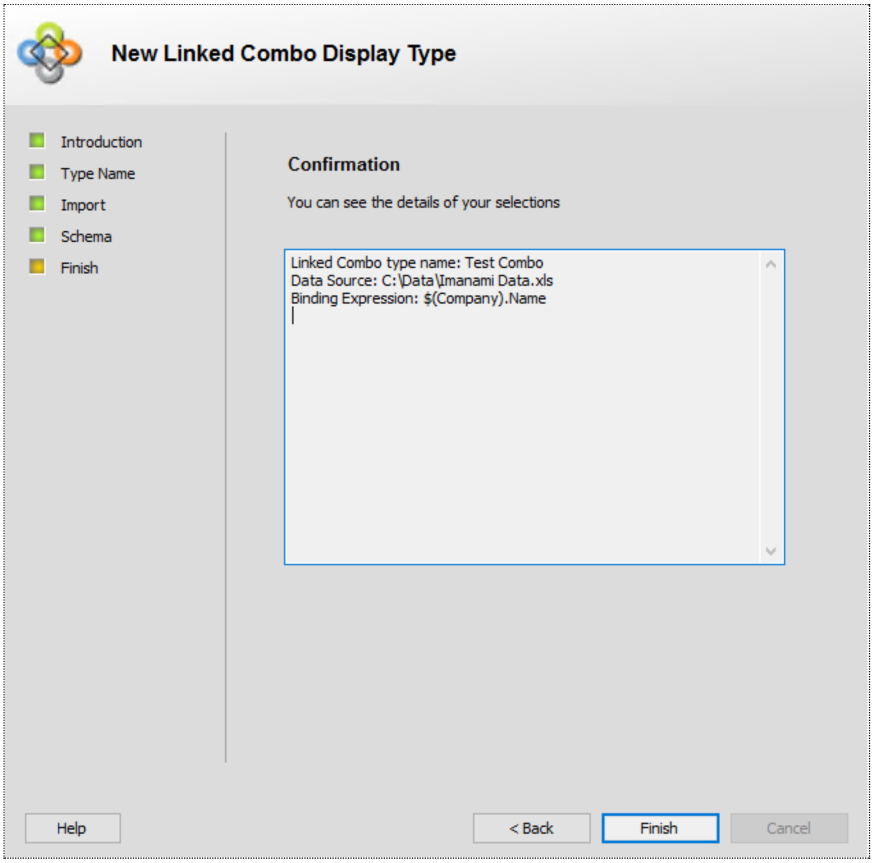
- The Company field, containing all records from the Name column on the Company worksheet, will be the primary linked combo field in the portal.
- The Country field in the portal will contain all records from the Name column on the Country worksheet.
- The State field in the portal will contain all records from the State column on the Country worksheet. The Country field will be the parent field for the State field, which means that when a user selects a country, the State field will show the states in the selected country. These states are filtered on the basis of the record IDs.
- The City field in the portal will contain all records from the Name column on the City worksheet. The State field will be the parent field for the City field, which means that when a user selects a state, the City field will show the cities in the selected state. These cities are filtered on the basis of the record IDs.

The complete structure for the data in the Excel workbook is explained in the following table.

Worksheet	Columns	Description	Example
0-Company	ID	Company identifier	1000 2000
	Name	Company name	Imanami Consulting Imanami Software
1-Country	FK	Company identifier with which to link this record	1000 2000
	ID	Country identifier	1010 2010
	Name	Country name	United States Pakistan
	State	State abbreviation	CA PU
2-City	FK	Country identifier with which to link this record	1010 2010
	ID	City identifier	1011 2011
	Name	City name	Livermore Lahore
	Address	Office address 1	5099 Preston Ave Siddiq Trade Center
	Address 2	Office address 2	
	Zip Code	Postal zip code or area code	94551 54600

Table 14: Data structure in a sample Excel workbook

11. Click **Next**.



Confirmation

You can see the details of your selections

Linked Combo type name: Test Combo
Data Source: C:\Data\Imanami Data.xls
Binding Expression: $(Company).Name

Figure 43: Finish page

12. On the **Finish** page, view the information you entered on the previous pages. Use the **Back** button to go to a previous page to make any changes.

13. , Click **Finish** to create the linked combo display type.

14. On the toolbar, click **Save** 💾.

The new linked combo display type is listed in the **Linked Combo Types** area on the **Custom Display Types** tab (Figure 14).

In this linked combo, you have linked different fields together, and specified the values that would be populated in each of the linked fields.

Implementing a Linked Combo

To use a linked combo in the portal, you must do the following:

1. Link a linked combo display type to a schema attribute on any of the **Search Forms**, **Update**, **Properties**, **Create Object**, or **Property Validation** tabs of the **Designs** node (Figure 14),

The linked combo is rendered as a drop-down list in the portal.

On the **Schema** page (Figure 40) of the **New Linked Combo Display Type** wizard, you selected an expression (representing a data column in the source Excel workbook) from the **Type Binding Expression** drop-down list. Each record in this column would be displayed as a value in the drop-down list on the portal. When a user selects a value, it would be stored as the value of the schema attribute mapped to the linked combo display type.

2. The fields listed in the **Linked Field** list on the **Schema** page (Figure 40) are already mapped to schema attributes. For all fields that you use in a linked combo, one of the following cases apply:

   - If a field’s schema attribute is already rendered as a field on the same portal page as the linked combo, it auto connects to the linked combo. Values in this field are displayed on the basis of the binding expression mapped to it on the **Schema** page (Figure 40).

     Suppose you select a field, Country, from the Linked Field list on the Schema page, which is mapped to the “co” attribute in Active Directory. You link it to the ‘Country Name’ column in the source file. This column contains the names of all countries in the world.

     Now in the default portal template, the ‘co’ attribute is already rendered as a drop-down list on the General tab in user properties and displays the names of Asian countries. When you apply your linked combo (containing the Country field) on the General tab, it auto-connects to the ‘co’ attribute and replaces its values (the list of Asian countries) with the values from the source data file (the names of all countries of the world.).

   - If a field’s schema attribute is not previously used on the same portal page as the linked combo, the field will not be displayed in the portal. You must link this attribute to a display type and render it on the same portal page as the linked combo. Values in this field will be displayed on the basis of the binding expression mapped to it on the **Schema** page (Figure 40).

   In any case, set the display type of each field in a linked combo to a Textbox or Dropdown list, depending on the kind of values it would hold.

An example case for implementing a linked combo is discussed below.

Step No 1: Link the linked combo to a schema attribute

1. In GroupID Management Console, select **Self-Service** > **Portals** > **[required portal]** > **Designs**.

2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.

3. Click the tab representing the portal page where you want to display this linked combo, for example, the **Properties** tab (Figure 50).

4. Make sure that the **User** option is selected in the **Select Directory Object** list, because in our example, we have to render the linked combo on the user properties page in the portal.

5. The names of all tabs on the portal's user properties page are listed under **Name**. You can add a new tab or render the linked combo on an existing tab (for example, the **General** tab).

   Select **General** in the **Name** list and click **Edit**.

6. On the **Edit Tab/Category** dialog box, you can define a new field on the tab or link an existing field (for example, the **Company** field) to the linked combo.

   Select **Company** in the **Fields** area and click **Edit**.

7. On the **Edit Field** dialog box, select the schema attribute to which you want to map your linked combo, and from the **Display Type** list, select the name of your linked combo display type.

8. Click **OK** on the dialog boxes to close them.

9. On the toolbar, click **Save** 💾.

The Company field would be displayed as a drop-down list on the General tab of the user properties page in the portal. Values in this list will be populated from the combo's source data file, on the basis of the expression selected in the Type Binding Expression list on the **Schema** page (Figure 40) of the **New Linked Combo Display Type** wizard.

Step No 1: Render the linked fields in the combo on the portal

If the fields defined in a linked combo are already rendered on the same portal page as the linked combo, you only have to make sure that the appropriate display type is used for them. Some examples are shown in Table 15.

On the other hand, if the fields defined in a linked combo are not available on the same portal page as the linked combo, you must create the fields first. These fields must be linked to the same schema attributes as the combo's fields are linked with, and an appropriate display type must be set for them. Table 15 shows an example of the field names and the display types to set for them.

Field	Display Type to set	Notes
Country	Dropdown List	Create a Dropdown List display type and set that for this field or use the default dropdown list, lstCountry. The default dropdown list, lstCountry, set for this field has default values set for it, which may produce undesirable results.
State	Dropdown List	Create a Dropdown List display type and set that for this field or use the default dropdown list, lstState.
City	Dropdown List	Create a Dropdown List display type and set that for this field or use the default dropdown list, lstCity.
Address	Textbox	Use a simple textbox display type with this field. No display type has been predefined for it.
Zip	Textbox	Use a simple textbox display type with this field or use the default textbox display type, maskZIPCode. This default display type comes with a validation check that ensures that users enter the zip code in the required format.

Table 15: Example of display types to use with linked fields in a linked combo

Updating the source data file

If data in the source file is updated, you must reload the file for changes to take effect.

1. In GroupID Management Console, select **Self-Service** > **Portals** > **[required portal]** > **Designs**.
2. Select an identity store to define a custom display type for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Custom Display Types** tab (Figure 14).
4. In the **Linked Combo Types** area, select the linked combo for which you want to reload the source data file and click **Edit**.

5. On the **Edit Linked Combo Display Type** wizard, click **Next** until you reach the **Import** page.
6. On the **Import** page (Figure 39), click **Browse** to select the file to load and click **Next**.
7. On the **Schema** page (Figure 40), make changes to the relationships, if required, and click **Next**.
8. On the **Finish** page, click **Finish** to close the wizard.
9. On the toolbar, click **Save** 💾.

Chapter 5 - Customizing a Portal

Display types enable you to control the layout and appearance of a portal's web pages, as well as the functionality and fields displayed in the portal.

A new Self-Service portal comes with a default design template; however, you can customize it to suit your requirements. Examples of customization include adding new web pages and adding new fields to pages.

When multiple identity stores are associated with a portal, you can design a different portal for each identity store. In this way, the portal offers a different design and functionality for each of the associated identity stores.

Display types enable you to customize the following for a portal:

- Search Forms: control the fields to be displayed on different search forms and search result pages in a portal.
- Quick Search: control the schema attributes quick search would run on.
- Update Wizard: customize the pages and fields of the Update wizard, which is available in the Update Wizard functionality mode of the portal.
- Object Properties: control what properties of directory objects you want to display in the portal.
- Toolbars: customize the buttons on the portal toolbars.
- Navigation bar: customize the left navigation bar of the portal.
- Bad Words List: restrict users from entering offensive words while using the portal.
- Import/Export: assign descriptive and meaningful names to schema attributes being used for importing/exporting members and additional owners for groups.
- Create Object: control the schema attributes displayed on object creation wizards for different object types.
- Smart Group Attributes: control what schema attributes you want to display in the portal for creating Smart Group queries.
- Property Validation: manage the schema attributes for user profile validation and group attestation.

- Organizational Hierarchy: specify user attributes for display on the organizational hierarchy chart in the portal.
- Card View: specify the attributes to display on an object card and the object list view in the portal.
- The Send As and Send on Behalf features: configure the Send As and Send on Behalf functionality for the portal; users can then add objects to their Send As and Send on Behalf lists using the portal.

Customize Search Forms

Self-Service enables you to customize the search forms and corresponding search result pages for a portal. This customization allows you to do the following on a form:

- Add a new field
- Edit an existing field
- Remove an existing field
- Change the arrangement of fields on a page

Several search forms are available, depending on the portal's specified functionality mode.

The following table lists the search forms that you can customize, the functionality modes that they apply to, and a brief description of each.

Search Form Name	Functionality Mode	Description
Smart Group Preview	Enterprise, Groups	This search form is displayed when a user clicks the **Preview** button on the **Query Designer** dialog box. The form enables you to preview the results returned with the specified query for the Smart Group. The Query Designer dialog box can be launched from the Smart Group page of the Create New Group wizard, and from the Smart Group tab in group properties.
Default	Enterprise, Groups, Phone Book	The search form is displayed when a user clicks the **Advanced Search** link on the portal pages.

Search Form Name	Functionality Mode	Description
		It is also displayed when a user clicks the **User Search** button on the **Users** page of the portal. On this form, users can search directory objects by different attributes.
Expiring Groups	Enterprise, Groups	This search form is displayed when a user clicks the **My Expiring Groups** tab on the **Groups** page. This form displays the logged-on user's groups that will expire in 30 days or less.
Expired Groups	Enterprise, Groups	This search form is displayed when a user clicks the **My Expired Groups** tab on the **Groups** page. This form displays the logged-on user's groups that have expired.
Groups	Enterprise, Groups	The search form is displayed when a user clicks the **Group Search** button on the **Groups** page of the portal. On this form, users can search for groups.
Find Dialog	Enterprise, Groups	This search form can be launched from various portal pages, for example, from the **Owner** tab, **Members** tab, and **Member Of** tab in group properties. This dialog box is used to search and select the required objects for different purposes.
Disabled Users	Enterprise	This search form is displayed when the administrator or Helpdesk user clicks the **Disabled Users** tab on the **Users** page. This form displays the identity store users that have been disabled and expired by the User Life Cycle job.

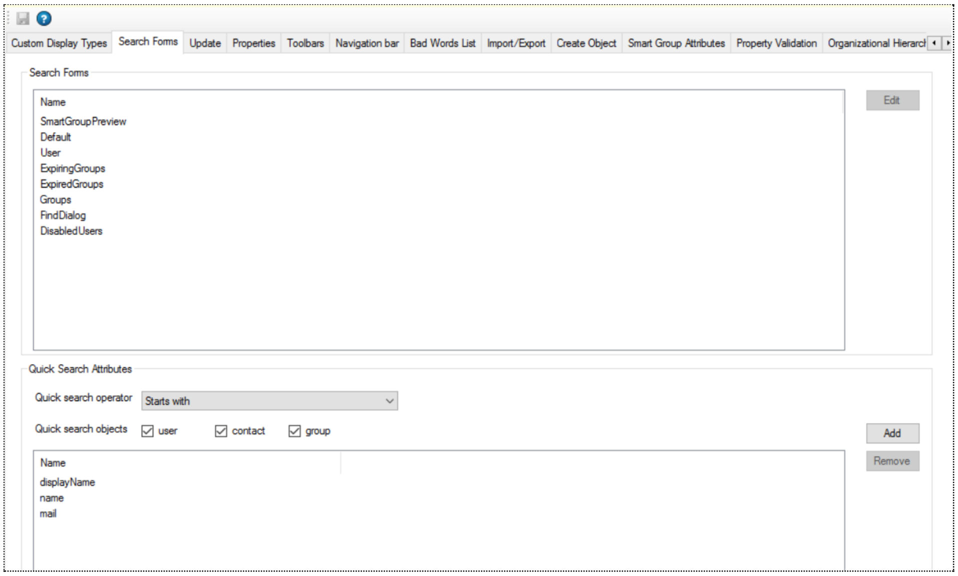
Table 16: Search Forms in the portal

NOTE You can only customize existing search forms; Self-Service does not provide the functionality to add new ones.

Customize search forms and search result pages

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Search Forms** tab.



Name
SmartGroupPreview
Default
User
ExpiringGroups
ExpiredGroups
Groups
FindDialog
DisabledUsers

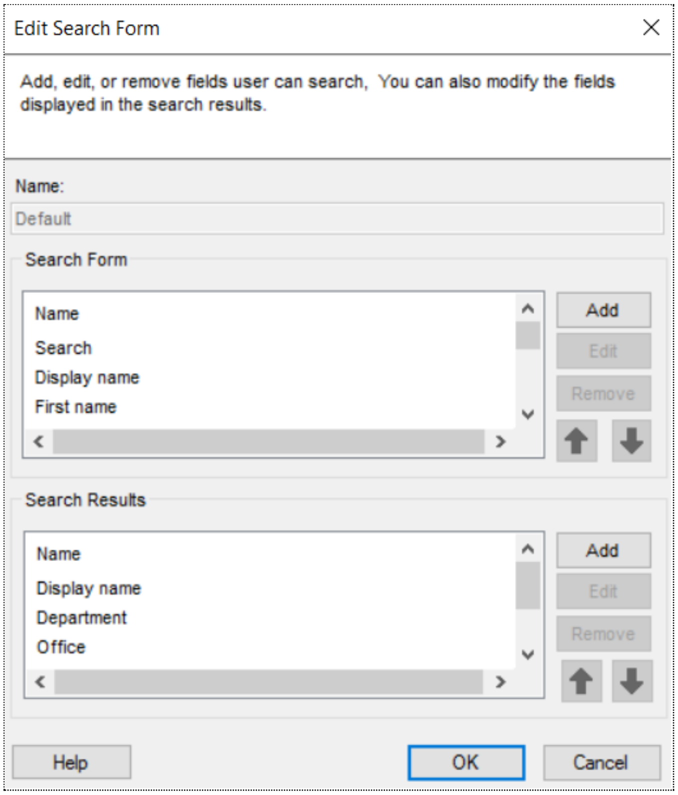
Quick search operator: Starts with

Quick search objects: ☑ user ☑ contact ☑ group

Name
displayName
name
mail

Figure 44: Search Forms tab

4. All search forms available in the portal are listed under **Name**. To modify a form, select it and click **Edit**.



Edit Search Form

Add, edit, or remove fields user can search, You can also modify the fields displayed in the search results.

Name: Default

Search Form

Name
Search
Display name
First name

Search Results

Name
Display name
Department
Office

Figure 45: Edit Search Form dialog box

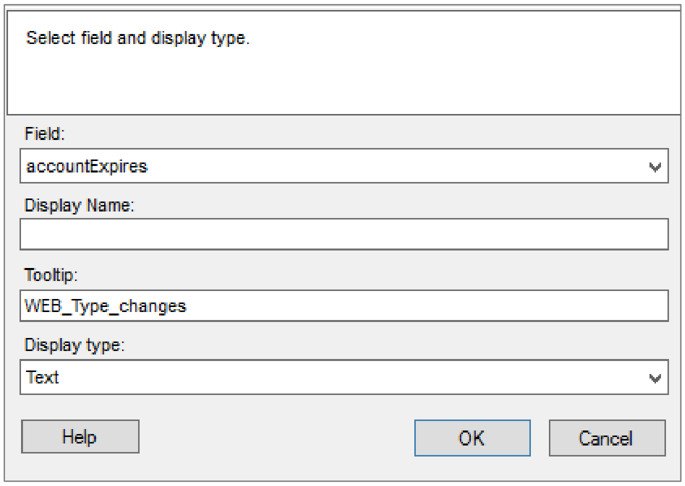
The **Search Form** and **Search Results** areas list the fields currently available on the search form and the search results pages of the selected search form.

