GroupID

by imanami | NOW PART OF netwrix

Version 10.2

GroupID Authenticate

GroupID Automate

GroupID Self-Service

GroupID Synchronize

GroupID Password Center

GroupID Insights

GroupID Mobile App

GroupID Reports

User Guide

Automate

This publication applies to GroupID Version 10.2 and subsequent releases until otherwise indicated in new editions.

Contents

Chapter 1 - Getting Started

You must connect GroupID Management Console to an identity store before using Automate. You can then manage groups and perform other operations in the connected identity store.

You can sign into an identity store using any of the following methods:

- Enter the username and password of your identity store account.
- Sign in using a SAML provider.
  (This option is available if a SAML provider is configured with GroupID.)
- Scan the QR code with the GroupID app installed on your smartphone.
  (This option is available if the QR code is enabled for an identity store.)

Next, you may have to pass second factor authentication, depending on whether it is enabled for your role in the connected identity store. Passing it completes the authentication process.

You can perform tasks in GroupID Management Console depending on your role and permissions in the connected identity store.

Connect GroupID Management Console to an identity store

1. In GroupID Management Console, right-click the **GroupID** node and select **Connect to Identity Store**.

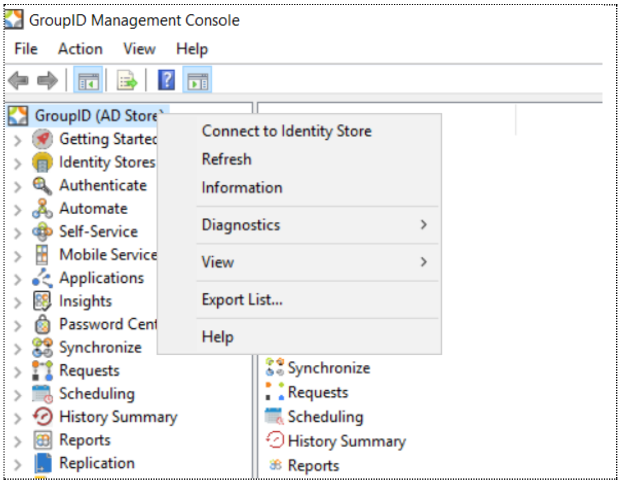


Figure 1: Connect to Identity Store option

The **Login** window is displayed.

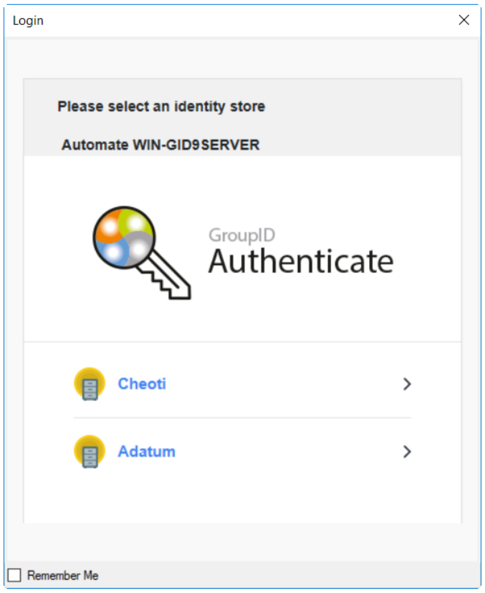


Figure 2: Login window

The window displays the GroupID module (Automate) that you want to connect to an identity store, followed by the machine name (the client name of Automate on that instance).

If QR code has been enabled for any of the listed identity stores, it is displayed on the window. Scroll down to view the QR code.

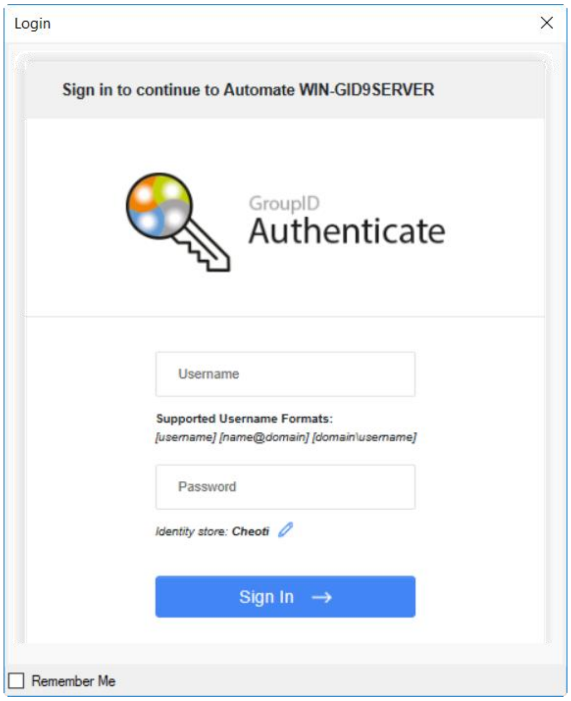
2. You can sign in using any of the following methods:

   - Identity store account credentials
   - SAML provider

- QR code

Sign in with your identity store account

1. On the **Login** window (Figure 2), click an identity store to connect to. The **Login** window changes to display the login fields.



Sign in to continue to Automate WIN-GID9SERVER

Supported Username Formats:
[username] [name@domain] [domain\username]

Identity store: Cheoti

Figure 3: Login window (2)

2. In the **Username** and **Password** boxes, enter the user name and password of your directory account, or click **Change** to connect to a different identity store.
3. Select the **Remember Me** check box to save your credentials. The next time you launch GroupID Management Console, it will automatically connect to the identity store with the saved credentials.
4. Click **Sign In** to connect GroupID Management Console to the identity store.

Sign in with a SAML provider

You can opt for single sign-on across all GroupID modules, provided that a SAML provider is configured with GroupID.

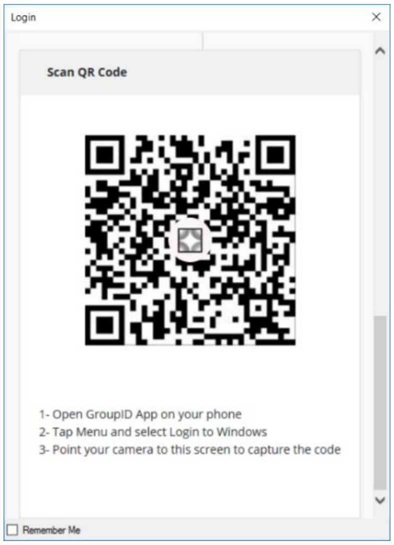
On the **Login** window (Figure 3), click the button or image for the provider and proceed to sign in.