5. Customize the search form or search results page by:

   - Adding a new field
   - Modifying the properties of an existing field
   - Removing a field
   - Changing the order in which fields are displayed on the portal page Select a field and click ↑ or ↓.

Add a field to the search form or results page

1. On the **Edit Search Form** dialog box (Figure 45), click **Add** in the required area.



Select field and display type.

Field: accountExpires

Display Name:

Tooltip: WEB_Type_changes

Display type: Text

Figure 46: Add Field dialog box

2. From the **Field** list, select a schema attribute to link to this field.
   - For the search form, the search string you enter in this field will be matched to the value of this attribute.
   - For the search results page, the field will display the value of this attribute.
3. In the **Display Name** box, type a display name for the field. This name is the field’s label on the search form or search results page.
4. In the **Tooltip** box, type the text to appear when a user hovers the pointer over the field.
5. From the **Display type** list, select the display type to use for rendering this field on the portal. The list contains all basic and custom display types defined on the **Custom Display Types** tab (Figure 14).

   This box is not available while adding/editing fields for Search Results.
6. Click **OK** to close the dialog box.
   The new field is displayed in the respective area on the **Edit Search Form** dialog box (Figure 45).
7. Click **OK** to close the **Edit Search Form** dialog box (Figure 45).
8. On the toolbar, click **Save** 💾.

Modify a field on the search form or results page

1. On the **Edit Search Form** dialog box (Figure 45), select the field you want to modify.
2. Click **Edit** in the required area.

   The **Edit Field** dialog box is displayed, which is similar to the **Add Field** dialog box (Figure 46). Refer to steps 2-5 under the figure to edit the field and click **OK**.
3. Click **OK** on the **Edit Search Form** dialog box (Figure 45).
4. On the toolbar, click **Save** 💾.

Remove a field from the search form or results page

1. On the **Edit Search Form** dialog box (Figure 45), select the field you want to remove.
2. Click **Remove** in the required area.
3. Click **OK** on the **Edit Search Form** dialog box (Figure 45).
4. On the toolbar, click **Save** 💾.

Customize Quick Search

In a Self-Service portal, the quick search box is available at the top of the page. You can specify the schema attributes users can perform quick search on. When the user enters a search string, the values of all specified attributes would be matched to return the results.

You can also specify a search operator that determines what part of the attribute value should match the search string.

Specify a schema attribute to perform Quick Search on

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.

3. Click the **Search Forms** tab (Figure 44).
4. In the **Quick Search Attributes** area, the **Name** column lists the schema attributes whose values will be matched when a user enters a search string in the quick search box.

   Click **Add** to add a new attribute to this list.
5. On the **Quick Search Attribute** dialog box, select a schema attribute from the **Field** drop-down list.
6. Click **OK**.
   The attribute is displayed in the **Name** column in the **Quick Search Attributes** area.

   To remove an attribute from the list, select it and click **Remove**.
7. From the **Quick search operator** drop-down list, select an option.
   - **Equal** - looks up the values of all attributes listed in the **Name** column and returns records having a value that exactly matches the search string.
   - **Contains** - looks up the values of all attributes listed in the **Name** column and returns records having a value that contains the search string.
   - **Starts with** - looks up the values of all attributes listed in the **Name** column and returns records with values starting with the search string.
   - **Ends with** - looks up the values of all attributes listed in the **Name** column and returns records with values ending with the search string.
8. You can specify the object type(s) that will be searched when users perform a search using the quick search function of the portal.

   Select the **user**, **group**, and/or **contact** check boxes next to **Quick search objects** to make that object type searchable in quick search.
9. On the toolbar, click **Save** 💾.

Customize a portal’s Update wizard

Self-Service allows you to customize the pages of the Update wizard for a portal. The wizard is accessible in the **Update Wizard** functionality mode, and enables the logged-on user to update his or her profile information in the directory using a wizard.

Customization includes:

At the category level:

- Adding a new page (referred to as a category) to the wizard
- Modifying the properties of an existing page
- Removing a page from the wizard

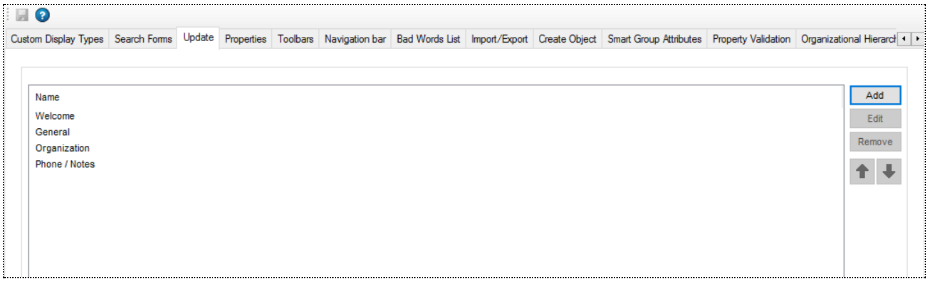
At the field level:

- Adding a field to a wizard page
- Modifying the properties of a field on a wizard page
- Arranging the fields on a wizard page
- Removing a field from a wizard page

Add a new wizard page

1. In GroupID Management Console, select **Self-Service** > **Portals** > **[required portal]** > **Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Update** tab.

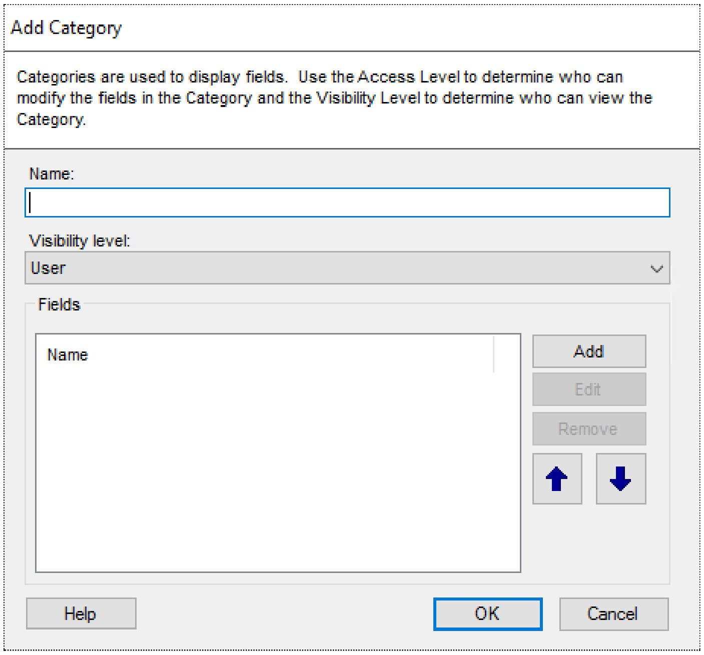


Name
Welcome
General
Organization
Phone / Notes

Figure 47: Update tab

   The **Name** list displays pages currently available on the Update wizard. The pages are referred to as **Categories**.

4. Click **Add** to add a new category to the Update wizard.



Add Category

Categories are used to display fields. Use the Access Level to determine who can modify the fields in the Category and the Visibility Level to determine who can view the Category.

Name:

Visibility level: User

Figure 48: Add Category dialog box

5. In the **Name** box, type a name for the category. The page will be displayed in the wizard with this name.

6. From the **Visibility level** drop-down list, select a security role. The category would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   Select **Never** to hide the category from all users.

   The visibility level determines the security role(s) whose members can view the category (page) on the wizard. The **Visibility level** list contains all security roles defined for the identity store.

7. To add fields to the page, see Add a new field to a wizard page on page 84.

8. Click **OK** to close the **Add Category** dialog box.

9. On the toolbar, click **Save** .

Modify the properties of a wizard page

1. On the **Update** tab (Figure 47), select the required page in the **Name** list and click **Edit**.

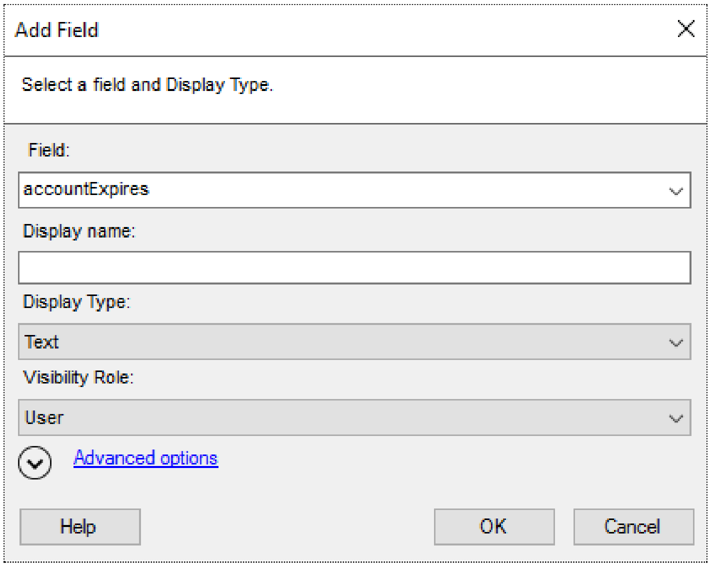
2. The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48). Refer to the instructions under the figure to edit the wizard page.

Remove a page from the wizard

1. On the **Update** tab (Figure 47), select the required page in the **Name** list and click **Remove**.
2. On the toolbar, click **Save** .

Add a new field to a wizard page

1. On the **Add Category** or **Edit Category** dialog box (Figure 48), click **Add** in the **Fields** area. The **Add Field** dialog box is displayed.



Add Field

Select a field and Display Type.

Field: accountExpires

Display name:

Display Type: Text

Visibility Role: User

Figure 49: Add Field dialog box

2. From the **Field** list, select a schema attribute to link to this field.
3. In the **Display Name** box, type a display name for the field. This name is the field's label on the wizard.
4. From the **Display Type** drop-down list, select the display type to use for rendering this field on the wizard.

   The list contains all basic and custom display types defined on the **Custom Display Types** tab (Figure 14).
5. From the **Visibility Role** drop-down list, select a security role. The field would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   Select **Never** to hide the field from all users.

The visibility level determines the security role(s) whose members can view the field on the wizard page. The **Visibility Role** list contains all security roles defined for the identity store.

6. Click the **Advanced options** link to enter further details for the field.
7. As mentioned for *Visibility Role*, the field is visible to members of the selected role and roles having a priority value higher than the selected role.

   Use the **Exclude Role** option to exclude a higher priority role or roles from getting visibility on the field.

   In the **Exclude Role** area, select the check boxes for the roles you want to hide the field from.
8. In the **Tooltip** box, enter the text to display when a user hovers the mouse over the field.
9. In the **Max Length** box, enter a number that represents the maximum number of characters that users can enter as value for this field.

   Entering 0 indicates that users can enter an unlimited number of characters as value.
10. Use the **Search Object Types** area to specify the object types (User, Contact, and/or Group) that can be searched on the portal’s *Find* dialog box, to set as value for the field being defined.

    The following display types support the *Find* dialog box:

    - DN
    - DNs
    - Custom display types created with the Grid type

    When you select any of these display types, GroupID identifies that the value for the field being defined will have to be searched using the *Find* dialog box. The **Search Object Types** area is displayed, where you can select the required object type(s). For example, if you select Group, only groups can be searched and selected as value for the field being defined.

    You can launch the *Find* dialog box from multiple portal pages to search for objects to designate as owners, managers, additional owners, members, and more. While specifying the searchable object type(s), you must be aware of the kind of value required by the field in question.

The contact object type is not supported in a Microsoft Azure based identity store.

11. In the **Default Value** box, enter the default value that would be displayed in the field on the portal.

    Users can modify this value, provided that the **Is Read Only** check box is not selected.

12. Select the **Is Required** check box to make it mandatory for the user to provide a value for the field.
13. Select the **Is Read Only** check box if the field is meant to be read-only.
14. Select the **Filter Bad Words** check box to ensure that users do not enter any bad word, as specified on the **Bad Words List** tab (Figure 59), in this field.
15. Click **OK** to close the **Add Field** dialog box.

    The field is displayed in the **Fields** area on the **Add Category** or **Edit Category** dialog box (Figure 48). You can arrange the fields, modify a field, and even remove a field from the wizard page.

16. Click **OK** on the **Add Category** or **Edit Category** dialog box (Figure 48).
17. On the toolbar, click **Save** 💾.

Modify a field on a wizard page

1. On the **Update** tab (Figure 47), select a wizard page (category) to edit its field(s) and click **Edit**.

   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).

2. In the **Fields** area, select the field to modify and click **Edit**.

   The **Edit Field** dialog box is displayed, which is similar to the **Add Field** dialog box (Figure 49).

3. Refer to the steps under the figure to modify the required information and click **OK** to close the **Edit Field** dialog box.
4. Click **OK** on the **Edit Category** dialog box.
5. On the toolbar, click **Save** 💾.

Arrange the fields on a wizard page

1. On the **Update** tab (Figure 47), select the required page from the **Name** list and click **Edit**.

   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).

2. In the **Fields** area, select the required field and click ↑ or ↓ to rearrange the fields on the wizard page.
3. Click **OK** on the **Edit Category** dialog box.
4. On the toolbar, click **Save** 💾.

Remove a field from a wizard page

1. On the **Update** tab (Figure 47), select a wizard page (category) to remove a field from it and click **Edit**.

   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).

2. In the **Fields** area, select the field you want to remove and click **Remove**.
3. Click **OK** to close the **Edit Category** dialog box.
4. On the toolbar, click **Save** 💾.

Customize Object Properties pages

Self-Service enables you to customize the property pages displayed on the portal for these directory objects:

- User
- Contact
- Group
- Smart Group
- Computer: In the Self-Service portal, the computer object type is only available for adding to the membership of a group. Its properties are read-only.
- Mailbox

The computer and contact object types are not available for a Microsoft Azure based identity store.

In the Self-Service portal, the property page of an object has multiple tabs, where each tab groups similar attributes. These tabs are referred to as categories.

Customization of an object's property page includes:

At the category level:

- Adding a new tab (referred to as a category) to a properties page
- Modifying the properties of an existing tab
- Removing a tab from a properties page

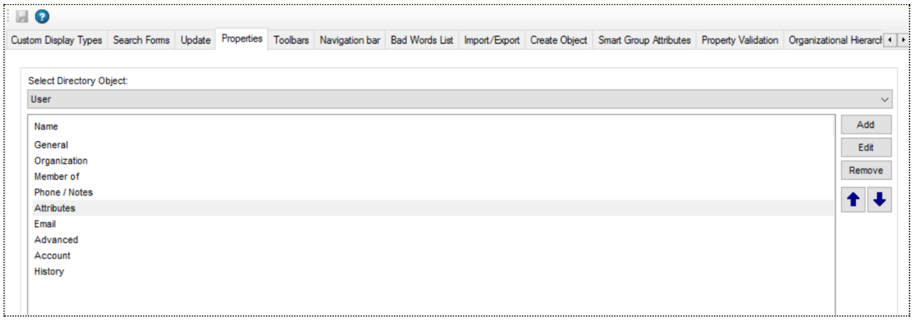
At the field level:

- Adding a field to a tab
- Modifying the properties of a field on a tab
- Arranging the fields on a tab
- Removing a field from a tab

Add a new tab (category)

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Properties** tab.



Select Directory Object: User

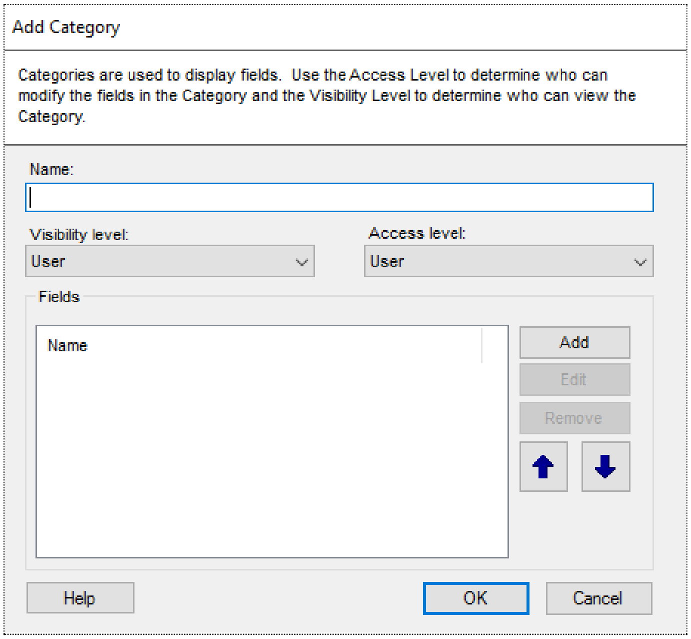
Name
General
Organization
Member of
Phone / Notes
Attributes
Email
Advanced
Account
History

Figure 50: Properties tab

4. From the **Select Directory Object** list, select a directory object to add a tab to its properties page.

The **Name** list shows the tabs (categories) currently available on the object's properties page.

5. Click **Add.** The **Add Tab/Category** dialog box is displayed.



Add Category

Categories are used to display fields. Use the Access Level to determine who can modify the fields in the Category and the Visibility Level to determine who can view the Category.

Name:

Visibility level: User

Access level: User

Figure 51: Add Tab/Category dialog box

6. In the **Name** box, type a name for the category. The tab will be displayed on the properties page with this name.

7. From the **Visibility level** drop-down list, select a security role. The category would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   - Select **Never** to hide the category from all users.
   - Select **Manager and Owner** to make the category visible only to the owner (in case of a group) or manager (in case of a user or contact). It would not be visible to any other user, such as group members or the user itself.

     For example, if the *Manager and Owner* role is selected for the *Email* tab in group properties, the tab would be visible to group owners for their respective groups in the portal.

     Similarly, if the *Manager and Owner* role is selected for the *Account* tab in user properties, the tab would be visible to managers for their respective direct reports in the portal.

- If you have selected ‘User’ or ‘Mailbox’ in the **Select Directory Object** list, the *Self* option will also be available in the **Visibility level** drop-down list.