Sign in with QR code

If the QR code is enabled for any of the identity stores, the **Login** window displays the code too. Use the QR code to sign into an identity store.

To scan QR code:

1. Scroll down the **Login** window (Figure 2 or Figure 3) to display the QR code.



1- Open GroupID App on your phone
2- Tap Menu and select Login to Windows
3- Point your camera to this screen to capture the code

Figure 4: Login window - Scan QR Code

2. Open the **GroupID** app on your smartphone and connect to an identity store. This identity store should have the QR code feature enabled for it.

   GroupID Management Console would connect to the same identity store you connect the **GroupID** app to.

3. Tap **Configure Application Using QR Code** in the app.

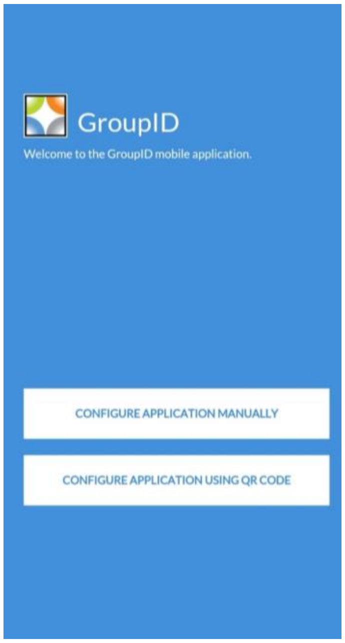

GroupID
Welcome to the GroupID mobile application.
CONFIGURE APPLICATION MANUALLY
CONFIGURE APPLICATION USING QR CODE

Figure 5: GroupID app – Welcome page

4. Capture the QR code through the GroupID app on your phone. One of the following happens:
   - If the identity store that the GroupID app is connected to does not have the QR code option enabled, an error message is displayed.
   - If the identity store that the GroupID app is connected to has the QR code option enabled, GroupID Management Console will connect to this identity store.

Pass second factor authentication

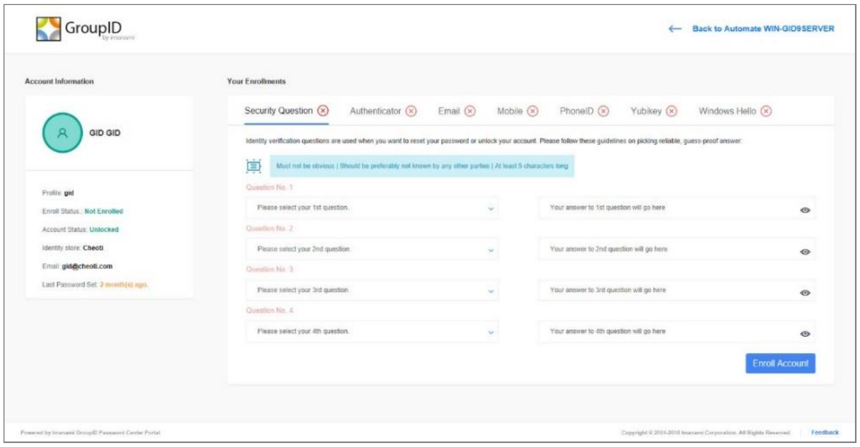
The administrator can enable second factor authentication for a security role in an identity store.

If enabled for your role in the connected identity store, you must pass second factor authentication after signing in via any of the above methods.

For second factor authentication, one of the following applies:

- If you have not enrolled your identity store account in GroupID, you must enroll using at least one authentication type.

  The **Enroll Account** window is displayed as follows:



Profile: gid
Enroll Status.: Not Enrolled
Account Status: Unlocked
Identity store: Cheoti
Email: gid@cheoti.com
Last Password Set: 2 month(s) ago.

Identity verification questions are used when you want to reset your password or unlock your account. Please follow these guidelines on picking reliable, guess-proof answer:

Must not be obvious | Should be preferably not known by any other parties | At least 5 characters long

Please select your 1st question.

Your answer to 1st question will go here

Please select your 2nd question.

Your answer to 2nd question will go here

Please select your 3rd question.

Your answer to 3rd question will go here

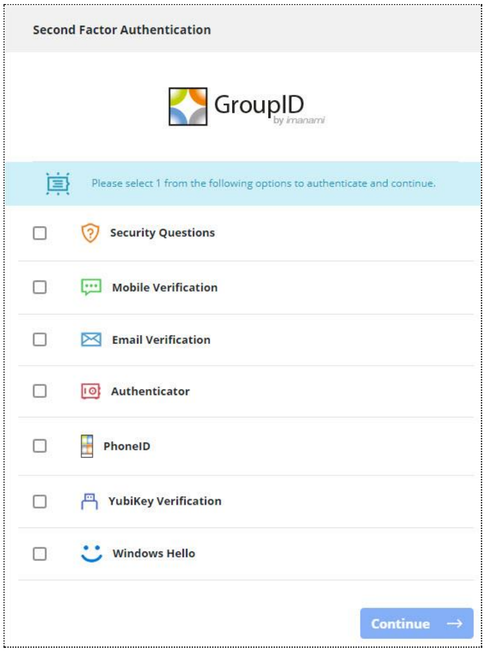
Please select your 4th question.

Your answer to 4th question will go here

Figure 6: Enroll Account window

  Tabs on this window represent the different authentication types that the administrator has enabled for enrollment. You can choose to enroll your account with as many authentication types as you want; however, enrollment with only one authentication type is mandatory.

- If you have already enrolled your account, you must authenticate this account in order to connect to the console. The **Authenticate Account** window is displayed as follows:



Second Factor Authentication

Please select 1 from the following options to authenticate and continue.

□ Security Questions

□ Mobile Verification

□ Email Verification

□ Authenticator

□ PhoneID

□ YubiKey Verification

□ Windows Hello

Figure 7: Authenticate Account window

Options on this window represent the different authentication types that you used to enroll your account with. You have to authenticate with one authentication type,

See Chapter 3 - Second Factor Authentication on page 14 for details.

Chapter 2 - About GroupID Automate

Automate enables you to manage directory groups, that includes both static groups and Smart Groups. You can:

- Create static groups, Smart Groups and Dynasties.
- Manage the type, scope, security type, and ownerships of groups.
- Manage group membership dynamically.
- Specify an expiry policy for groups. This policy defines the period for which the group remains active. When the period is over, the group becomes inactive and is locked for all activities.
- Groups can also be moved between domains within a single forest.

Examples of directory groups include distribution lists and security groups.

Automate updates Smart Groups and Dynasties on the basis of user-defined queries. When directory information changes, Automate automatically updates the appropriate groups, thus ensuring that groups are never out of date. This allows administrators to easily maintain large groups without having to manually add and remove members.

NOTE This user guide discusses Automate in the context of Active Directory in particular and other identity providers in general.

Role-based security

To manage access in GroupID, security roles are defined for an identity store. Each role is granted a set of permissions that enable role members to access specific GroupID functions.

Priority value

Each security role is assigned 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.

Identity Stores in GroupID

To create and manage groups on a directory server using Automate, the administrator must first create an identity store for that identity provider in GroupID.

GroupID supports the following providers for creating an identity store:

- Active Directory
- Generic LDAP
- Microsoft Azure
- Digium Switchvox
- Google Workspace
- Health Meter

NOTE When two identity stores (say, ID1 and ID2) are connected to the same domain (for example, demo1.com), then objects in demo1.com would have a distinct state in ID1 and ID2. For example, an object's state (such as expiry policy, Smart Group criteria, additional owners, etc.) would be different in both identity stores.

Identity Store configurations essential to Automate

The following must be configured for an identity store before you can manipulate it using Automate:

An SMTP server

An SMTP server must be configured for each identity store you want to connect Automate to, so that email notifications can be sent to designated recipients for different actions performed in Automate.

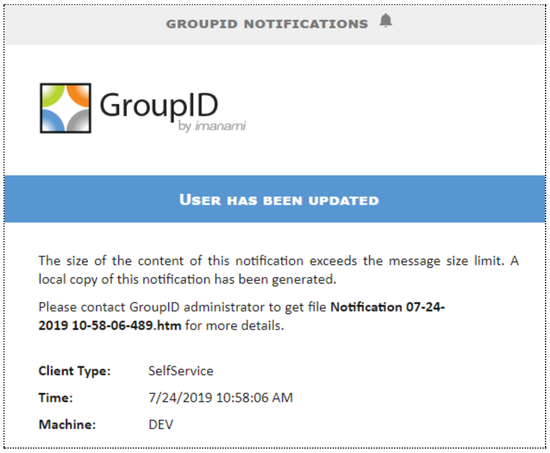
By default, notifications are sent to users in the English language. However, a user can opt to receive notifications in a different language by personalizing the language settings from the **User Settings** panel in the Self-Service portal.

NOTE When a notification exceeds 8 MB in size, its content is moved to a file that is generated and stored at the location:

<GroupID 10 root directory>\Notifications\
Example: C:\Program Files\Imanami\GroupID 10.0\Notifications\

File name: Notification <date and time of generation>.htm
Example: Notification 07-24-2019 10-58-06-489.htm

The user also receives a notification that redirects him/her to the notification file. It is as:



USER HAS BEEN UPDATED

The size of the content of this notification exceeds the message size limit. A local copy of this notification has been generated.

Please contact GroupID administrator to get file **Notification 07-24-2019 10-58-06-489.htm** for more details.

Client Type: SelfService
Time: 7/24/2019 10:58:06 AM
Machine: DEV

Figure 8: Redirect notification

A messaging provider

You can only create mail-enabled groups in an identity store if the administrator has configured a messaging provider, such as Microsoft Exchange, for the identity store.

Scheduled jobs

Scheduled jobs must be defined for the identity store, so that different activities in Automate, such as group membership update, group expiry and deletion, and orphan group ownership, are automatically carried out on a scheduled basis.

See Scheduled jobs impacting Automate on page 11 for details.

Role-based permissions

A user must belong to at least one user role in the identity store in order to perform tasks in Automate. The user can only perform the tasks his or her role has permissions for.

Role policies

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

- **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

  In an Azure based identity store, a primary owner must be specified for groups, whether the policy enforces it or not.

- **Group name prefixes policy**
  The administrator can enforce the use of prefixes in group names (as discussed in Group name prefixes).

- **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 Automate to a container for role members. The administrator can also designate a criterion to filter specific objects in searches.

  The Search policy has the following impact on Automate:

  - It sets the search scope for the **Find** dialog box (Figure 46).
  - It determines the groups to display in group listings (see Table 1).

Group name prefixes

The administrator can enforce group naming consistency by defining prefixes at the identity store level or role level or both. Identity store-specific prefixes are available to all roles defined for the identity store while role-specific prefixes are only available to role members for use.

When a user creates a group, he or she must select a prefix, which is added to the group's name and display name.

For information on group naming in an Azure based identity store, see, Group naming policy in Appendix B.

Membership update settings for Smart Groups and Dynasties

To manage membership changes to Smart Groups and Dynasties, the administrator can configure the 'Out of Bounds' setting at the identity store level.

See Membership settings on page 89 for details.

Membership lifecycle policies for static groups

The administrator can specify membership lifecycle policies for static groups. These policies state that all members added or removed from target groups during a specified period are treated as temporary addition or removal respectively.

When applied to the existing membership of a group, these policies can effectively remove all members or convert all to permanent members.

Dynasty settings

The administrator can specify certain settings to control how Automate processes the Dynasties in an identity store. These settings are discussed in Dynasty settings on page 138.

Workflows

With workflows enabled for an identity store, changes made to an object are approved by an authorized user before they are committed to the directory server.

GroupID provides several pre-defined system workflows, of which the following apply to Automate:

- **Require Admin Approval to Change Group Expiration Policy** - This workflow is triggered when a user changes the expiry policy for a group.
- **Workflow to Nest a Group** - This workflow is triggered when a user adds a group to the membership of another group.

The administrator can also define more workflows for the identity store.

History tracking

Automate can maintain a track of actions performed on a group since its creation, provided that history tracking is enabled for the identity store.

See Group history on page 84 for details.

Event logging

GroupID employs Windows logging and File logging, to maintain event logs for Automate.

Log settings are defined at the identity store level and may vary for different identity stores.