  Select **Self** to make the category visible only to the logged-in user. It would not be visible to any other user, such as the user’s manager or a role with a higher priority value.

  For example, if the *Self* role is selected for the *General* tab in user properties, it means that a user can view the *General* tab of his or her properties page only. He or she cannot view this tab on the properties page of another user. A role with a higher priority value cannot see it for another user, user managers cannot view it for their respective direct reports, and even a role with the ‘Manage any profile’ permission in the identity store cannot view it for other users.

The visibility level determines the security roles whose members can view the category on the **Properties** page. The **Visibility level** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

8. From the **Access level** drop-down list, select a security role. Users of this role as well as of roles with a priority value higher than the selected role can add/update the values of fields on this tab.

   - Select **Never** to make the fields on this tab non-editable for all users.

   - Select **Manager and Owner** to enable only the owner (in case of a group) or manager (in case of a user or contact) to specify or modify the value of the fields on the tab. It would not be editable for any other user, such as group members or the user itself.

     For example, if the *Manager and Owner* role is selected for the *Email* tab in group properties, it means that only group owners can specify or modify the values of fields on this tab for their respective groups in the portal. A role with a higher priority value cannot change the value; group members cannot change the value; and even a role with the ‘Manage any Group’ permission in the identity store cannot change the value.

   - If you have selected ‘User’ or ‘Mailbox’ in the **Select Directory Object** list, the *Self* option will also be available in the **Access level** drop-down list.

     Select **Self** to enable only the logged-in user to specify or modify the value of the fields on the tab. It would not be editable for the user’s manager or even for a role with a higher priority value

For example, if the *Self* role is selected for the *General* tab in user properties, it means that only the user can update the values of fields on the *General* tab of his or her properties page. A role with a higher priority value cannot change the values; the user's manager cannot change the values; and even a role with the 'Manage any profile' permission in the identity store cannot change the values.

The access level determines whether a user can modify the fields on the tab. The **Access level** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

9. To add fields to the tab, see Add a new field to a tab on page 91.
10. Click **OK** to close the **Add Tab/Category** dialog box.
11. On the toolbar, click **Save** 💾.

Modify the properties of a tab (category)

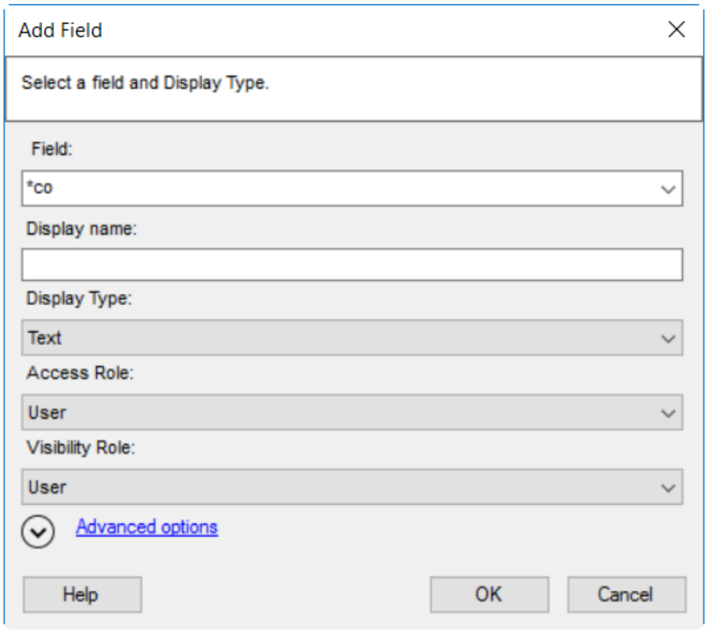
1. On the **Properties** tab (Figure 50), select the required directory object and then the tab to be modified.
2. Click **Edit**.
3. The **Edit Tab/Category** dialog box is displayed, which is similar to the **Add Tab/Category** dialog box (Figure 51). Refer to the instructions under the figure to edit the properties page.

Remove a tab from an object's properties page

1. On the **Properties** tab (Figure 50), select the required directory object and then the tab to be removed.
2. Click **Remove**.
3. On the toolbar, click **Save** 💾.

Add a new field to a tab

1. On the **Add Tab/Category** or **Edit Tab/Category** dialog box (Figure 51), click **Add** in the **Fields** area. The **Add Field** dialog box is displayed.



Add Field

Select a field and Display Type.

Field: *co

Display name:

Display Type: Text

Access Role: User

Visibility Role: User

Figure 52: Add Field dialog box

2. From the **Field** list, select a schema attribute to link to this field.
3. In the **Display Name** box, type a display name for the field. This name is the field's label on the properties page.
4. From the **Display Type** drop-down list, select the display type to use for rendering this field on the tab.

   The list contains all basic and custom display types defined on the **Custom Display Types** tab (Figure 14).
5. From the **Access level** drop-down list, select a security role. Users of this role and of roles with a priority value higher than the selected role can add/update the value of this field.
   - Select **Never** to make this field non-editable for all users.
   - Select **Manager and Owner** to enable only the owner (in case of a group) or manager (in case of a user or contact) to specify or modify the value of this field. It would not be editable for any other user, such as group members or the user itself.

     For example, if the *Manager and Owner* role is selected for the *Expiration Date* field on the *General* tab in group properties, it means that only group owners can specify or modify the value of this field for their respective groups in the portal. A role with a higher priority value cannot change the value; group members cannot change the value; and even a role with the ‘Manage any Group’ permission in the identity store cannot change the value.

- If you have selected ‘User’ or ‘Mailbox’ in the **Select Directory Object** list, the *Self* option will also be available in the **Access Role** drop-down list.

  Select **Self** to enable only the logged-in user to specify or modify the value of the field. It would not be editable for any other user, such as the user’s manager or a role with a higher priority value.

  For example, if the *Self* role is selected for the *Notes* field on the *Phone / Notes* tab in user properties, it means that only the user can update the value of this field on his or her properties page. A role with a higher priority value cannot change the value; the user’s manager cannot change the value; and even a role with the ‘Manage any profile’ permission in the identity store cannot change the value.

The access level determines whether a user can add/update the value of this field. The **Access level** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

6. From the **Visibility Role** drop-down list, select a security role. The field would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   - Select **Never** to hide the field from all users.
   - Select **Manager and Owne**r to make the field visible only to the owner (in case of a group) or manager (in case of a user or contact). It would not be visible to any other user, such as group members or the user itself.

     For example, if the *Manager and Owner* role is selected for the *Expiration Date* field on the **General** tab in group properties, it means that the field would be visible to group owners for their respective groups in the portal.

     Similarly, if the *Manager and Owner* role is selected for the *Manager* field on the *Organization* tab in user properties, it means that the field would be visible to managers for their respective direct reports in the portal.
   - If you have selected ‘User’ or ‘Mailbox’ in the **Select Directory Object** list, the *Self* option will also be available in the **Visibility Role** drop-down list.

     Select **Self** to make the field visible only to the logged-in user. It would not be visible to any other user, such as the user’s manager or a role with a higher priority value.

For example, if the *Self* role is selected for the *Notes* field on the *Phone/Notes* tab in user properties, it means that the user can view the field on his or her properties page only. He or she cannot see this field on the properties page of another user. A role with a higher priority value cannot see it for another user, managers cannot view it for their respective direct reports, and even a role with the 'Manage any profile' permission in the identity store cannot view it for other users.

The visibility level determines the security roles whose members can view the field on the tab. The **Visibility Role** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

7. Click the **Advanced options** link to enter further details for the field.
8. As mentioned for *Access Role* and *Visibility Role*, the field is accessible and visible to members of the selected role and roles having a priority value higher than the selected role.

   Use the **Exclude Role** option to exclude a higher priority role or roles from getting access and visibility on the field.

   In the **Exclude Role** area, select the check boxes for the roles to whom you want to deny access and visibility on the field.
9. In the **Tooltip** box, enter the text to display when a user hovers the mouse over the field.
10. In the **Max Length** box, enter a number that represents the maximum number of characters that users can enter as value for this field.

    Entering 0 indicates that users can enter an unlimited number of characters as value.
11. The **Image Attribute** list is available when 'DN' is selected as the display type. This list supports 'thumbnailPhoto' as its value.
    - Select the 'thumbnailPhoto' attribute from the **Image Attribute** drop-down list when you want to auto upload an image with the field being defined. For example, when you apply this setting to the *Primary Manager* field in group properties. then the primary manager's image will be displayed alongside his or her name on the portal's group properties page.

      Note that for the image to display, the 'thumbnailPhoto' attribute must have a value stored; in case of no value, a blank image is displayed.

- If you do not want to auto upload an image with the field, clear the value in the **Image Attribute** box.

12. Use the **Search Object Types** area to specify the object types (User, Contact, and/or Group) that can be searched on the portal's *Find* dialog box, to set as value for the field being defined.

    The following display types support the *Find* dialog box:

    - DN
    - DNs
    - Custom display types created with the Grid type

    When you select any of these display types, GroupID identifies that the value for the field being defined will have to be searched using the *Find* dialog box. The **Search Object Types** area is displayed, where you can select the required object type(s). For example, if you select Group, only groups can be searched and selected as value for the field being defined.

    You can launch the *Find* dialog box from multiple portal pages to search for objects to designate as owners, managers, additional owners, members, and more. While specifying the searchable object type(s), you must be aware of the kind of value required by the field in question.

The contact object type is not supported in a Microsoft Azure based identity store.

13. Select the **Is Required** check box to make it mandatory for the user to provide a value for the field.
14. Select the **Is Read Only** check box if the field is meant to be read-only.
15. Select the **Filter Bad Words** check box to ensure that users do not enter any bad word, as specified on the **Bad Words List** tab (Figure 59), in this field.
16. Click **OK** to close the **Add Field** dialog box.

    The field is displayed in the **Fields** area on the **Add Tab/Category** or **Edit Tab/Category** dialog box (Figure 51). You can arrange the fields, modify a field, and even remove a field from the tab.

17. Click **OK** on the **Add Tab/Category** or **Edit Tab/Category** dialog box (Figure 51).
18. On the toolbar, click **Save** 💾.

Modify a field on a tab

1. On the **Properties** tab (Figure 50), select the required directory object and then the category for which you want to edit the field(s).
2. Click **Edit**.

   The **Edit Tab/Category** dialog box is displayed, which is similar to the **Add Tab/Category** dialog box (Figure 51).
3. In the **Fields** area, select the field to modify and click **Edit**.

   The **Edit Field** dialog box is displayed, which is similar to the **Add Field** dialog box (Figure 52).

   Refer to the steps under the figure to modify the required information and click **OK** to close the **Edit Field** dialog box.
4. Click **OK** on the **Edit Tab/Category** dialog box.
5. On the toolbar, click **Save** 💾.

Arrange the fields on a tab

1. On the **Properties** tab (Figure 50), select the required directory object and then the required category.
2. Click **Edit**.

   The **Edit Tab/Category** dialog box is displayed, which is similar to the **Add Tab/Category** dialog box (Figure 51).
3. In the **Fields** area, select the required field and click ↑ or ↓ to rearrange the order of fields on the tab.
4. Click **OK** on the **Edit Tab/Category** dialog box.
5. On the toolbar, click **Save** 💾.

Remove a field from a tab

1. On the **Properties** tab (Figure 50), select the required directory object and then the category you want to remove a field from.
2. Click **Edit**.
   The **Edit Tab/Category** dialog box is displayed, which is similar to the **Add Tab/Category** dialog box (Figure 51).

3. In the **Fields** area, select the field to remove and click **Remove**.
4. Click **OK** on the **Edit Tab/Category** dialog box.
5. On the toolbar, click **Save** 💾.

Customize the Toolbars

Toolbars are available on different pages of a Self-Service portal; however, not all of these toolbars are customizable. You can only customize the following toolbars:

- **User**: Available on the My Profile and user properties pages of the portal.
- **Group**: Available on the group properties page.
- **Default Search**: Available on the search results pages for Quick search and Advanced search.
- **Users Search**: Available on the My Direct Reports page of the portal. It is also available on the search results page that opens when a user clicks the Users link on the navigation bar and performs a search.
- **Groups Search**: Available on the **My Groups** page of the portal. It is also available on the search results page that opens when a user clicks the **Groups** link on the navigation bar and performs a search.
- **Members grid**: Available on the **Members** tab in group properties.
- **User members of grid**: Available on the **Member Of** tab in user properties.
- **Computer members of grid**: Available on the **Member Of** tab in computer properties.
- **Additional owner**: Available on the **Owner** tab in group properties.
- **Additional manager**: Available on the **Organization** tab in user properties.
- **Create group wizard – members**: Available on **Members** page of the Create Group wizard.
- **Create group wizard - additional owner**: Available on **Owners** page of the Create Group wizard.
- **Group member of grid**: Available on the **Member Of** tab in group properties.
- **Contact member of grid**: Available on the **Member Of** tab in contact properties.

- **Direct reports grid**: Available on the **Organization** tab in user properties.

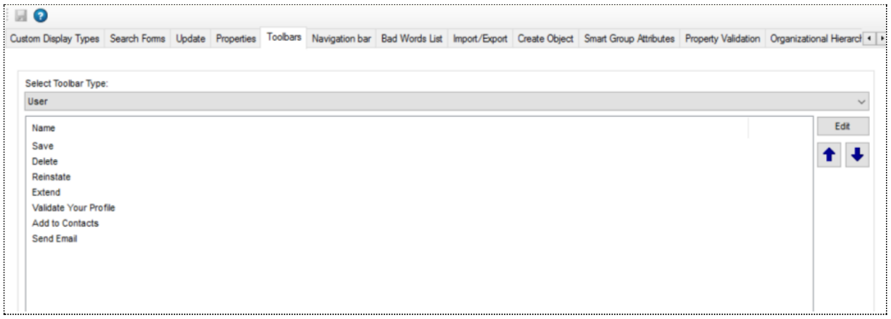
The **Computer members of grid** and **Contact member of grid** toolbars are not available for a Microsoft Azure based identity store.

The buttons available on these toolbars are predefined. You cannot add or remove a button; you can only edit a few details for each button, such as the button text and tooltip text.

Modify the properties of a toolbar button

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Toolbars** tab.



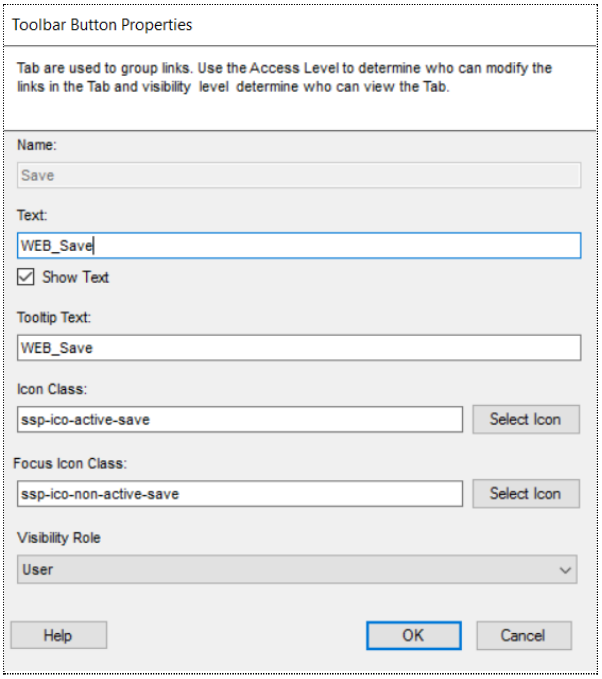
Select Toolbar Type: User

Name
Save
Delete
Reinstate
Extend
Validate Your Profile
Add to Contacts
Send Email

Figure 53: Toolbars tab

4. From the **Select Toolbar Type** drop-down list, select the toolbar you want to modify.

   The **Name** area lists all buttons on this toolbar.
5. Select a button to modify it and click **Edit**.



Toolbar Button Properties

Tab are used to group links. Use the Access Level to determine who can modify the links in the Tab and visibility level determine who can view the Tab.

Name:
Save

Text:
WEB_Save

☑ Show Text

Tooltip Text:
WEB_Save

Icon Class:
ssp-ico-active-save

Focus Icon Class:
ssp-ico-non-active-save

Visibility Role
User

Figure 54: Toolbar Button Properties dialog box

6. Modify the following information as required:

    a. **Name** – The name of the toolbar button. It is non-editable.

    b. **Text** – The text that would appear on the button as its name.

    c. **Show Text** – Select this check box to display the text on the button; else the button would be displayed without the text.

    d. **Tooltip Text** - The text to appear when the user hovers the pointer over the button.

    e. **Icon Class** – Use the **Select Icon** button to browse and select the image to be displayed on the toolbar for the button.

    f. **Focus Icon Class** – Use the **Select Icon** button to browse and select the image to be displayed when a user hovers the mouse over this button.

    g. **Visibility Role** – Select a security role. The toolbar button would be visible to users of the selected role and to roles with a priority value higher than the selected role.

       Select **Never** to hide the button from all users.

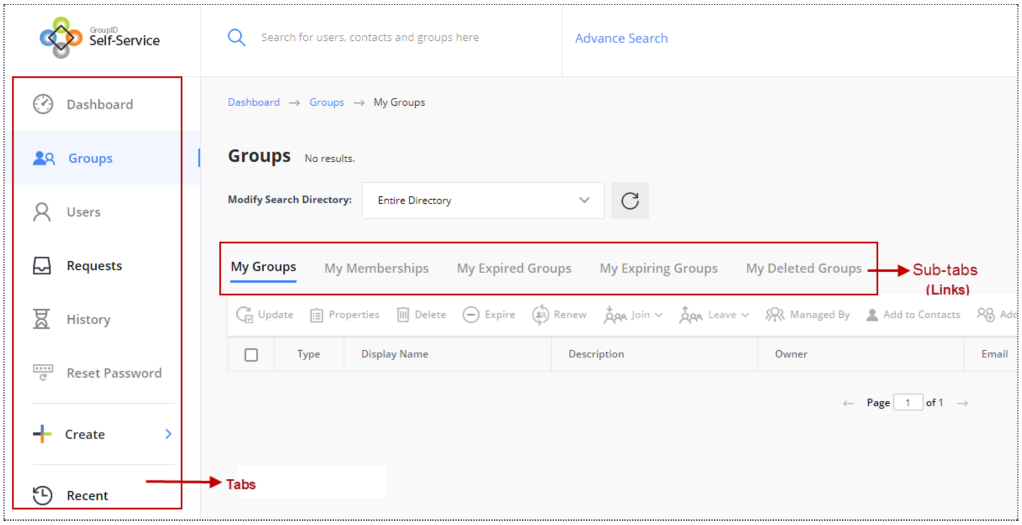
       The visibility level determines the security role(s) whose members can view the button on the toolbar. The **Visibility Role** list contains all security roles defined for the identity store.