Second factor authentication

If the GroupID administrator enforces second factor authentication for a user role in an identity store, role members must authenticate their identity store accounts while connecting GroupID Management Console to that identity store.

See Chapter 3 - Second Factor Authentication on page 14 for details.

GroupID configurations essential to Automate

The GroupID administrator can specify global configurations for Automate that apply irrespective of the identity store. These configurations are:

Set object limit for display

The GroupID administrator can specify:

- the number of group members to be displayed on the **Members** tab (Figure 37) in group properties. Users will have to click the **Show All** link on the tab to get a list of all members.
- the number of most recently used recipients (set as group owners) to show on the shortcut menu (Figure 47) for specifying the owner of multiple groups.
- pagination for the **History** tab (Figure 40) in group properties. This sets the number of records to be displayed on a page; the next records are moved to the next page, and so on.

Set default settings for groups

The GroupID administrator can specify certain default settings to ensure that groups, when created, acquire a set of values for the desired settings. Settings include:

- The recipients for the non-delivery report (NDR), that is sent when a message sent to a group is not delivered.
- Whether to show or hide the membership of mail-enabled groups in the messaging provider's address book (such as the Outlook address book).
- Standard text to appear in the notes for Smart Groups and Dynasties created using Automate.

These settings can be modified for each group individually on the **Exchange Advanced** tab (Figure 43) in group properties.

Additionally, the administrator can also specify the following settings, that cannot be modified.

- Whether to use the Global Catalog or the domain specified for the identity store as the default container for finding recipients (for Active Directory-based identity stores only).
- Whether to display nested ownership in the My Groups pane (Figure 9).

  If nested ownership is not displayed, the My Groups listing will display groups that have the logged-in user set as the primary owner, additional owner or Exchange additional owner.

  If nested ownership is displayed, then the My Groups listing will display groups with nested ownership as well. Suppose the logged-in user is a member of a security group that is set as a primary or additional owner of other groups. In nested ownership, those groups will be listed too.

Set group naming convention

The administrator can specify a regular expression to enforce a naming convention for groups when they are created using Automate.

Enforce Job Selection

The GroupID administrator can enforce users, regardless of the identity store, to apply a Smart Group Update job to Smart Groups and Dynasties while creating them.

The job is applied on the **Update Options** page (Figure 34) of the **New Smart Group** and **New Dynasty** wizards.

Getting familiar with Automate’s user interface

In GroupID Management Console, expand the Automate node to view its sub-nodes.

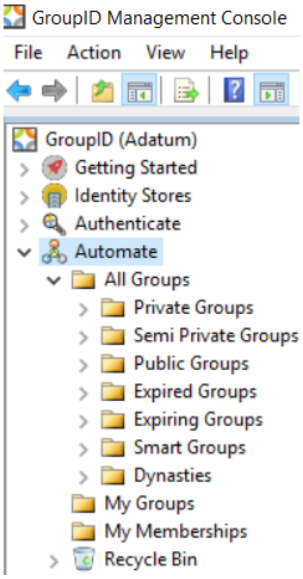


Figure 9: The Automate node

Following is a brief description of the Automate sub-nodes:

Sub-node	Description
All Groups	Shows all groups defined in the connected identity store. The list includes all groups whether they are: • Universal, Global, or Local • Private, semi-private, or public • Static group, Smart Group or Dynasty • Distribution list or security group • Active, expiring, expired, and logically deleted groups Learn more about these group types in Appendix A - Group Management Concepts. Viewing all groups on the directory server may slow down the loading of groups in this view, especially when there are more than 100 groups. You can specify the maximum number of groups to display in a view. See Set Pagination for Automate listings on page 163 for details.
Private Groups	Shows only the private groups created using GroupID in the connected identity store. It does not list expired or deleted private groups.
Semi Private Groups	Shows only the semi-private groups created using GroupID in the connected identity store. It does not list expired or deleted semi-private groups.

Public Groups	Shows only the public groups created using GroupID in the connected identity store. It does not list expired or deleted public groups.
Expired Groups	Shows only the expired groups in the connected identity store. A group expires when: • its validity period, as defined in its expiry policy, ends, or • The administrator manually expires a group Expired groups are locked for all activities until renewed. Group expiry is discussed in detail in Expire groups on page 75.
Expiring Groups	Shows only the expiring groups in the connected identity store. Groups that will expire in 30 days or less are considered as expiring groups. The expiry date is calculated from a group's expiry policy. The Group Life Cycle job is responsible for expiring these groups on their respective expiry dates; however, you can also manually expire a group before it reaches the expiry date.
Smart Groups	Shows only the Smart Groups created using GroupID in the connected identity store. It does not list expired or deleted Smart Groups.
Dynasties	Shows only the Dynasties created using Automate in the connected identity store. It does not list expired or deleted Dynasties. The **Type** column shows whether a Dynasty is a parent, middle, or leaf Dynasty. Both middle and leaf Dynasties are child Dynasties. The parent Dynasty comes at the top of the hierarchy, followed by middle and then leaf Dynasties. Dynasty names help you group a parent Dynasty with its respective child Dynasties. • For an organizational/geographical/custom Dynasty: The name of a child Dynasty starts with the name of its parent Dynasty (unless you change the naming template for Dynasty children). • For a managerial Dynasty: By default, the naming template for its child Dynasties starts with "Direct reports of <manager>". To modify the display name template for child Dynasties, see Modify alias and display name structure on page 136.
My Groups	Shows all groups for which the logged-in user is the direct or indirect owner, depending on the 'Display nested ownership in My Groups' setting in GroupID configurations. • If the GroupID administrator does not apply this setting, the My Groups listing displays groups that have the logged-in user set

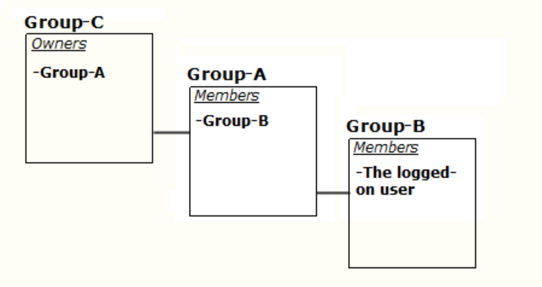
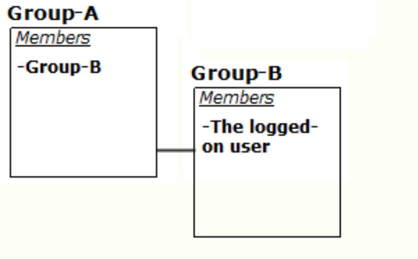
	as the primary owner, additional owner or Exchange additional owner. • If nested ownership is displayed, then the My Groups listing displays groups that have the logged-in user set as the direct or indirect owner. To understand the concept of indirect ownership, consider the scenario shown in the following figure:  Group-C Owners -Group-A Group-A Members -Group-B Group-B Members -The logged-on user Here, the logged-in user is a member of Group-B and Group-B is a member of Group-A. Now, when Group-A is set as a primary or additional owner of Group-C, the **My Groups** page for the logged-in user will include Group-C, because the user is an indirect owner of this group. The view also includes expiring, expired, and logically deleted groups.
My Memberships	Shows the groups that the logged-on user is a direct or indirect member of. To understand the concept of indirect membership, consider the scenario shown in the following figure:  Group-A Members -Group-B Group-B Members -The logged-on user Here, the logged-on user is a member of Group-B and Group-B is a member of Group-A. Now, the **My Memberships** page for the logged-on user will include both Group-B (the user is a direct member of this group) and Group-A (the user is an indirect member of this group). The view also includes expiring, expired, and logically deleted groups.
Recycle Bin	The Recycle Bin displays logically and physically deleted groups. Deleted groups are discussed in detail in Group Deletion on page 82.

Table 1: The Automate node and its sub-nodes

Right-click a node or sub-node to display its respective shortcut menu with commands that you can execute at that level.

Scheduled jobs impacting Automate

Different types of scheduled jobs can be defined for an identity store. These jobs run at a set frequency and perform their respective operations. Of these, the following jobs impact Automate:

- Group Life Cycle job
- Managed By Life Cycle job
- Membership Life Cycle job
- Smart Group Update job
- Orphan Group Update job

Group Life Cycle job

The Group Life Cycle job is responsible for expiring groups and then logically deleting expired groups.

Based on the Group Life Cycle policy defined for the identity store, the Group Life Cycle job performs the following functions:

- Expires groups according to their expiry policy.
- Logically deletes expired groups after x number of days, starting from the expiry date.
- Extends or reduces the life of mail-enabled distribution groups based on group usage.

NOTE The Group Life Cycle job is licensed with GroupID Self-Service.

Managed By Life Cycle job

The Managed By Life Cycle job updates the temporary additional owners for groups and temporary additional managers for users.

- Group owners and users with the ‘Manage any Group’ permission in the identity store can specify a start and end date for adding or removing an object as the additional owner of a group. On this start date and end date, the Managed By Life Cycle job adds/removes that object as the group’s temporary additional owner.

- User managers and users with the ‘Manage any Profile’ permission in the identity store can specify a start and end date for adding or removing an object (user or contact) as an additional manager of a user. On this start date and end date, the Managed By Life Cycle job adds/removes that object as the temporary additional manager.

Membership Life Cycle job

The Membership Life Cycle job updates the temporary membership of groups.

- Group owners can specify dates for an object to be added or removed for a temporary period from the membership of a group (see the **Members** tab in group properties - Figure 37). When the period starts or ends, the Membership Life Cycle job adds/removes these members from group membership accordingly.
- Using the Self-Service portal, managers and peers can join and leave a group temporarily on behalf of other users. The Membership Life Cycle job adds/removes those users from group membership on the specified dates.
- The job also executes the membership lifecycle policy for static groups in an identity store.
- The job also removes members when group owners inactivate them during group attestation (if group attestation has been enabled in the Group Life Cycle policy defined for the identity store).

Smart Group Update job

This is a scheduled job that updates the following for Smart Groups and Dynasties:

- Group membership
  A Smart Group or Dynasty has a user-defined query specified for it. When a Smart Group Update job associated with the group runs, it updates group membership with records fetched by the query.
- Certain attribute values for nested Smart Groups and Dynasty children

A Smart Group or Dynasty will not be automatically updated if it is not linked with a Smart Group Update job,

For more details, see Appendix C: Define a Smart Group Update job.

Orphan Group Update job

This job assigns a primary owner to orphan groups.

The orphan group must have at least one additional owner, since the first additional owner in the group’s additional owners list is promoted as primary owner.

Chapter 3 - Second Factor Authentication

The GroupID administrator can enable second factor authentication for a user role in an identity store.

This implies that, in addition to providing a valid username and password to connect GroupID Management Console to an identity store, role members must authenticate their identity store account using an authentication type.

Second factor authentication works differently for enrolled and unenrolled users, as discussed in step 6 under Connect GroupID Management Console to an identity store on page 1.

Supported authentication types

GroupID supports the following authentication types:

- Security Questions
- SMS
- Email
- Authenticator
- YubiKey
- PhoneID
- Windows Hello

Security Questions authentication

The administrator is responsible for configuring the security questions that users must answer to enroll their identity store accounts in GroupID.

To authenticate using the security questions, users must provide answers to the security questions they used to enroll their accounts with.

SMS verification

In SMS authentication, confirmation codes sent on the user's mobile phone are used to enroll and authenticate.

- To enroll an identity store account through SMS verification, a user has to provide his or her mobile number. GroupID will send a verification code on this number via SMS and the user has to enter it in GroupID to enroll his or her account.
- To authenticate using SMS, a user has to provide the last 4 digits of his or her registered mobile number. GroupID then sends a confirmation code on this number; the user has to enter the code in GroupID for authentication.

NOTE For SMS authentication to work, an SMS gateway account must be associated with the identity store.

Email verification

In Email authentication, confirmation codes sent on the user's email address are used to enroll and authenticate.

- To enroll an identity store account through Email verification, a user has to provide his or her email address. GroupID will send a verification code to this email address and the user has to enter it in GroupID to enroll his or her account.
- To authenticate using Email, a user has to complete the email address he or she provided during enrollment. GroupID then sends a confirmation code to this email address; the user has to enter the code in GroupID for authentication.

NOTE For Email authentication to work, an SMTP server must be defined for the identity store.

Authenticator app

Users have to install the Google Authenticator or Microsoft Authenticator app on their smartphones and use it to enroll and authenticate their identity store accounts in GroupID.