7. Click **OK** on the **Toolbar Button Properties** dialog box.
8. You can rearrange the order of buttons on a toolbar.
   On the **Toolbars** tab (Figure 53), select a toolbar and use ↑ and ↓ to rearrange its buttons.
9. On the toolbar, click **Save** 💾.

Customize the Navigation bar

You can customize items on the left navigation bar of a Self-Service portal. Items consist of tabs and their sub-tabs that redirect users to other pages of the portal. Sub-tabs are referred to as *links*.

On clicking a tab on the navigation bar, users are redirected to a page that contains the links defined under it. It is as:



Sub-tabs (Links)

Tabs

Figure 55: Navigation bar in the portal

Self-Service enables you to customize the tabs and their respective links for each functionality mode. Customization includes:

At the tab level:

- Adding a new tab on the navigation bar
- Modifying the properties of an existing tab
- Removing a tab from the navigation bar

At the link level:

- Adding a new link for a tab

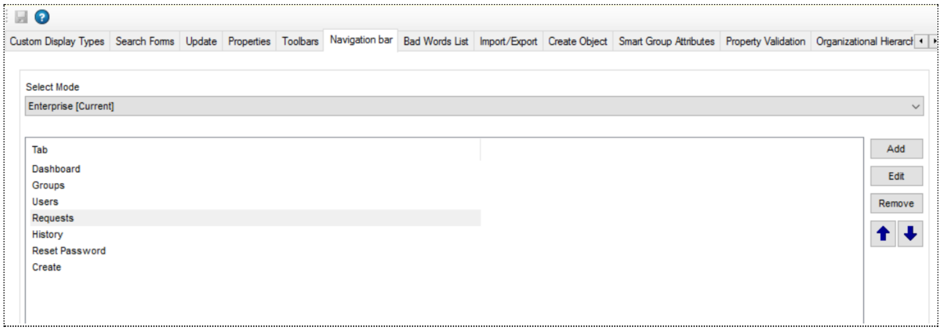
- Modifying the properties of a link
- Arranging the links for a tab
- Removing a link

If a tab or link is being used in multiple functionality modes, then changes made to it in one mode are restricted to that mode only.

Add a new tab on the navigation bar

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Navigation bar** tab.

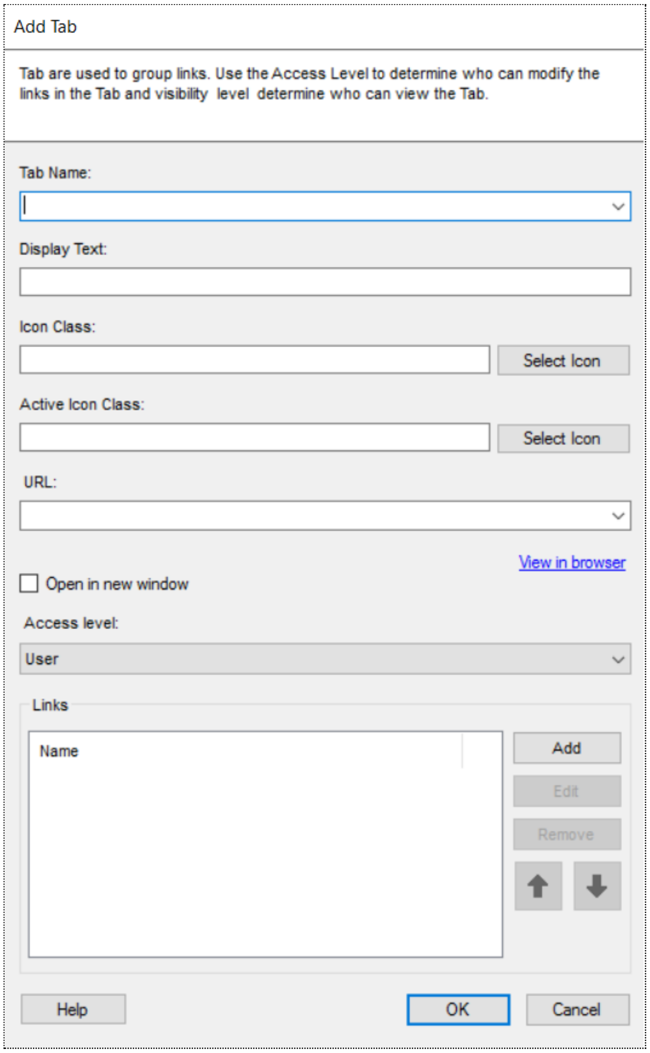
   Select Mode: Enterprise [Current]

   Tab
   Dashboard
   Groups
   Users
   Requests
   History
   Reset Password
   Create

   Figure 56: Navigation bar tab

   The Tab list displays a list of tabs for the selected functionality mode.
4. From the **Select Mode** list, select the functionality mode to add a new tab to.

   The tabs for the selected mode are displayed in the **Tab** list.
5. To add a new tab, click **Add**.



Add Tab

Tab are used to group links. Use the Access Level to determine who can modify the links in the Tab and visibility level determine who can view the Tab.

Tab Name:

Display Text:

Icon Class:

Active Icon Class:

URL:

□ Open in new window

Access level: User

Figure 57: Add Tab dialog box

6. In the **Tab Name** box, type a name for the new tab or select a pre-defined one from the list.

   Selecting a tab from the list populates its default configurations, which you can modify.

7. In the **Display Text** box, type the text to display as the tab title on the navigation bar.
8. Use the **Select Icon** button next to the **Icon Class** box to browse and select the image to be displayed with the tab name on the navigation bar.
9. Use the **Select Icon** button next to the **Active Icon Class** box to browse and select the image to be displayed when a user hovers the mouse over the tab name on the navigation bar.

10. In the **URL** box, provide the address of the page to display when a user clicks the tab.

    - To link a page in the portal, select the required page from the list.
    - To link to an external page or website, type its address.

    Click **View in browser** to preview the linked page in a browser window.

11. Select the **Open in new window** check box to open the linked page in a new browser window when the user clicks the tab.

12. From the **Access level** drop-down list, select a security role. The tab would be clickable for users of the selected role and to roles with a priority value higher than the selected role. For all other users, the tab would be greyed out (disabled) and users would not be able to access its respective page.

    Select **Never** to grey out the tab for all users.

    The access level determines the security role(s) whose members can access the tab on the portal's navigation bar. The **Access level** list contains all security roles defined for the identity store.

13. Use the **Links** area to add, edit or remove links for this tab.
    To define a new link, see Add a link for a tab on page 104.

14. Click **OK** to close the dialog box.

15. On the toolbar, click **Save** 💾.

Modify a tab

1. On the **Navigation bar** tab (Figure 56), select the required functionality mode and then the tab you want to modify.

2. Click **Edit**.

3. The **Edit Tab** dialog box is displayed, which is similar to the **Add Tab** dialog box (Figure 57). Refer to the instructions under the figure to edit the information for the tab.

Remove a tab

1. On the **Navigation bar** tab (Figure 56), select the required functionality mode and then the tab you want to remove from the portal's navigation bar.

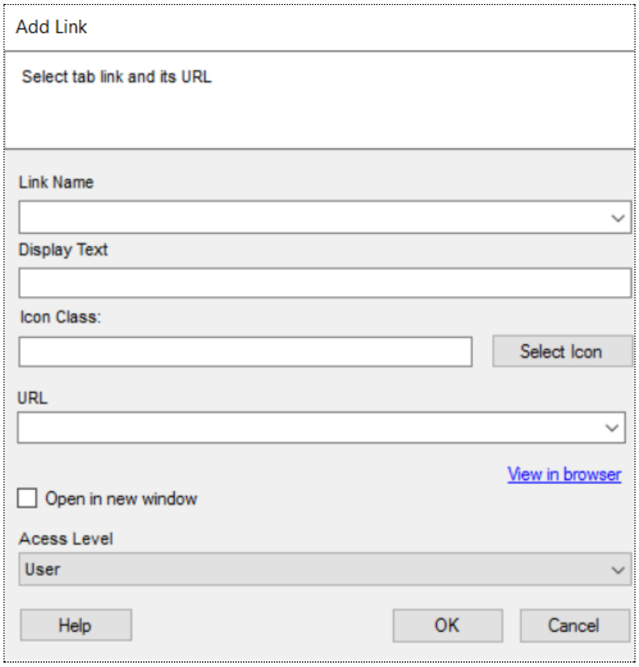
2. Click **Remove**.

3. On the toolbar, click **Save** .

Removing a tab also removes all links defined for it.

Add a link for a tab

1. On the **Add Tab** or **Edit Tab** dialog box (Figure 57), click **Add** in the **Links** area to add a new link under the tab.



Add Link

Select tab link and its URL

Acess Level: User

Figure 58: Add Link dialog box

2. In the **Link Name** box, type a name for the new link or select a pre-defined one from the list.

   Selecting a link from the list populates its default configurations, which you can modify.

3. In the **Display Text** box, type the text to display for the link in the portal.

4. Use the **Select Icon** button next to the **Icon Class** box to browse and select the image to be displayed with the link name.

5. In the **URL** box, provide the address of the page to display when a user clicks the link.

   - To link a page in the portal, select the required page from the list.
   - To link to an external page or website, type its address.

   Click **View in browser** to preview the linked page in a browser window.

6. Select the **Open in new window** check box to open the linked page in a new browser window when a user clicks the link.
7. From the **Access level** drop-down list, select a security role. The link would be clickable for users of the selected role and to roles with a priority value higher than the selected role. For all other users, the link would be greyed out (disabled) and users would not be able to access its respective page.

   Select **Never** to grey out the link for all users.

   The access level determines the security role(s) whose members can access the link in the portal. The **Access level** list contains all security roles defined for the identity store.
8. Click **OK** to close the **Add Link** dialog box.

   The link is displayed in the **Links** area on the **Add Tab** or **Edit Tab** dialog box (Figure 57). You can rearrange the links, modify a link, and even remove a link.
9. Click **OK** on the **Add Tab** or **Edit Tab** dialog box (Figure 57).
10. On the toolbar, click **Save** 💾.

Modify a link

1. On the **Navigation bar** tab (Figure 56), select the required functionality mode and then the tab for which you want to modify link(s).
2. Click **Edit**.

   The **Edit Tab** dialog box is displayed, which is similar to the **Add Tab** dialog box (Figure 57).
3. In the **Links** area, select the link to modify and click **Edit**.

   The **Edit Link** dialog box is displayed, which is similar to the **Add Link** dialog box (Figure 58).
4. Refer to the steps under the figure to modify the required information and click **OK** to close the **Edit Link** dialog box.
5. Click **OK** on the **Edit Tab** dialog box.
6. On the toolbar, click **Save** 💾.

Change the order of links for a tab

1. On the **Navigation bar** tab (Figure 56), select the required functionality mode and then the tab for which you want to rearrange the links.
2. Click **Edit**.

   The **Edit Tab** dialog box is displayed, which is similar to the **Add Tab** dialog box (Figure 57).
3. In the **Links** area, select the required link and click ↑ or ↓.to move it up or down under the tab.
4. Click **OK** on the **Edit Tab** dialog box.
5. On the toolbar, click **Save** 💾.

Remove a link

1. On the **Navigation bar** tab (Figure 56), select the required functionality mode and then the tab for which you want to remove a link.
2. Click **Edit**.

   The **Edit Tab** dialog box is displayed, which is similar to the **Add Tab** dialog box (Figure 57).
3. In the **Links** area, select the link to remove and click **Remove**.
4. Click **OK** to close the dialog box.
5. On the toolbar, click **Save** 💾.

Manage the Bad Words List

Self-Service enables you to restrict portal users from saving data containing words that might be offensive. You can maintain a list of such words for each portal separately.

The Bad Words list feature applies to:

- Fields with the ‘Filter Bad Words’ option enabled in field properties.
- History notes that a user enters for a logged history action.

If a user enters a value that contains a word on the list, the portal will not save the entry until the word is removed or corrected.

Add a bad word to the list

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Bad Words List** tab.

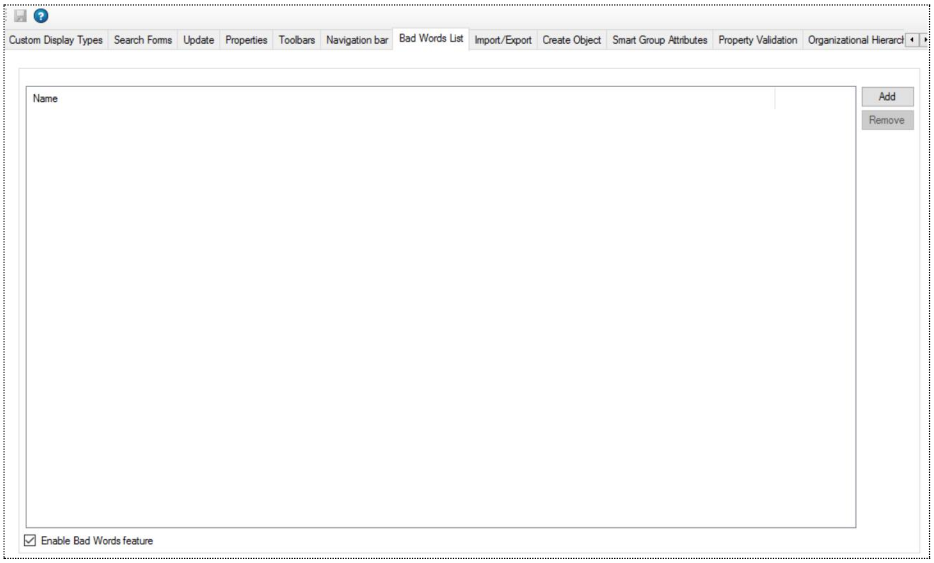
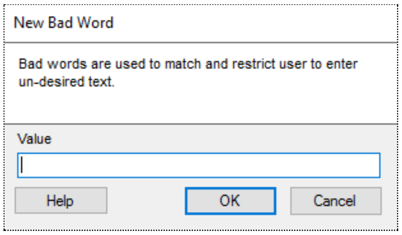


Figure 59: Bad Words List tab

4. Click **Add**.


New Bad Word

Bad words are used to match and restrict user to enter un-desired text.

Value

Figure 60: New Bad Word dialog box

5. In the **Value** box, type the word that you want to block from use by portal users.
6. Click **OK** to close the dialog box.
   The bad word is displayed in the **Name** list on the **Bad Words List** tab.

7. Make sure that the **Enable Bad Words feature** check box is selected to enforce the implementation of the bad words filter for the portal.
8. On the toolbar, click **Save** 💾.

Remove a bad word from the list

1. On the **Bad Words List** tab (Figure 59), select the bad word that you want to remove from the list.
2. Click **Remove**.
3. On the toolbar, click **Save** 💾.

Disable the Bad Words feature for a portal

1. On the **Bad Words List** tab (Figure 59), clear the **Enable Bad Words feature** check box.
2. On the toolbar, click **Save** 💾.

You can enable the feature any time by selecting the **Enable Bad Words feature** check box.

Specify schema attributes for importing/exporting group members and owners

In the Self-Service portal, users can import and export members and additional owners for a group using an external file.

On the **Import/Export** tab, you can specify schema attributes that will be used in the export and import functions. You also have to provide a plain-language, user-friendly name for each attribute.

- The import action reads the objects' information from the external file and searches for matching objects in the directory based on field mapping (where a column name in the external file is mapped to any of the attributes specified here).

  Objects having the same values for the mapped fields are added to the membership or additional ownership of the target group.
- The export action reads the membership/additional ownership of the group and exports the values of the specified attributes for members/additional owners to an external file.

The schema attributes you specify on the **Import/Export** tab are displayed with their user-friendly names on the following wizards in the Self-Service portal.

Wizard Name	Description
Import Members	This wizard is used to import members into a group using an external file. Users can launch it from the Members page on the Create New Group wizard and from the Members tab in group properties.
Export Members	This wizard is used to export the members of a group to an external file. Users can launch it from the Members tab in group properties.
Import Additional Owners	This wizard is used to import additional owners for a group using an external file. Users can launch it from the Owners page on the Create New Group wizard and from the Owner tab in group properties.
Export Additional Owners	This wizard is used to export the additional owners of a group to an external file. Users can launch it from the Owner tab in group properties.

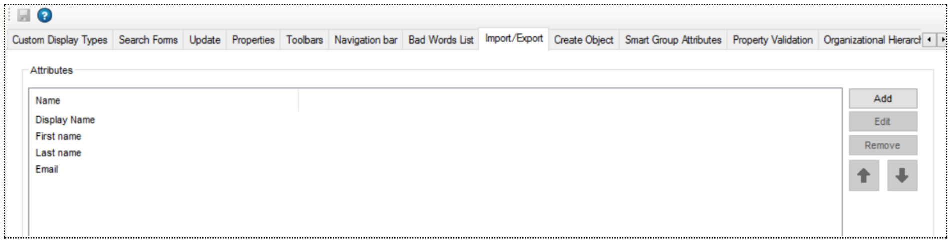
Table 17: Import/Export wizards in the portal

The attributes you specify apply to all four wizards. You cannot specify a different set of attributes for any of these wizards.

Specify an attribute for import and export

1. In the GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Import/Export** tab.



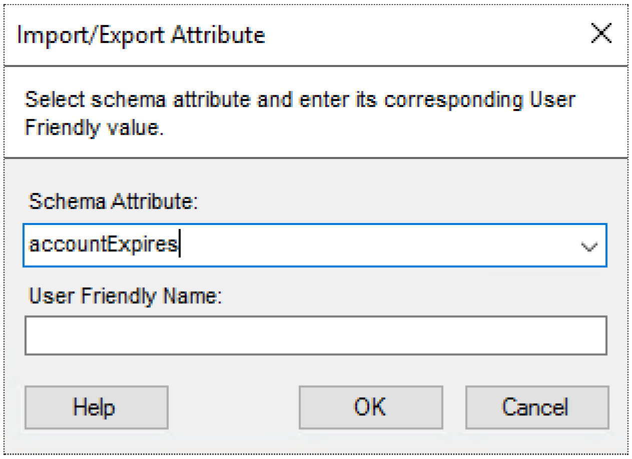
Attributes

Name
Display Name
First name
Last name
Email

Figure 61: Import/Export tab

Schema attributes for *first name*, *last name*, and *email* have been specified in the default portal template. These attributes are available in the portal for the export and import of group members and additional owners, as discussed in Table 17.