- To enroll, a user has to use the Authenticator app on his or her phone to scan the QR (Quick Response code) image displayed in GroupID. This generates a verification code in the app, that the user has to enter in the console to enroll. Authenticator apps use the TOTP (Time-based One-Time

Password) algorithm and generate a new code every 30 seconds, so each code expires after 30 seconds.

- To authenticate, the user simply has to launch the Authenticator app on his or her phone and enter the QR code generated by the app in GroupID.

YubiKey authentication

YubiKey is a key-sized device that users can plug into the computer's USB slot to provide another layer of security when accessing their identity store accounts.

- To enroll your identity store account using YubiKey, insert the YubiKey device in the USB slot of your computer, enter a name for your device in GroupID and tap on the device.
- To authenticate with this YubiKey, insert the device in your computer and with the GroupID window displayed, tap on the device.

Users can enroll and authenticate with a YubiKey only on a physical machine. Virtual machines are not supported.

YubiKey supported browsers:

- Google Chrome version 38 or later
- Opera version 40 or later
- Firefox (requires the U2F Support Add-on extension)

IE and Microsoft Edge are not supported.

PhoneID authentication

The PhoneID app offers a password-less identity solution. It can work with any application to validate users' identity.

To use PhoneID for authentication, users have to install the PhoneID app on their phones. The app is available on Google Play as well as on App Store.

- To enroll using PhoneID, the user has to provide his or her mobile number in GroupID. GroupID sends a notification on this mobile number, asking for a confirmation. Tapping 'Yes' on the notification enrolls the user in GroupID.
- To authenticate using PhoneID, the user has to provide the last four digits of his or her mobile phone number. GroupID sends a notification on this mobile number, asking for confirmation. Tapping 'Yes' on the notification authenticates the user in GroupID.

PhoneID installation and registration

1. Open Google Play or App Store on your mobile and search for Imanami PhoneID.
2. Tap . PhoneID will take a few minutes to get installed on your phone.
3. Launch the PhoneID app on your phone and on the main page, tap .
4. The page displays the steps you have to follow to start using PhoneID. Tap .
5. On the next page, select your country and enter your mobile phone number.
6. Click .
7. PhoneID sends a verification code on your phone number by SMS. One of the following happens:
   - PhoneID automatically detects the verification code. This completes the installation and registration process.
   - If PhoneID does not automatically detect the code, enter it manually in the **Please Enter Verification Code** box and click **Verify**. This completes the installation and registration process.

You can unregister your mobile number using the button.

Windows Hello authentication

The Windows Hello authentication type can be used on devices running Windows 10 with specialized hardware installed, such as fingerprint reader and 3D camera.

To enable Windows Hello on Windows 10:

1. Go to the **Start** ⊞ menu and select **Settings**.
2. Go to **Accounts** > **Sign-in options**.
3. Windows Hello prompts you to enter a PIN; click/tap **Add** under **PIN** to set up a PIN code first.
   Having set a PIN, proceed to add biometric data.
4. In the **Windows Hello** section, click **Set up** under **Face** or **Fingerprint** to add the recognition data.

NOTE

If your device does not meet the hardware requirements, Windows Hello is not available, even if Windows 10 is installed on it.

Window Hello supports the Microsoft Edge browser only.

Enroll your identity store account

With second factor authentication enabled, unenrolled users must enroll their identity store account in GroupID while connecting GroupID Management Console to that identity store.

Enrolling an identity store account means that a user must register this account in GroupID using an authentication type.

Once a user has enrolled his or her identity store account, he or she must authenticate with the same authentication type every time he or she attempts to connect GroupID Management Console to that identity store.

To enroll an identity store account:

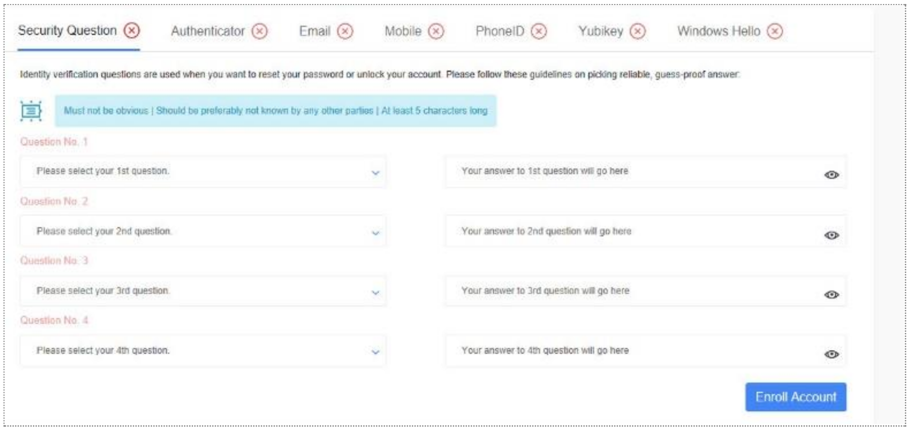
On clicking **Log in** on the **Login** window (Figure 3), unenrolled users are directed to the **Enroll Account** window (Figure 6).

The authentication type(s) enabled by the administrator for enrollment are listed as tabs on this window. You must enroll using one authentication type.

- If only one authentication type is available, you must enroll with it.
- If more than one authentication types are available, you can choose an authentication type to enroll with.

Enroll your account using Security Questions

1. On the window, click the tab.


Security Question ⊗
Authenticator ⊗
Email ⊗
Mobile ⊗
PhoneID ⊗
Yubikey ⊗
Windows Hello ⊗
Question No. 1
Please select your 1st question.
Your answer to 1st question will go here
Question No. 2
Please select your 2nd question.
Your answer to 2nd question will go here
Question No. 3
Please select your 3rd question.
Your answer to 3rd question will go here
Question No. 4
Please select your 4th question.
Your answer to 4th question will go here
Enroll Account

Identity verification questions are used when you want to reset your password or unlock your account. Please follow these guidelines on picking reliable, guess-proof answer:

Must not be obvious | Should be preferably not known by any other parties | At least 5 characters long

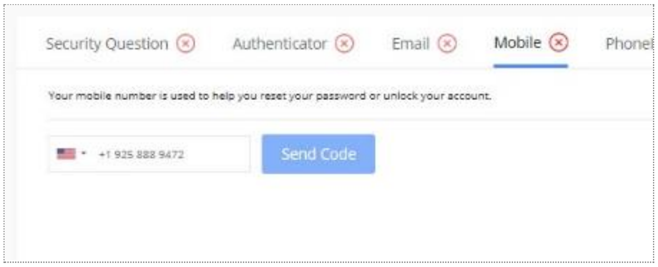
Figure 10: Security Questions tab for enrollment

2. From a list, select a security question of your choice (X represents the question number).

3. In the a box, type an answer for the selected question.
   If the answer meets the requirements, such as length-related checks, a tick mark is displayed for it.
4. Repeat steps 2 and 3 to select another security question and provide an answer.
5. Click .

Enroll your account using SMS

1. On the window, click the tab.



Your mobile number is used to help you reset your password or unlock your account.

+1 925 888 9472

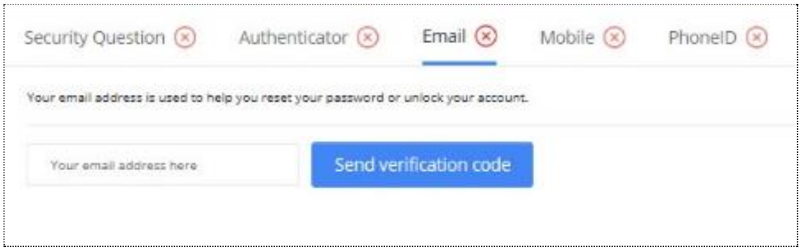
Figure 11: Mobile tab for enrollment

2. Select your country and then type your mobile number in the box.
3. Click .
4. When the verification code is successfully sent to your provided mobile number, a box is displayed; enter the received code in it.
5. Click .

If you do not receive the code, recheck your mobile number and click **Send code again**.

Enroll your account using Email

1. On the window, click the tab.



Your email address is used to help you reset your password or unlock your account.

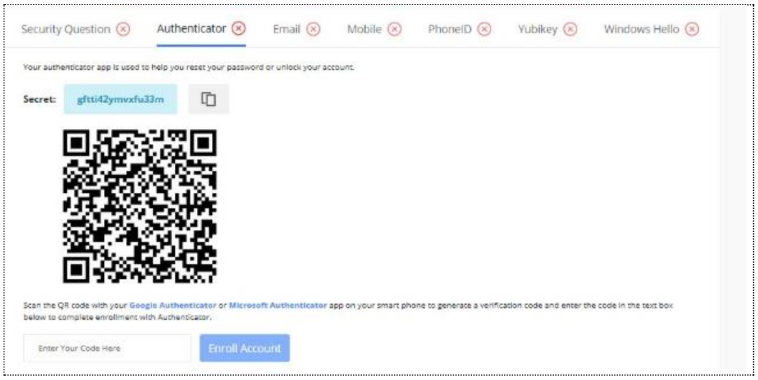
Figure 12: Email tab for enrollment

2. Type your email address in the box and click .
3. When the code is successfully sent to your provided email address, a box is displayed; enter the received code in it.
4. Click .

If you do not receive the code, recheck your email address and click .

Enroll your account using Authenticator

1. On the **Enroll Account** window, click the **Authenticator** tab.



Your authenticator app is used to help you reset your password or unlock your account.

Secret: gftti42ymvxfu33m

Scan the QR code with your Google Authenticator or Microsoft Authenticator app on your smart phone to generate a verification code and enter the code in the text box below to complete enrollment with Authenticator.

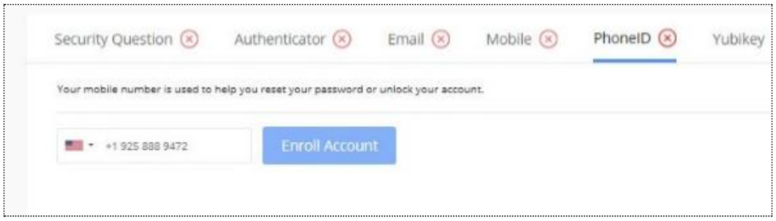
Figure 13: Authenticator tab for enrollmentScan the QR code (Quick Response code) with the authenticator app installed on your phone.
The app generates a verification code and displays it on your phone’s screen.

3. Enter this code in the box and click .

The authenticator app generates a new code every 30 seconds, so each code expires after 30 seconds.

Enroll your account using PhoneID

1. On the **Enroll Account** window, click the **PhoneID** tab.



Your mobile number is used to help you reset your password or unlock your account.

+1 925 888 9472

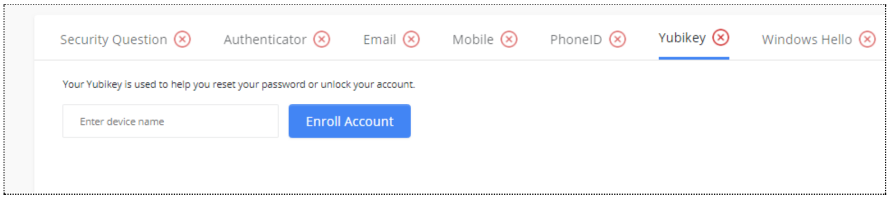
Figure 14: PhoneID tab for enrollment

2. Select your country and enter your phone number.

3. Click **Enroll Account**.
   GroupID sends a verification request on your mobile number.
4. You will receive a PhoneID login request notification on your mobile. Tapping ‘Yes’ on this notification enrolls your account in GroupID.

Enroll your account using YubiKey

1. Insert the YubiKey device in the USB slot of your computer.
2. On the window, click the tab.



Your Yubikey is used to help you reset your password or unlock your account.

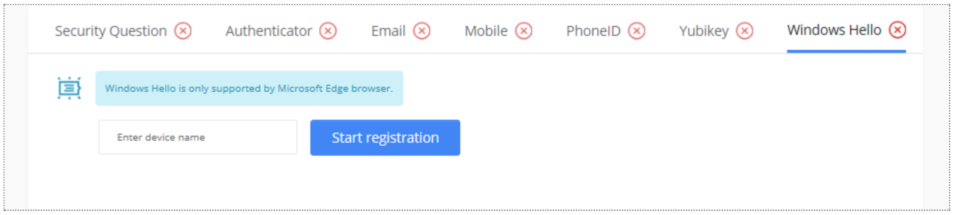
Figure 15: YubiKey tab for enrollment

3. Enter a name for your YubiKey device.
4. Click .

GroupID directs you to tap on the device. This enrolls your account in GroupID.