4. Click **Add**.



Import/Export Attribute

Select schema attribute and enter its corresponding User Friendly value.

Schema Attribute: accountExpires

User Friendly Name:

Figure 62: Import/Export Attribute dialog box

5. In the **Schema Attribute** list, select a schema attribute to be used for import/export.
6. In the **User Friendly Name** box, type an easy and meaningful name for the selected attribute. The attribute will be displayed with this name on the Import Members, Export Members, Import Additional Owners, and Export Additional Owners wizards in the portal.
7. Click **OK**.
   The attribute’s user friendly name is displayed on the **Import/Export** tab.
8. On the toolbar, click **Save** 🖫.

Edit an attribute's user-friendly name

1. On the **Import/Export** tab (Figure 61), select an attribute from the **Name** list and click **Edit**.
2. On the **Import/Export Attribute** dialog box (Figure 62), modify the required information. Refer to the instructions under the figure for help.
3. On the toolbar, click **Save** .

Remove an attribute from import and export

1. On the **Import/Export** tab (Figure 61), select the attribute you want to remove from the Import Members, Export Members, Import Additional Owners, and Export Additional Owners wizards in the portal.
2. Click **Remove**.
3. On the toolbar, click **Save** .

Customize the Object Creation wizards

Using a Self-Service portal, users can create different directory objects, namely:

- User
- Contact
- Static Group
- Smart Group
- Mailbox

The contact object type is not supported in a Microsoft Azure based identity store.

The portal provides a separate wizard for creating each of these objects. On the **Create Object** tab, you can customize these wizards. You can:

At the wizard level:

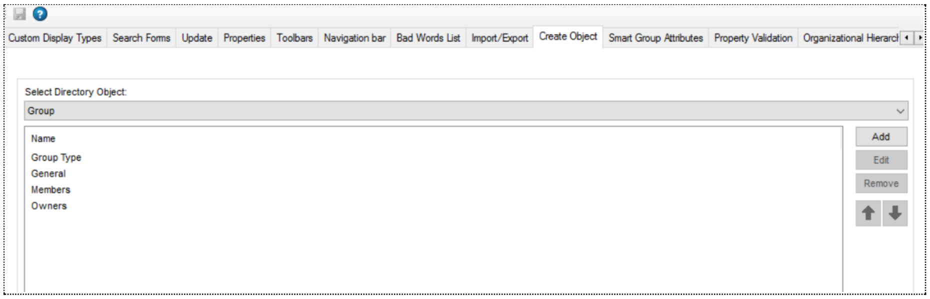
- Add a new page to a wizard
- Modify the properties of a wizard page
- Remove a page from a wizard

At the field level:

- Add a field to a wizard page
- Modify the properties of a field
- Rearrange the fields on a wizard page
- Remove a field from a wizard page

Add a new wizard page

1. In the GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.
   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Create Object** tab.



Select Directory Object: Group

Name
Group Type
General
Members
Owners

Figure 63: Create Object tab

4. From the **Select Directory Object** list, select a directory object to add a new page to its creation wizard.

   The **Name** list displays the existing pages of the wizard.
5. Click **Add**. The **Add Category** dialog box is displayed, which is the same as shown in Figure 48. Follow the instructions under the figure to add a new page to the wizard.

Modify the properties of a wizard page

1. On the **Create Object** tab (Figure 63), select a directory object to edit a page in its creation wizard.

2. In the **Name** list, select a wizard page to modify its properties and click **Edit**.

   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48). Refer to the instructions under the figure to edit the wizard page.

Remove a page from a wizard

1. On the **Create Object** tab (Figure 63), select a directory object to remove a page from its creation wizard.
2. In the **Name** list, select the wizard page you want to remove and click **Remove**.
3. On the toolbar, click **Save** 💾.

Add a new field to a wizard page

1. On the **Create Object** tab (Figure 63), select a directory object to add a new field to its creation wizard.
2. In the **Name** list, select the wizard page you want to add a field to, and click **Edit**.
3. The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).

   Click **Add** in the **Fields** area; the **Add Field** dialog box is displayed (Figure 49). Follow the instructions under the figure to add a new field to the wizard page.

Modify the properties of a field

1. On the **Create Object** tab (Figure 63), select the required directory object and then the wizard page for which you want to edit the field(s).
2. Click **Edit**.

   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).
3. In the **Fields** area, select the field to modify and click **Edit**.

   The **Edit Field** dialog box is displayed, which is similar to the **Add Field** dialog box (Figure 49).

Follow the instructions under the figure to modify the properties of the field.

Arrange the fields on a wizard page

1. On the **Create Object** tab (Figure 63), select the required directory object and then a wizard page to rearrange its fields.
2. Click **Edit**.

   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).
3. In the **Fields** area, select the required field and click ↑ or ↓ to rearrange the fields on the page.
4. Click **OK** on the **Edit Category** dialog box.
5. On the toolbar, click **Save** 💾.

Remove a field from a wizard page

1. On the **Create Object** tab (Figure 63), select the required directory object and then the wizard page you want to remove a field from.
2. Click **Edit**.

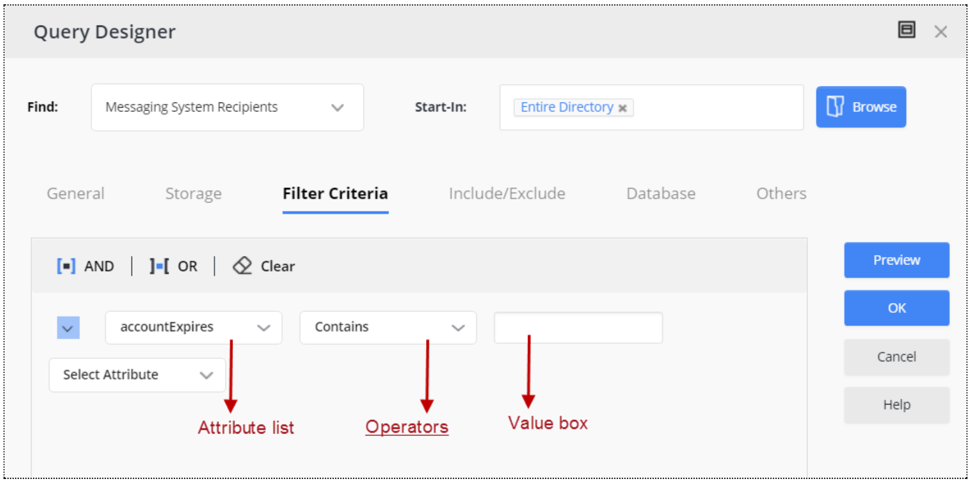
   The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 48).
3. In the **Fields** area, select the field to remove and click **Remove**.
4. Click **OK** on the **Edit Category** dialog box.
5. On the toolbar, click **Save** 💾.

Specify Smart Group Query attributes

While creating a Smart Group in a Self-Service portal, users have to design a query for Smart Group membership update.

On the **Smart Group Attributes** tab, you can specify what schema attributes of the connected directory would be available to portal users on the Filter Criteria tab of the Query Designer for building Smart Group queries.

For each attribute, you can also specify the operator(s) that can be applied to it while creating queries, as well as specify the maximum number of characters that can be entered as value.


Query Designer

Find: Messaging System Recipients

Start-In: Entire Directory

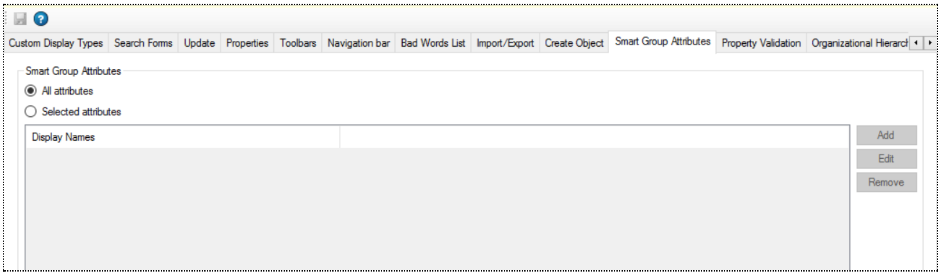
accountExpires Contains

Figure 64: Query Designer - Filter Criteria tab

Provide all schema attributes for Smart Group Query

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Smart Group Attributes** tab.

   
   Smart Group Attributes

   ● All attributes

   ○ Selected attributes

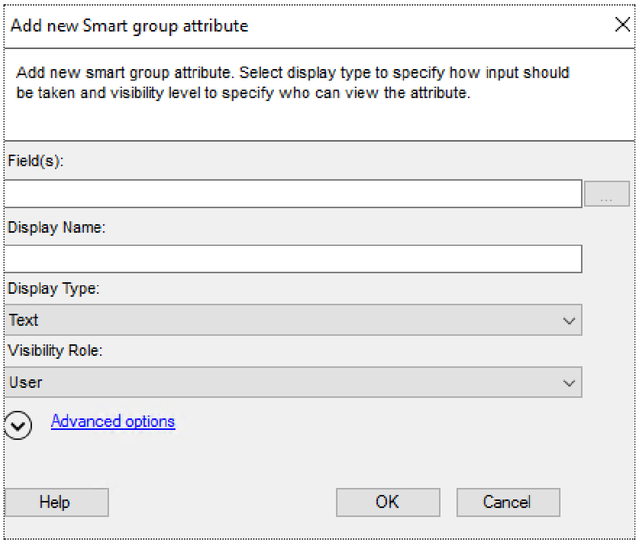
   Figure 65: Smart Group Attributes tab
4. Select the **All attributes** option button under **Smart Group Attributes**.

   All schema attributes would be available to portal users for building Smart Group queries.
5. On the toolbar, click **Save** .

Provide selected schema attributes for Smart Group Query

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Smart Group Attributes** tab (Figure 65).
4. Select the **Selected attributes** option button under **Smart Group Attributes**.
5. To specify schema attributes that would be available to portal users for building Smart Group queries, click **Add**.



Add new Smart group attribute

Add new smart group attribute. Select display type to specify how input should be taken and visibility level to specify who can view the attribute.

Field(s):

Display Name:

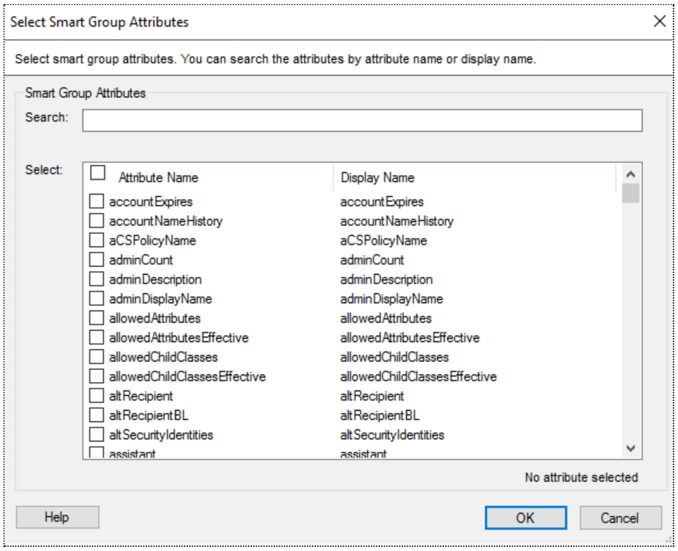
Display Type: Text

Visibility Role: User

Figure 66: Add new Smart Group attribute dialog box

6. Click the ellipsis button next to the **Field(s)** box to launch the **Select Smart Group Attribute** dialog box, where you can select one or more schema attributes. These attributes would be available in the Self-Service portal, where users can use them in building Smart Group queries.

   The **Select Smart Group Attributes** dialog box is as follows:



Select Smart Group Attributes

Select smart group attributes. You can search the attributes by attribute name or display name.

Smart Group Attributes

Search:

Select:

□ Attribute Name	Display Name
□ accountExpires	accountExpires
□ accountNameHistory	accountNameHistory
□ aCSPolicyName	aCSPolicyName
□ adminCount	adminCount
□ adminDescription	adminDescription
□ adminDisplayName	adminDisplayName
□ allowedAttributes	allowedAttributes
□ allowedAttributesEffective	allowedAttributesEffective
□ allowedChildClasses	allowedChildClasses
□ allowedChildClassesEffective	allowedChildClassesEffective
□ altRecipient	altRecipient
□ altRecipientBL	altRecipientBL
□ altSecurityIdentities	altSecurityIdentities
□ assistant	assistant

No attribute selected

Figure 67: Select Smart Group Attributes dialog box

Use the **Search** box to filter the schema attributes listed in the **Select** area.

a. Select the check boxes for the attributes that you want to make available in the Self-Service portal for building Smart Group queries.

b. Click **OK**.

   The selected attribute(s) get listed in the **Field(s)** box on the **Add new Smart Group attribute** dialog box (Figure 66). All other fields on the dialog box are auto populated with the default configurations of the attribute(s).

7. Use the **Display Name** box to specify a name for the attribute. The attribute would be displayed in the portal with this name.

   This box is not available if you select multiple attributes in the **Field(s)** box.

8. Use the **Display Type** drop-down list to specify the display type to use for rendering the attribute(s) on the portal. The list contains all basic and custom display types defined on the **Custom Display Types** tab (Figure 14).

   When multiple attributes are selected in the **Field(s)** box, this display type applies to each of them.

9. The **Visibility Role** drop-down list is for specifying a security role. The attribute(s) would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   Select **Never** to hide the attribute(s) from all users.

The visibility level determines the security role(s) whose members can view the attribute(s) for building a query. The **Visibility Role** list contains all security roles defined for the identity store.

10. Click the **Advanced options** link to enter further details for the attribute(s).
11. In the **ToolTip Text** box, enter the text to display when a user hovers the mouse over the attribute(s).
12. In the **Max Length** box, enter a number that represents the maximum number of characters that users can enter as value for each of the selected attribute(s).

    Entering 0 indicates that the attribute can accept an unlimited number of characters for its value.
13. The **Selected Operators** area lists the operators that can be applied to attributes while designing a Smart Group query in the portal.

    Select the check box for the operator(s) you want to associate with the selected attribute(s).
14. Click **OK** to close the dialog box.
15. On the toolbar, click **Save** 💾.

Edit a selected attribute

With the **Selected attributes** option button selected on the **Smart Group Attributes** tab (Figure 65) and one or more attributes specified, the **Edit** button is enabled. You can select an attribute to modify it.

1. On the **Smart Group Attributes** tab (Figure 65), select an attribute in the **Display Name** area and click **Edit** to modify its details.
2. The **Edit Smart Group attribute** dialog box is displayed, which is similar to the **Add new Smart Group attribute** dialog box (Figure 66), except that the **Field(s)** box is not editable in the edit function. It displays the name of the attribute being edited.

   Follow steps 7 to 15 in the Provide selected schema attributes for Smart Group Query section on page 116 to modify the attribute’s information.

Remove a selected attribute

With the **Selected attributes** option button selected on the **Smart Group Attributes** tab (Figure 65) and one or more attributes specified, the **Remove** button is enabled.

You can select an attribute to remove it. Removed attributes would not be available in the portal for building Smart Group queries.

1. On the **Smart Group Attributes** tab (Figure 65), select an attribute in the **Display Name** area and click **Remove**.
2. On the toolbar, click **Save** 💾.

Manage Property Validation attributes

In GroupID, property validation applies to:

- Users
- Groups

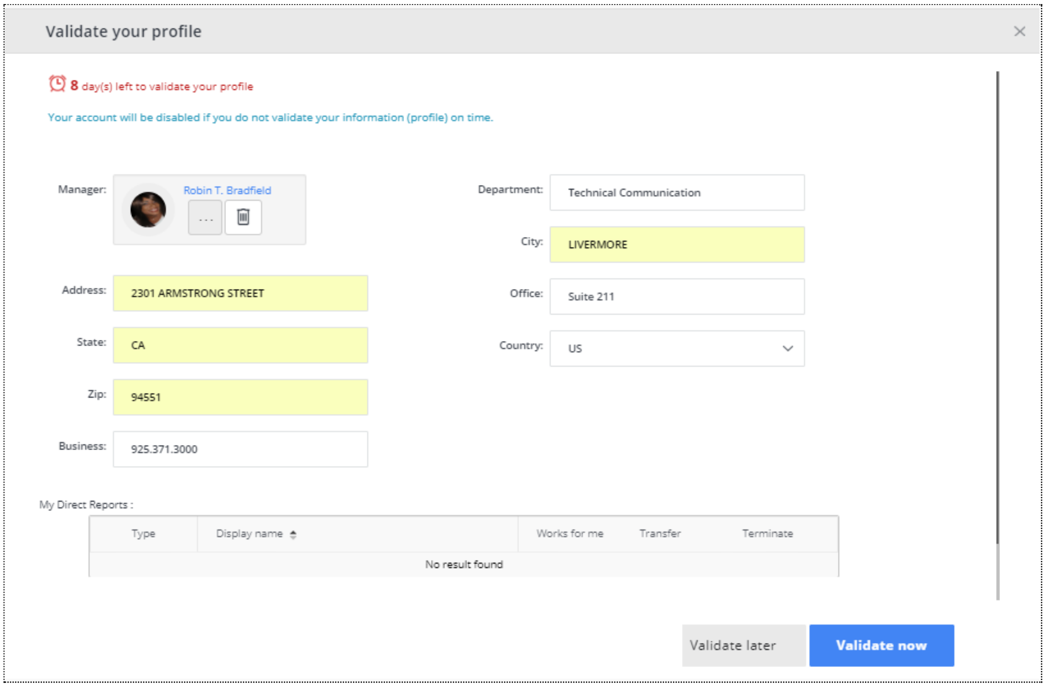
Profile validation for Users

The profile validation feature in GroupID is designed to ensure the accuracy of users' information in the directory. It only applies to users who are members of the group specified for profile validation in an identity store. These users must verify and update their directory profile information at a set frequency using the Self-Service portal.

While validating his or her the profile, a user can:

- Update his or her directory profile information
- Change his or her primary manager
- Transfer his or her direct reports to another manager
- Terminate his or her direct reports

On the **Property Validation** tab (Figure 70), you can specify the schema attributes (fields) for user profile validation. These attributes (fields) are displayed on the **Validate Profile Properties** window of the Self-Service portal, where users can validate and update the values for these attributes. It is as:



8 day(s) left to validate your profile

Your account will be disabled if you do not validate your information (profile) on time.

Manager:	Robin T. Bradfield	Department:	Technical Communication
		City:	LIVERMORE
Address:	2301 ARMSTRONG STREET	Office:	Suite 211
State:	CA	Country:	US
Zip:	94551		
Business:	925.371.3000		

My Direct Reports :

Type	Display name	Works for me	Transfer	Terminate
No result found				

Figure 68: Validate Profile Properties window in the Self-Service portal

NOTE

A few fields for profile validation are specified in the default portal template. You can add more fields, edit the existing fields, or remove them. However, the **My Direct Reports** field can neither be edited nor removed.

Property validation for Groups

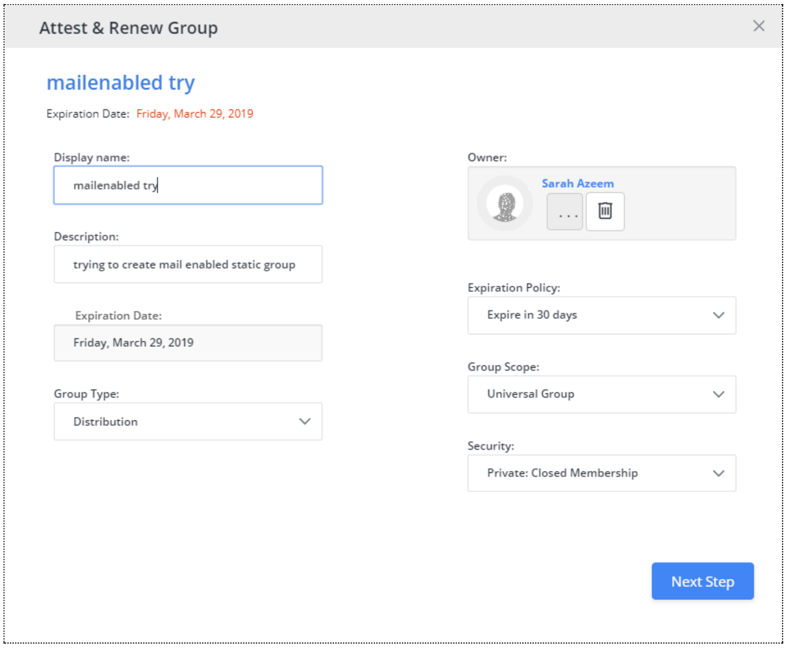
The GroupID administrator can enforce group owners to review and validate the attributes and membership of an expiring group before renewing it.

While attesting a group, the owner can:

- Update a few attributes, such as the group’s display name, expiration policy, security type, etc.
- Verify the group’s membership and inactivate unrequired members. Inactive members are removed from group membership instantly or after x number of days, depending on the configurations made by the administrator.

Group attestation applies to expiring groups with an expiry policy other than ‘never expire’.

On the **Property Validation** tab (Figure 70), you can specify the schema attributes (fields) for group attestation. These attributes (fields) are displayed on the **Attest & Renew Group** wizard in the Self-Service portal, where group owners can validate and update the values for these attributes. It is as:



Attest & Renew Group

mailenabled try

Expiration Date: Friday, March 29, 2019

Display name: mailenabled try

Description: trying to create mail enabled static group

Expiration Date: Friday, March 29, 2019

Group Type: Distribution

Owner: Sarah Azeem

Expiration Policy: Expire in 30 days

Group Scope: Universal Group

Security: Private: Closed Membership

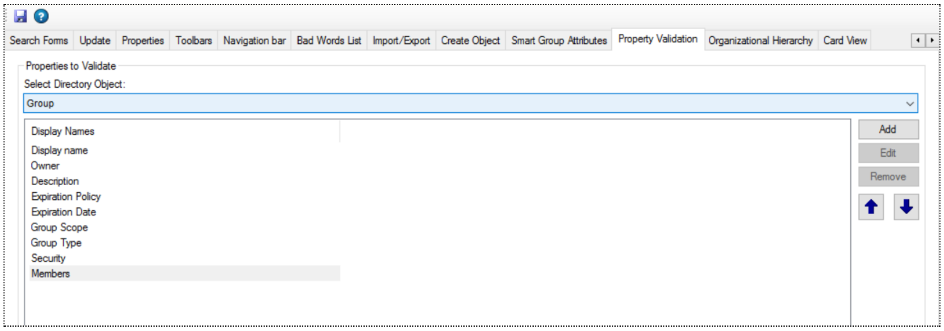
Figure 69: Attest & Renew Group wizard in the Self-Service portal

A few fields for group attestation are specified in the default portal template. You can add more fields, edit the existing fields, or remove them. However, the **Members** grid can neither be edited nor removed.

Add a new profile validation field

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Property Validation** tab.



Properties to Validate

Select Directory Object: Group

Display Names

Display name
Owner
Description
Expiration Policy
Expiration Date
Group Scope
Group Type
Security
Members

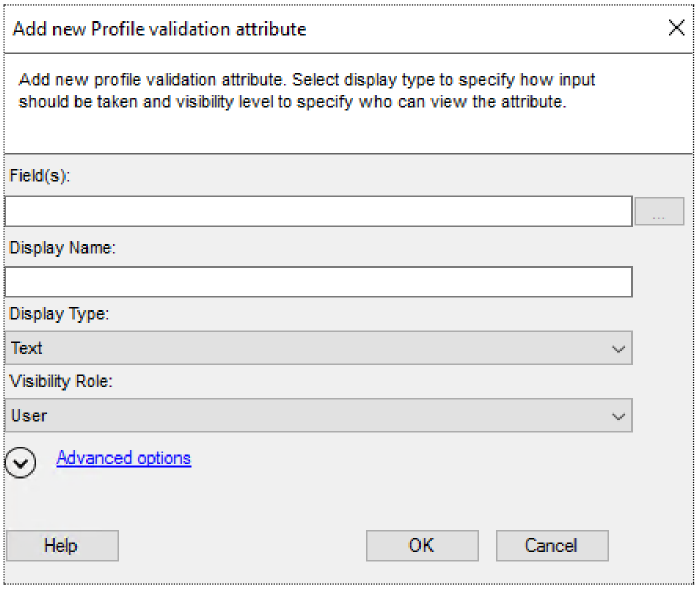
Figure 70: Property Validation tab

4. From the **Select Directory Object** list, select:

   - **Group**: to add, edit, or remove attributes for group attestation.
   - **User**: to add, edit, or remove attributes for user profile validation.

   On selecting an option, all fields currently available for group attestation/profile validation in the Self-Service portal are listed under **Display Name**.

5. Click **Add** to specify a new attribute (field) for group attestation/profile validation.



Add new Profile validation attribute

Add new profile validation attribute. Select display type to specify how input should be taken and visibility level to specify who can view the attribute.

Field(s):

Display Name:

Display Type: Text

Visibility Role: User

Figure 71: Add new profile validation attribute dialog box

6. Click the ellipsis button next to the **Field(s)** box to launch the **Select Profile Validation Attributes** dialog box, where you can select one or more schema attributes. For each of these attributes, a separate field would be displayed on the Attest & Renew Group wizard/Validate Profile Properties window of the Self-Service portal.

   The **Select Profile Validation Attributes** dialog box is as shown in Figure 67.

   a. Use the **Search** box to filter the schema attributes listed in the **Select** area.

   b. Select the check boxes for the attributes that you want to make available for group attestation/user profile validation in the portal.

   c. Click **OK**.

      The selected attribute(s) get listed in the **Field(s)** box on the **Add new profile validation attribute** dialog box (Figure 71). All other fields on the dialog box are auto-populated with the default configurations of the attribute(s).

7. In the **Display Name** box, specify a name to display as the field's label in the portal.

   This box is not available if you select multiple attributes in the **Field(s)** box.

8. Use the **Display Type** drop-down list to specify the display type to use for rendering the attribute(s) in the portal. The list contains all basic and custom display types defined on the **Custom Display Types** tab (Figure 14).

   When multiple attributes are selected in the **Field(s)** box, this display type applies to each of them.

9. From the **Visibility Role** drop-down list, select a security role. The field(s) would be visible to users of the selected role and to roles with a priority value higher than the selected role.

   - Select **Never** to hide the field(s) from all users.
   - Select **Manager and Owner** to make the field(s) visible only to the user's manager. They would not even be visible to the user itself.

     For example, if the *Manager and Owner* role is selected for the *Manager* field on the *Validate Profile Properties* page, the field would be visible to user managers for their respective direct reports in the portal.
   - Select **Self** to make the field(s) visible only to the logged-in user. They would not be visible to any other user, such as the user's manager or a role with a higher priority value or even a role with the 'Manage any profile' permission in the identity store.

   The visibility role determines which role members can view the field(s) in the portal. The **Visibility Role** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

10. Click the **Advanced options** link to enter further details for the field(s).

11. As mentioned for **Visibility Role**, the field is visible to members of the selected role and roles having a priority value higher than the selected role.

    Use the **Exclude Role** option to exclude a higher priority role or roles from getting visibility on the field.

    In the **Exclude Role** area, select the check boxes for the roles you want to hide the field from.

12. In the **ToolTip Text** box, enter the text to display when a user hovers the mouse over the field(s).

13. In the **Max Length** box, enter a number that represents the maximum number of characters that users can enter as value for each of the selected field(s).

    Entering 0 indicates that the field can accept an unlimited number of characters for its value.

14. The **Image Attribute** list is available when 'DN' is selected as the display type. This list supports 'thumbnailPhoto' as its value.

    - Select the 'thumbnailPhoto' attribute from the **Image Attribute** drop-down list when you want to auto upload an image with the field being defined. For example, when you apply this setting to the *Primary Manager* field on the *Validate Profile Properties* window, the primary manager's photo will be displayed alongside his or her name on the window.

      Note that for the image to display, the 'thumbnailPhoto' attribute must have a value stored; in case of no value, a blank image is displayed.

    - If you do not want to auto upload an image with the field, clear the value in the **Image Attribute** box.

15. Select the **Is Required** check box to make it mandatory for the user to provide a value for the field.

16. Select the **Is Read Only** check box if the field is meant to be read-only.

17. Click **OK** to close the dialog box.

18. On the toolbar, click **Save** 💾.

Modify the properties of a field

You can modify the properties of a field available in the portal for group attestation or user profile validation.

1. On the **Property Validation** tab (Figure 70), select *Group* or *User* from the **Select Directory Object** list. Then select a field in the **Display Name** area and click **Edit** to modify its details.

2. The **Edit Profile Validation attribute** dialog box is displayed, which is similar to the **Add new profile validation attribute** dialog box (Figure 71), except that the **Field(s)** box is not editable in the edit function. It displays the name of the attribute linked to the field being edited.

Follow steps 7 to 18 in the Add a new profile validation field section on page 121 to modify the field's properties.

Remove a field

You can remove a field from the **Validate Profile Properties** window or the **Attest & Renew Group** wizard, when it is not required anymore for user profile validation or group attestation respectively.

1. On the **Property Validation** tab (Figure 70), select *Group* or *User* from the **Select Directory Object** list. Then select a field in the **Display Name** area and click **Remove**.
2. On the toolbar, click **Save** 💾.

Specify attributes for Organizational Hierarchy

Using the Self-Service portal, you can view the organizational hierarchy for a user. This hierarchy is displayed in graphical form, creating a kind of an organogram. This organigram is configurable with respect to the attributes that it displays for each user.

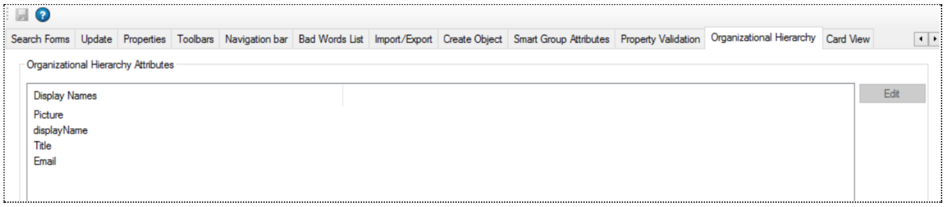
By default, the organizational hierarchy chart is displayed for the logged-in user. However, the user can view it for any other user in the organization. This chart presents a 360° view of the organization with the specified user as the focal point.

Using the **Designs** node, the administrator can specify the attributes that will be displayed for each user on the organizational hierarchy chart.

Specify attributes for display on the organizational hierarchy tree

1. In GroupID Management Console, select **Self-Service > Portals > [Required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Organizational Hierarchy** tab.



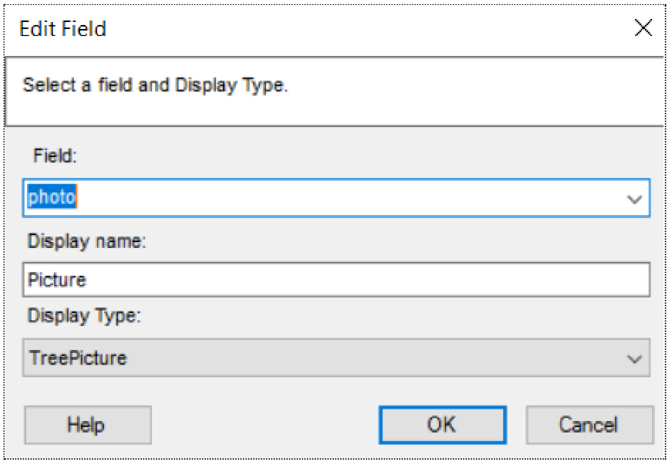
Organizational Hierarchy Attributes

Display Names
Picture
displayName
Title
Email

Figure 72: Organizational Hierarchy tab

By default, the **Organizational Hierarchy Attributes** area displays four attributes. For each user shown on the organizational hierarchy chart in the portal, the values of these attributes will be displayed. You can only replace an attribute with another attribute; you cannot add a fifth attribute or reduce the list to three attributes.

4. In the **Organizational Hierarchy Attributes** area, select the attribute you want to replace with another attribute, and click **Edit**.



Edit Field

Select a field and Display Type.

Field: photo

Display name: Picture

Display Type: TreePicture

Figure 73: Edit Field dialog box

5. In the **Field** list, select a schema attribute to display it for a user on the organizational hierarchy chart.

6. In the **Display name** box, enter a user friendly name for the attribute, that would serve as the field label for the attribute on the chart.

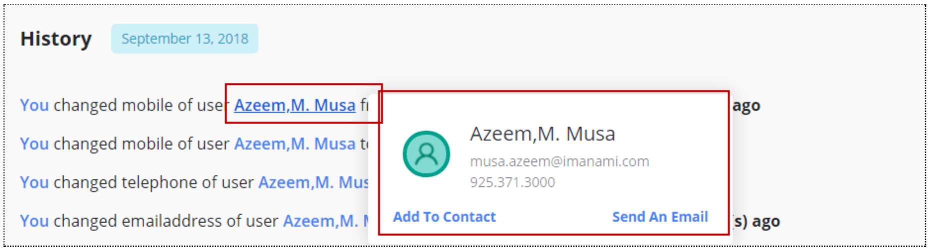
7. In the **Display Type** list, select the display type to use for rendering the attribute on the organizational hierarchy chart in the portal.
   The list contains all pre-defined and custom display types.

8. Click **OK**.
   The selected attribute is displayed in the **Organizational Hierarchy Attributes** area.

9. On the toolbar, click **Save** .

Specify attributes for the Object Card

In the Self-Service portal, the names of directory objects are displayed as links. When a user hovers the mouse over this link, a card is displayed, showcasing information about the object. For a user object, for example, the card displays the name, email address and phone number. It is as:



History September 13, 2018

You changed mobile of user Azeem,M. Musa fr ago

You changed mobile of user Azeem,M. Musa t

You changed telephone of user Azeem,M. Mus

You changed emailaddress of user Azeem,M. N s) ago

Azeem,M. Musa

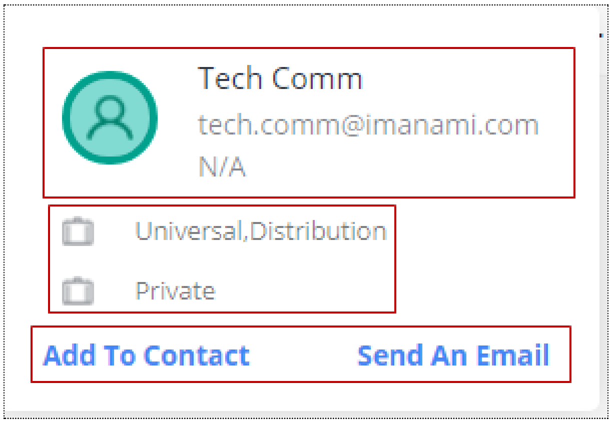
musa.azeem@imanami.com

925.371.3000

Add To Contact Send An Email

Figure 74: Card for the user object

For each object type, you can specify a different set of attributes to display on this card. For a group, the card is as:



Tech Comm

tech.comm@imanami.com

N/A

Universal,Distribution

Private

Add To Contact Send An Email

Figure 75: Card for the user object

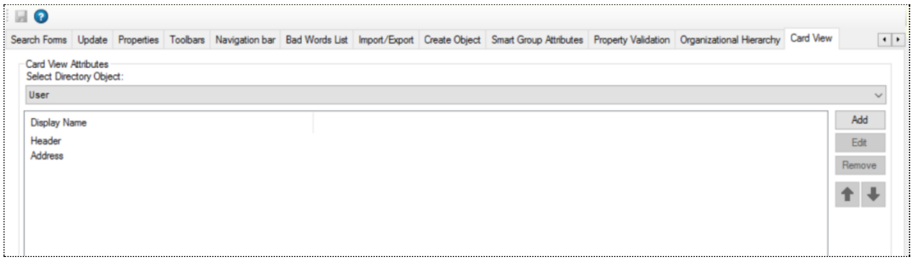
Notice that the card has three section, namely:

- Header
  The portal template allows for four attributes to be specified for display in the header. When a specified attribute does not contain a value, NA is displayed on the card.
- The middle part
  You can specify any number of attributes for this section. When you do not specify any attribute, this section is not displayed, as in Figure 74.
- Footer
  This section has the *Add To Contact* and *Send An Email* buttons. You can choose whether you want to display these buttons on the card or not.

Specify attributes for card header

By default, four attributes are specified for display in the card header. You can change the default attributes, but you cannot add a fifth attribute or reduce the number to three.

1. In GroupID Management Console, select **Self-Service > Portals > [Required portal] > Designs**.
2. Select an identity store to customize the portal design for it.
   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Card View** tab.

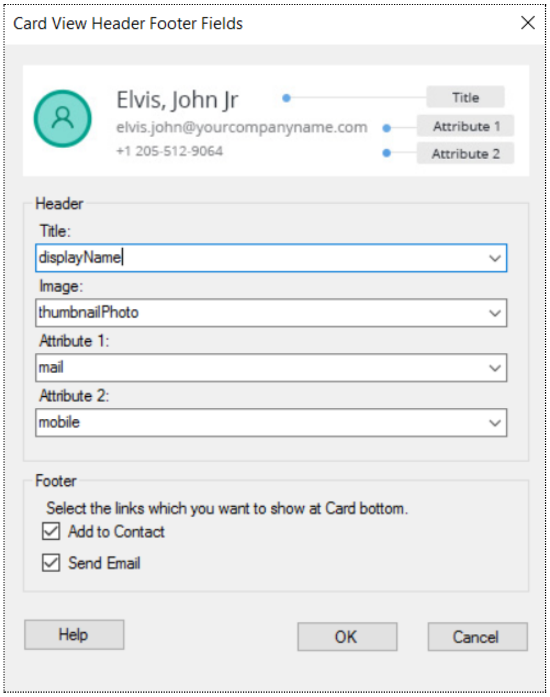


Select Directory Object: User

Display Name
Header
Address

Figure 76: Card View tab

4. From the **Select Directory Object** list, select *User*, *Contact*, *Group*, or *Mailbox* to manage the card for.
5. Select *Header* in the **Display Name** list and click **Edit**.



Header

Title: displayName

Image: thumbnailPhoto

Attribute 1: mail

Attribute 2: mobile

Footer

Select the links which you want to show at Card bottom.

☑ Add to Contact

☑ Send Email

Figure 77: Card View Header/Footer fields dialog box

The dialog box displays a sample header and how the specified attributes would populate it.

6. Use the **Title** box to select an attribute whose value will be displayed as the title of the header. By default, the title is set to the object's display name.
7. Use the **Image** box to set an attribute that can store images for directory objects.
8. Use the **Attribute 1** and **Attribute 2** boxes to display any other object attributes on the card.
   By default, the 'email' and 'mobile' attributes are selected.
9. Click **OK**.
10. On the toolbar, click **Save** 💾.

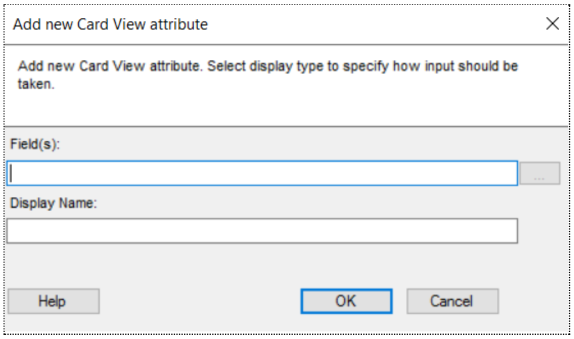
Manage footer options

1. In the **Footer** section of the **Card View Header/Footer fields** dialog box (Figure 77), select the **Add to Contact** and **Send Email** check boxes to display the respective buttons on the card.
2. Click **OK**.
3. On the toolbar, click **Save** 💾.

Specify an attribute for display on the card

In addition to the card header, you can specify more attributes for the card. The values of these attributes would be displayed for objects in the portal.

1. In GroupID Management Console, select **Self-Service > Portals > [Required portal] > Designs**.
2. Select an identity store to customize the portal design for it.
   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Card View** tab (Figure 76).
4. From the **Select Directory Object** list, select *User*, *Contact*, *Group*, or *Mailbox* to manage the card for.
5. Click **Add** to add a new attribute to the card.



Add new Card View attribute

Add new Card View attribute. Select display type to specify how input should be taken.

Field(s):

Display Name:

Figure 78: Add new Card View Attribute dialog box

6. Click the ellipsis button next to the **Field(s)** box to launch the **Select Card View Attributes** dialog box, where you can select one or more attributes. Values for each of these would be displayed on the card.

   The **Select Card View Attributes** dialog box is as shown in Figure 67.

   a. Use the **Search** box to filter the attributes listed in the **Select** area.
   b. Select the check boxes for the attributes that you want to display on the card.
   c. Click **OK**.
      The selected attribute(s) get listed in the **Field(s)** box on the **Add new card view attribute** dialog box (Figure 78).
7. Specify a name for the attribute in the **Display Name** box. The attribute value would be displayed next to this label on the card.

This box is not available if you select multiple attributes in the **Field(s)** box.

8. Click **OK** to close the dialog box.
9. On the toolbar, click **Save** 💾.

Edit an attribute

1. In GroupID Management Console, select **Self-Service > Portals > [Required portal] > Designs**.
2. Select an identity store to customize the portal design for it.
   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Card View** tab (Figure 76).
4. From the **Select Directory Object** list, select *User*, *Contact*, *Group*, or *Mailbox* to manage the card for.
5. In the **Display Name** list, select an attribute and click **Edit**.
   The **Edit Card View Attribute** dialog box is displayed, which is similar to the **Add new Card View Attribute** dialog box (Figure 78).

   The **Field(s)** box is not editable, so you cannot change the attribute. However, you can specify a different display name for it. This display name would be displayed on the card and the attribute's value would be shown next to it.
6. Click **OK** to close the dialog box.
7. On the toolbar, click **Save** 💾.

Remove an attribute

You can remove an attribute from the object card.

1. In GroupID Management Console, select **Self-Service > Portals > [Required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

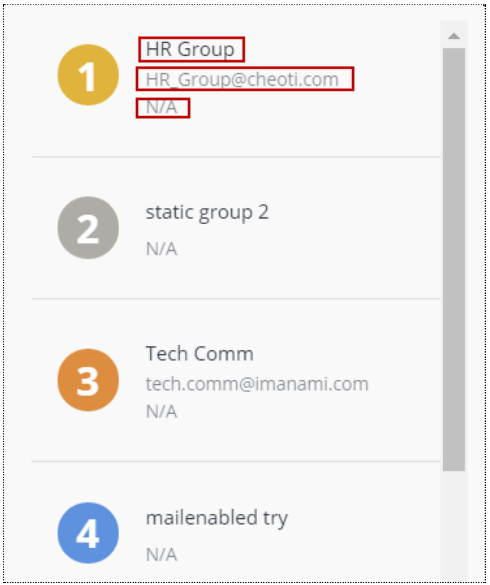
   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Card View** tab (Figure 76).

4. From the **Select Directory Object** list, select *User*, *Contact*, *Group*, or *Mailbox* to manage the card for.
5. In the **Display Name** list, select the attribute you want to remove from the card and click **Remove**.
6. Click **Yes** on the confirmation message box.
7. On the toolbar, click **Save** .

Specify attributes for object list view

In the Self-Service portal, the object list refers to a listing of groups that are similar to a certain group, Group similarity is measured in the context of group type and membership.

Suppose you want to view the groups that are similar to Group A. On the **Similar Groups** tab in Group A's properties, six groups bearing the strongest similarity to Group A are listed, with the most similar of these groups at the top. It is as:



1 HR Group
HR_Group@cheoti.com
N/A

2 static group 2
N/A

3 Tech Comm
tech.comm@imanami.com
N/A

4 mailenabled try
N/A

Figure 79: Object list on the Similar Groups tab

For a similar group, three attributes are displayed:

- The group's display name. This attribute cannot be changed.
- Attribute 1: You can specify any attribute. The default attribute is 'mail'.
- Attribute 2: You can specify any attribute. The default attribute is 'expiration policy'.

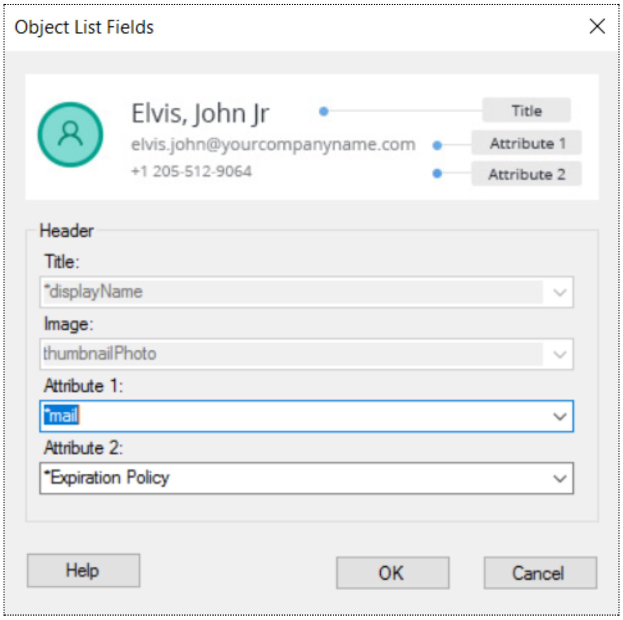
Change attributes for the object list

1. In GroupID Management Console, select **Self-Service > Portals > [Required portal] > Designs**.

2. Select an identity store to customize the portal design for it.
All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.

3. On the **Card View** tab (Figure 76), select *Object List* from the **Select Directory Object** list.

4. Select *Header* in the **Display Name** list and click **Edit**.
(The **Add** and **Remove** buttons are disabled, so you cannot add another attribute or remove the header option).



Header
Title: *displayName
Image: thumbnailPhoto
Attribute 1: *mail
Attribute 2: *Expiration Policy

Figure 80: Object List Fields dialog box

On the **Object List Fields** dialog box, you can view the attributes currently displayed for a similar group in the portal.

5. The **Title** box displays the displayName attribute. The value of this attribute will be displayed as the name of a similar group.

6. The **Image** box displays the thumbnailPhoto attribute, which can store images for directory objects.

7. Use the **Attribute 1** and **Attribute 2** boxes to display any other object attributes for similar groups.
By default, the ‘mail’ and ‘expiration policy’ attributes are selected.

8. Click **OK**.
9. On the toolbar, click **Save** 🖫.

The ‘Send on Behalf’ and ‘Send As’ features

The **Send on Behalf** permission in Microsoft Exchange and Office 365 allows a user to send an email as another user, while showing the recipient that it was sent from a user on behalf of another user. The recipient can see who actually initiated the sending message.

For example, when User A grants Send on Behalf permissions to User B, it means that User B can send email on behalf of User A. User B will be able to choose User A’s email address in the *From* field when composing a message in Outlook. However, message recipients will see both User A’s address and User B’s address (as the actual author of the message). This means that when User B sends a message using User A’s address, the ‘From’ address will show ‘*From: Mailbox <User B's address> on behalf of Mailbox <User A’s address>*’.

The **Send As** permission in Microsoft Exchange and Office 365, on the other hand, enables a user to send a message as another user.

For example, if User A grants Send As permissions to User B, User B will be able to choose User A’s email address in the ‘From’ field when composing a message in Outlook. In this instance, the message, while sent by User B, will appear as sent by User A.

You can provide both the Send As and Send on Behalf features in a Self-Service portal. Portal users will be able to grant the Send As and Send on Behalf permissions to other objects. Such objects will see the impact of these permissions in their mailboxes.

Prerequisites for the Send As and Send on Behalf features

In the following content, a ‘target object’ refers to the object that can add other objects to its Send As and Send on Behalf lists using the Self-Service portal.

- The target object can only be a mailbox or a mail enabled group.
- Microsoft Exchange or Office 365 must be configured as the messaging provider for the identity store.
- An SMTP server must be configured for the identity store.
- The user logged on the Self-Service portal must have the “Manage any Profile” permission for its respective role in the identity store.

- The XAdPermissionExtendedRights attribute should be available for 'Send AS' and the publicDelegates attribute should be available for 'Send on Behalf'.

  The ExchangeTrustedsubsystem object should have Modify permissions on the respective target objects in Active Directory for the Send As permission to be set using the Self-Service portal.

  Click here for more information.

Set up the Send As feature

You can provide the Send As feature on any tab of the target object's properties page in the Self-Service portal.

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Properties** tab (Figure 50).
4. From the **Select Directory Object** list, select a Mailbox or Group object to add the Send As feature to its properties page.

   The **Name** list displays the tabs currently available on the object's properties page.
5. Select a tab (for example, the **Email** tab) in the list and click **Edit**.

   The **Edit Category** dialog box is displayed, with the **Fields** area displaying the fields currently available on the tab.
6. Click **Add** to add the Send As field.
   The **Add Field** dialog box (Figure 52) is displayed.
7. In the **Field** list, select the XAdPermissionExtendedRights attribute.
8. In the **Display Name** box, provide a label for the field, such as 'Send As Permissions'. The Send As field will be displayed on the respective tab of object properties with the name you specify here.
9. In the **Display Type** list, select the 'DNs' option.

10. In the **Visibility Role** list, select a security role. The Send As field would be visible to users of the selected role and to roles with a priority value higher than the selected role.

    - Select *Never* to hide the field from all users.
    - Select **Manager and Owne**r to make the field visible only to the owner (in case of a group) or manager (in case of a mailbox). It would not be visible to any other user, such as group members or the mailbox itself. In other words, the field would be visible to group owners for their respective groups and to managers for their respective direct reports in the portal.
    - If you have selected 'Mailbox' in the **Select Directory Object** list, the *Self* option will also be available in the **Visibility Role** drop-down list.

      Select **Self** to make the field visible only to the mailbox on his or her properties page. It would not be visible to any other mailbox, such as the mailbox's manager or a role with a higher priority value or even a role with the 'Manage any profile' permission in the identity store.

    The visibility level determines the security role(s) whose members can view the field on the tab. The **Visibility Role** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

11. In the **Access Role** list, select a security role. Users of this role as well as of roles with a priority value higher than the selected role can modify the value of the Send As field, i.e., add and remove objects in the Send As list.

    - Select *Never* to make the field non-editable for all users.
    - Select *Manager and Owner* to enable only the owner (in case of a group) or manager (in case of a mailbox) to specify or modify the value of this field. It would not be editable for any other user, such as group members or the mailbox itself.

      In other words, only group owners can specify or modify the value of this field for their respective groups in the portal. A role with a higher priority value cannot change the value; group members cannot change the value; and even a role with the 'Manage any Group' permission in the identity store cannot change the value.

      Similarly, only mailbox managers can specify or modify the value of this field for their respective direct reports in the portal. A role with a higher priority value cannot change the value; and even a role with the 'Manage any profile' permission in the identity store cannot change the value.

- If you have selected ‘Mailbox’ in the **Select Directory Object** list, the *Self* option will also be available in the **Access Role** drop-down list.

  Select **Self** to enable only the logged-in user to specify or modify the value of the field. It would not be editable for any other user, such as the mailbox’s manager or a role with a higher priority value or even a role with the ‘Manage any profile’ permission in the identity store.

The access level determines the security role(s) whose members can add/update the value of this field. The **Access Role** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

12. As mentioned for **Access Role** and **Visibility Role**, the field is accessible and visible to members of the selected role and roles having a priority value higher than the selected role.

    Use the **Exclude Role** option to exclude a higher priority role or roles from getting access and visibility on the field.

    In the **Exclude Role** area, select the check boxes for the roles to whom you want to deny access and visibility on the field.

13. In the **Tooltip** box, enter the text to display when a user hovers the mouse over the Send As field.

14. Use the **Search Object Types** area to specify the object types that can be searched on the portal’s Find dialog box, to set as value for the *Send As* field.

    The following display types support the Find dialog box:

    - DN
    - DNs
    - Custom display types created with the Grid type

    When you select any of these display types, GroupID identifies that the value for the *Send As* field will have to be searched using the Find dialog box. The **Search Object Types** area is displayed, where you can select the required object type(s). For example, if you select User, only users can be searched and selected as value for the field.

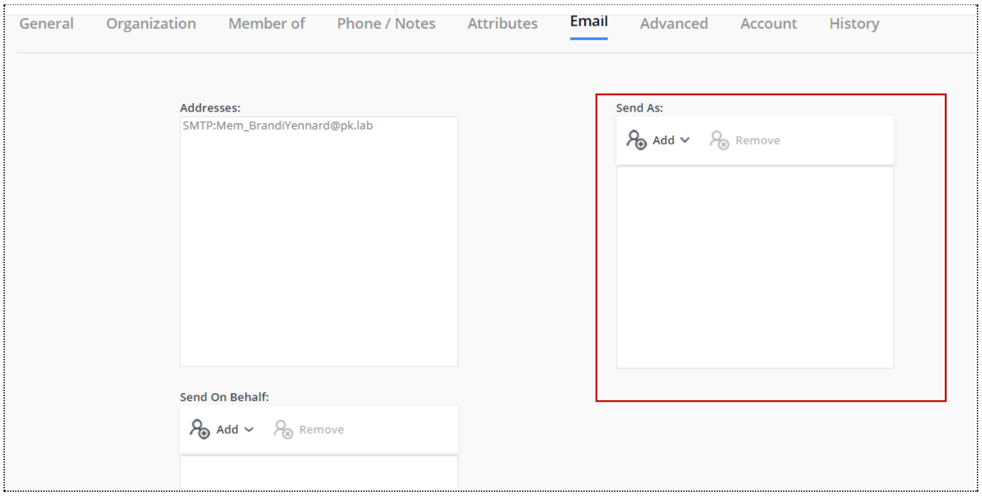
15. Select the **Is Required** check box to make it mandatory for the user to add at least one object to the Send As list.

16. Select the **Is Read Only** check box if the Send As field is meant to be read-only.

17. Click **OK** to close the **Add Field** and then the **Edit Category** dialog boxes.
18. On the toolbar, click **Save** .

Now launch the Self-Service portal for which you defined the Send As field.

On logging in, go to the properties of the object (group or mailbox) you defined the Send As field for, and click the respective tab. The Send As field is displayed as follows:



Addresses:
SMTP:Mem_BrandiYennard@pk.lab

Figure 81: Send As field in the Self-Service portal

Use the **Add** and **Remove** buttons to add and remove objects in the Send As list.

The added objects can send email for the object whose properties are being viewed, in accordance with the Send As functionality.

Set up the Send on Behalf feature

You can provide the Send on Behalf feature on any tab of the target object's properties page in the Self-Service portal.

1. In GroupID Management Console, select **Self-Service > Portals > [required portal] > Designs**.
2. Select an identity store to customize the portal design for it.

   All identity stores associated with the portal are listed under **Designs**. You can design a different portal for each of these.
3. Click the **Properties** tab (Figure 50).
4. From the **Select Directory Object** list, select a Mailbox or Group object to add the Send on Behalf feature to its properties page.

The **Name** list displays the tabs currently available on the object's properties page.

5. Select a tab (for example, the **Email** tab) in the list and click **Edit**.

   The **Edit Category** dialog box is displayed, with the **Fields** area displaying the fields currently available on the tab.

6. Click **Add** to add the Send on Behalf field.
   The **Add Field** dialog box (Figure 52) is displayed.

7. In the **Field** list, select the publicDelegates attribute.

8. In the **Display Name** box, provide a label for the field, such as 'Send on Behalf Permissions'. The Send on Behalf field will be displayed on the respective tab of object properties with the name you specify here.

9. In the **Display Type** list, select the 'DNs' option.

10. In the **Visibility Role** list, select a security role. The Send on Behalf field would be visible to users of the selected role and to roles with a priority value higher than the selected role.

    - Select *Never* to hide the field from all users.

    - Select *Manager and Owner* to make the field visible only to the owner (in case of a group) or manager (in case of a mailbox). It would not be visible to any other user, such as group members or the mailbox itself. In other words, the field would be visible to group owners for their respective groups and to managers for their respective direct reports in the portal.

    - If you have selected 'Mailbox' in the **Select Directory Object** list, the *Self* option will also be available in the **Visibility Role** drop-down list. Select *Self* to make the field visible only to the mailbox on his or her properties page. It would not be visible to any other user, such as the mailbox's manager or a role with a higher priority value or even a role with the 'Manage any profile' permission in the identity store.

    The visibility level determines the security role(s) whose members can view the field on the tab. The **Visibility Role** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

11. In the **Access Role** list, select a security role. Users of this role and of roles with a priority value higher than the selected role can modify the value of the Send on Behalf field, i.e., add and remove objects in the Send on Behalf list.

- Select *Never* to make the field non-editable for all users.
- Select *Manager and Owner* to enable only the owner (in case of a group) or manager (in case of a mailbox) to specify or modify the value of this field. It would not be editable for any other user, such as group members or the mailbox itself.

  In other words, only group owners can specify or modify the value of this field for their respective groups in the portal. A role with a higher priority value cannot change the value; group members cannot change the value; and even a role with the 'Manage any Group' permission in the identity store cannot change the value.

  Similarly, only mailbox managers can specify or modify the value of this field for their respective direct reports in the portal. A role with a higher priority value cannot change the value; and even a role with the 'Manage any profile' permission in the identity store cannot change the value.
- If you have selected 'Mailbox' in the **Select Directory Object** list, the *Self* option will also be available in the **Access Role** drop-down list.

  Select *Self* to enable only the mailbox to specify or modify the value of the field on his or her properties page. It would not be editable for any other user, such as the mailbox's manager or a role with a higher priority value or even a role with the 'Manage any profile' permission in the identity store.

The access level determines the security role(s) whose members can add/update the value of this field. The **Access Role** list contains all security roles defined for the identity store, along with the *Self* and *Manager and Owner* roles that are hard-coded and apply only to the portal.

12. As mentioned for **Access Role** and **Visibility Role**, the field is accessible and visible to members of the selected role and roles having a priority value higher than the selected role.

    Use the **Exclude Role** option to exclude a higher priority role or roles from getting access and visibility on the field.

    In the **Exclude Role** area, select the check boxes for the roles to whom you want to deny access and visibility on the field.
13. In the **Tooltip** box, enter the text to display when a user hovers the mouse over the Send on Behalf field.
14. Use the **Search Object Types** area to specify the object that can be searched on the portal's Find dialog box, to set as value for the *Send on Behalf* field.

The following display types support the Find dialog box:

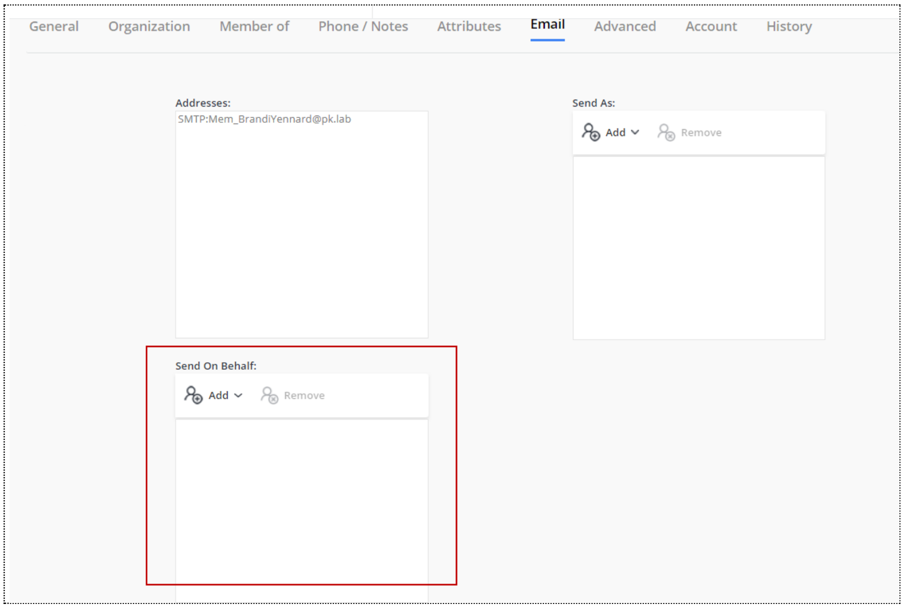
- DN
- DNs
- Custom display types created with the Grid type

When you select any of these display types, GroupID identifies that the value for the *Send on Behalf* field will have to be searched using the Find dialog box. The **Search Object Types** area is displayed, where you can select the required object type(s). For example, if you select User, only users can be searched and selected as value for the field.

15. Select the **Is Required** check box to make it mandatory for the user to add at least one object to the Send on Behalf list.
16. Select the **Is Read Only** check box if the Send on Behalf field is meant to be read-only.
17. Click **OK** to close the **Add Field** and then the **Edit Category** dialog boxes.
18. On the toolbar, click **Save** 💾.

Now launch the Self-Service portal for which you defined the Send on Behalf field.

On logging in, go to the properties of the object (group or mailbox) you defined the Send on Behalf field for, and click the respective tab. The Send on Behalf field is displayed as follows:



Addresses:
SMTP:Mem_BrandiYennard@pk.lab

Send As:

Send On Behalf:

Figure 82: Send on Behalf field in the Self-Service portal

Use the **Add** and **Remove** buttons to add and remove objects in the Send on Behalf list.

The added objects can send email on behalf of the object whose properties are being viewed, in accordance with the Send on Behalf functionality.

Chapter 6 - Integration with Other Applications

You can integrate a Self-Service portal with

- Microsoft Outlook
- SharePoint
- You can also Integrate Self-Service Search into web applications.

Integrate a portal with Microsoft Outlook

You can integrate a Self-Service portal with Outlook 98 and later versions by setting the portal as the home page for an Outlook public folder.

1. Using Outlook, create a new public folder with any name.
2. Right-click the folder and select **Properties**.
3. On the **Properties** dialog box, click the **Home Page** tab.
4. In the **Address** box, type the address of your required Self-Service portal.
5. Select the **Show home page by default for this folder** check box.
6. Click **OK** to close the **Properties** dialog box.

When you click the public folder in Outlook, you are automatically redirected to the Self-Service portal.

Integrate a portal with SharePoint

Integrate a portal with SharePoint 2007

1. Launch **SharePoint Central Administration**.
2. On the **Site Actions** menu, click **Create**.
3. In the **Web pages** section, click **Sites and Workspaces**.

4. On the **New SharePoint Site** page, provide the title, web site address, and access permissions for the site.
5. Click **Create** to create the site.
6. In the **Site Actions** menu, click **Edit Page** to add a Web Part to this site.
7. Click **Add a Web Part** on the Left or Right section as needed.
   The **Add Web Parts** dialog box is displayed.
8. In the **All Web Parts** section, select the **Page Viewer Web Part** check box.
9. Click **Add**.
   The Web Part is displayed in the corresponding section.
10. Click **open the tool pane** in the added Web Part to access the Web Part settings.
11. In the **Page Viewer** tool pane, do the following:
    a. Select **Web Page**.
    b. In the **Link** box, type the address for the required Self-Service portal.

       You can find this address in the GroupID Management Console by selecting Self-Service > Portals > [required portal] > Server > General tab.
12. Expand the **Appearance** section and do the following:
    a. Set **Height** to 650 pixels.
    b. Set **Width** to 850 pixels.
13. Click **OK** to save your changes.
14. Click **Exit Edit Mode** (below the **Site Actions** menu) to exit the edit mode.

Your site is now available for you to access.

Integrate a portal with SharePoint 2003

1. Launch **SharePoint Services Central Administration**.
2. In the **Virtual Server Configuration** section, click **Create a top-level Web site**.
3. On the **Virtual Server List** page, click the appropriate virtual server.
4. On the **Create Top-level Web Site** page, provide the appropriate information for the top-level website and click **OK**.
5. On the **Top-Level Site Successfully Created** page, click **OK**.

6. Access the newly created website by typing its address in a browser.
7. From the **Template** list, click **Team Site** or **Blank Site** and click **OK**.
   The default page is configured with the selected template.
8. To modify the content of the default page, open the **Modify Shared Page** menu, point to **Add Web Parts** and click **Browse**.
9. On the **Add Web Parts** panel at the left, do the following:

   a. Click **Virtual Server Gallery**.

   b. From the **Web Part List** section, select **Web Capture Web Part**.

   NOTE If you do not see the Web Capture Web Part option, you must download and install the Microsoft Office 2003 Add-in: Web Parts and Components, available on the Microsoft website.

   c. From the **Add to** list, select **Left** and click **Add**.
   The Web Part is displayed on the left section of the page.

10. (Optional) Remove non-relevant web parts, including announcements, events, site image, and links:

    a. In the **Modify Shared Page** menu, select **Modify Shared Web Parts**.

    b. Click the required shared web part name.

    c. Click **X** in the web part display to remove the Web Part from the page.

11. Click **Create Web Capture** for the Web Part to display the **Web Capture Web Part** panel, and do the following:

    d. Expand the **Web Capture** section.

    e. In the **Capture Link** box, type the address of the required Self-Service portal.

    You can find this address in the GroupID Management Console by selecting Self-Service > Portals > [required portal] > Server > General tab.

    f. Expand the **Appearance** section and type a title for the web part.

    g. Update the height to 650 pixels and the width to 850 pixels, and click **OK**.

The Self-Service portal is now available as a Web Part on the web page.

Integrate Self-Service Search into web applications

One of the key features of Self-Service is its ability to search for Active Directory objects based on user-provided criteria. Self-Service offers sophisticated and flexible methods that allow you to integrate this search capability in your intranet sites.

Search integration can be interactive as well as static.

- The interactive method collects search parameters from users, prepares a query string from user inputs, passes the string to the designated portal, and returns the search results according to the matches found. An example of interactive integration is the addition of a new search form on your site to collect the user inputs.
- The static approach carries out a search based on a pre-defined query string. An example of static integration is the addition of the query as a link on your site's page.

Before you integrate

Before you integrate, you should determine the following:

- The objects to search
- The fields to search
- The pattern to follow to find matches in Active Directory (starts with, contains, and so on)
- The title of the search results page

Search parameters

Before implementing integrated search, study the following search parameters. These parameters are required to prepare the query string. Self-Service only understands the query string if it contains the search criteria in these parameters.

Parameter Name	Optional	Value
c	Yes	This field is reserved for future use. If given, set "search" as its value.
sc	Yes	The distinguished name of the container to search. If not set; then, by default, the search will include all containers in the logged-on domain.

<table>
<tr><th>Parameter Name</th><th>Optional</th><th>Value</th></tr>
<tr><td>f</td><td>No</td><td>The LDAP query; for example, (displayName=williams*) or (&(displayName=williams*)(department=sal*)). Normally, this parameter is provided by the JavaScript code in the search form using the search text the user enters into the given text box.</td></tr>
<tr><td>cs</td><td>No</td><td>Specifies that a canned search is taking place. Should be set to 1.
NOTE The search integration feature is also known as Canned Search.</td></tr>
<tr><td>o</td><td>No</td><td>The type of objects to return. You can specify the type individually or in combination.
<table>
<tr><th>Object</th><th>Type</th></tr>
<tr><td>User</td><td>1</td></tr>
<tr><td>Contact</td><td>2</td></tr>
<tr><td>Group</td><td>4</td></tr>
<tr><td>Public Folder</td><td>8</td></tr>
<tr><td>User and Contact</td><td>3 (1+2)</td></tr>
<tr><td>All Objects</td><td>15 (1+2+4+8)</td></tr>
</table></td></tr>
<tr><td>t</td><td>Yes</td><td>The title of the search results page. The default is "Search Results".</td></tr>
<tr><td>sv</td><td>Yes</td><td>The view of the search results page. You can provide any of the values that represent the pre-defined view available in Self-Service: SearchResults.Default, SearchResults.Groups, SearchResults.ExpiringGroups. The default is SearchResults.Default.</td></tr>
</table>

Table 18: Parameters for query string

Interactive integration - Using a Search Form

As mentioned above, the interactive method involves collecting inputs from users on the basis of which the query string is prepared and sent to the portal. The following example illustrates how to prepare a simple HTML form comprising a text box and a Submit button. The form will take single input from user, prepare the query string based on the entered text using the values set for search parameters discussed in Table 18 (set as hidden for this example), and pass it to the designated portal.

```
<html>

<head>

<title>Sample Search Form</title>

<script language="javascript" type="text/javascript">

<!--

function fQuickSearch_onsubmit() {

var form = document.fQuickSearch;

var searchtext = document.fQuickSearch.ID_SEARCHTEXT;

var searchfilter = document.fQuickSearch.ID_FILTER;

if (searchtext.value!=""){

searchfilter.value = "(displayname=*" + searchtext.value +
"*)";

return true;

}

else{

window.alert("Please enter a value to search for before
clicking submit.");

return false;

}

}

//-->

</script>

</head>

<body>

<form method=get action="http://localhost/Portal
Name/default.aspx" name="fQuickSearch" autocomplete="on"
onsubmit="return fQuickSearch_onsubmit()" target="_blank">

<INPUT type="hidden" ID="ID_COMMAND" NAME="c"
VALUE="search">

<INPUT type="hidden" ID="ID_SEARCHCONTAINER" NAME="sc">

<INPUT type="hidden" ID="ID_FILTER" NAME="f">
```

```
<INPUT type="hidden" ID="ID_CANNEDSEARCHFLAG" NAME="cs"
value="1">

<INPUT type="hidden" ID="ID_OBJECTCLASS" NAME="o"
value="3">

<INPUT type="text" id="ID_SEARCHTEXT" name="sDisplayName"
language=javascript> <INPUT id="Submit1" type="submit"
value="Submit" name="Submit1">

</form>

</body>

</html>
```

Note the following statement in the preceding example's JavaScript code:

```
searchfilter.value = "(displayname=*" + searchtext.value +
"*)";
```

This statement prepares the LDAP query. This query is the key component of the query string by which the Active Directory objects are filtered. For example, if the user enters **Rob** in the text box and clicks the Submit button, the following LDAP query will be generated:

```
searchfilter.value = "(displayname=*Rob*)";
```

The asterisk represents a wild card so that the Active Directory will be searched for user and contact objects with **Rob** in their display names. The complete query string that will be passed to the portal is:

```
http://localhost/Portal Name
/SearchResults.aspx?c=search&sc=&f=%28displayName%3D*Rob*%2
9&cs=1&o=3&sDisplayName=d&Submit1=Submit
```

Static Integration - Using a Link

Self-Service search integration requires the query string in a standard pattern in order to perform the Active Directory search. You can prepare this query string and add it as a link on your website.

Preparing the query string

To prepare a query string, you first need to determine the values of all the required search parameters. For example, if you want to search all user and contact objects belonging to the Sales department in the container OfficeA, the values of the search parameters to set are as follows:

```
c = search

sc = OU=OfficeA,DC=Contoso,DC=com
```

```
f = (department=sal*)

cs = 1

o = 3

t = Sales Department

sv = SearchResults.Default
```

After determining the values of the above parameters, you can prepare your query string by following any of these methods:

Using the Canned Search URL Generator

The web page collects the portal URL and the values of the search parameters from the user, and generates the complete URL automatically.

Doing it yourself

This method requires you to join the search parameters and their values using the ampersand (&) character, as shown here:

```
c=search&sc=OU=OfficeA,DC=Contoso,DC=com&f=(department
=sal*)&cs=1&o=3&t=Sales
Department&sv=SearcgResults.Default
```

The next step is to append the combined search parameters with the portal URL using the question mark (?) character. The resulting URL is:

```
http://localhost/Portal
Name/default.aspx?c=search&sc=OU=OfficeA,DC=Contoso,DC
=com&f=(department=sal*)&cs=1&o=3&t=Sales
Department&sv=SearcgResults.Default
```

Once the URL is prepared by either of these methods, you can associate it with a link on your website. For example:

```
<a href="http://localhost/Portal
Name/default.aspx?c=search&sc=OU=OfficeA,DC=Contoso,DC=com&
f=(department=sal*)&cs=1&o=3&t=Sales
Department&sv=SearcgResults.Default" target="_blank">Show
objects for Rob (Opens in a new window)</a>
```

GroupID

by imanami | NOW PART OF netwrix

Imanami | Now part of Netwrix

6160 Warren Parkway, Suite 100,
Frisco, TX 75034,
United States.
https://www.imanami.com/

Support: (925) 371-3000, Opt. 3
support@imanami.com

Sales: (925) 371-3000, Opt. 1
sales@imanami.com

Toll-Free: (800) 684-8515
Phone: (925) 371-3000
Fax: (925) 371-3001