Enroll your account using Windows Hello

1. On the window, click the **Windows Hello** tab.



Windows Hello is only supported by Microsoft Edge browser.

Figure 16: Windows Hello tab for enrollment

2. Enter a name for your authentication device.
3. Click **Start Registration**.

Authenticate your identity store account

With second factor authentication enabled, users must authenticate the identity store account they want to use for connecting GroupID Management Console to that identity store.

Authenticating an identity store account means that a user must prove his or her identity using the authentication type he or she used to enroll his or her identity store account with.

To authenticate your identity store account:

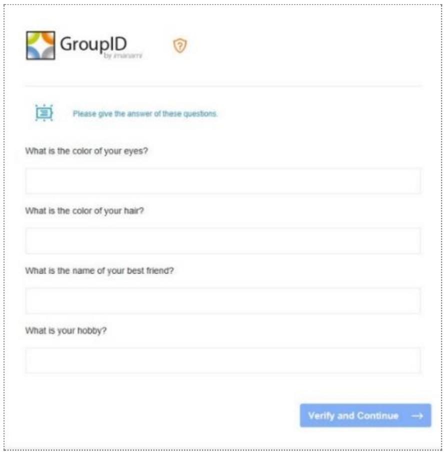
On clicking **Log in** on the **Login** window (Figure 3), enrolled users are directed to the **Authenticate Account** window (Figure 7).

This window displays the authentication type(s) you enrolled this account with. You must authenticate using one authentication type.

- If you enrolled with only one authentication type, then you can authenticate with this type only.
- If you enrolled with more than one authentication type, all these types are available on the **Authenticate Account** window. You can choose an authentication type to authenticate with.

Authenticate using Security Questions

1. On the **Authenticate Account** window (Figure 7), select **Security Questions** and click **Continue**.



Please give the answer of these questions.

What is the color of your eyes?

What is the color of your hair?

What is the name of your best friend?

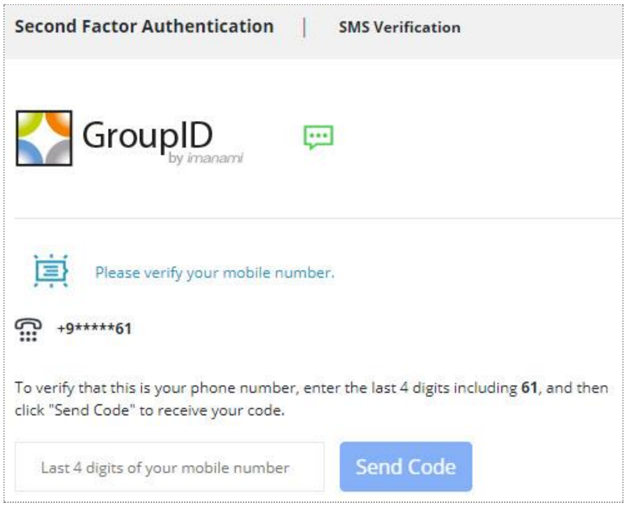
What is your hobby?

Figure 17: Security Questions tab for authentication

2. Provide answers to the security questions you enrolled your account with.
3. Click **Verify and Continue**.

Authenticate using SMS

1. On the **Authenticate Account** window (Figure 7), select **Mobile Verification** and click **Continue**.



Second Factor Authentication | SMS Verification
GroupID by imanami
Last 4 digits of your mobile number
Send Code

Please verify your mobile number.

☎ +9*****61

To verify that this is your phone number, enter the last 4 digits including **61**, and then click "Send Code" to receive your code.

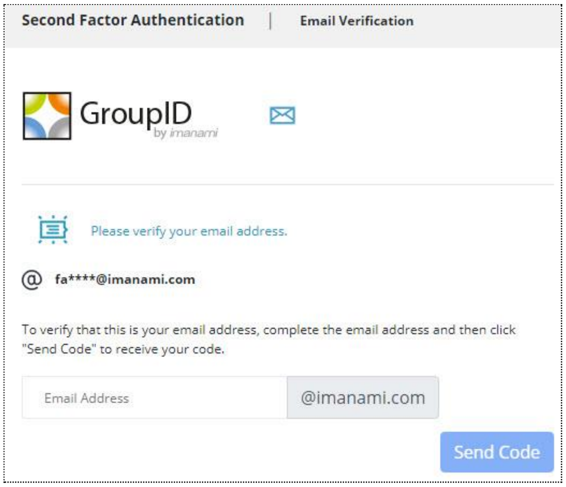
Figure 18: Mobile Verification tab for authentication

2. Type in the last four digits of your mobile number and click **Send Code**.
3. In the *access code* box, type the 5 digit access code sent on your mobile phone by SMS.
4. Click **Verify and Continue**.

If you do not receive a code, click **Send Again** and then enter the received code in the box.

Authenticate using Email

1. On the **Authenticate Account** window (Figure 7), select and click **Continue**.



Please verify your email address.

@ fa****@imanami.com

To verify that this is your email address, complete the email address and then click "Send Code" to receive your code.

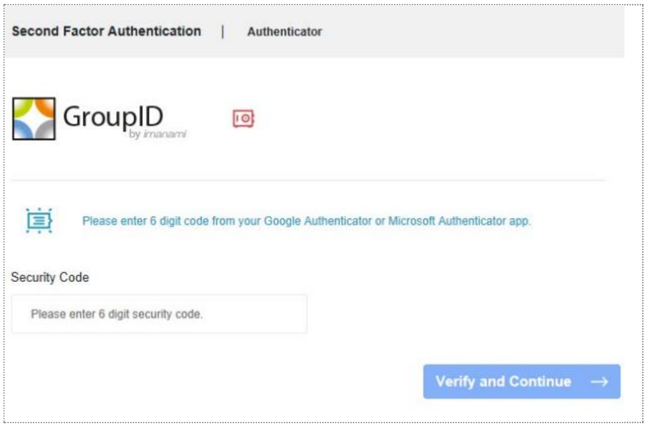
Figure 19: Email Verification tab for authentication

2. Complete your email address and click .
3. In the *a* box, type the 5 digit access code sent to the provided email address.
4. Click **Verify and Continue**.

If you do not receive a code, click and then enter the received code in the box.

Authenticator using Authenticator

1. On the **Authenticate Account** window (Figure 7), select **Authenticator** and click **Continue**.


Second Factor Authentication | Authenticator
GroupID by imanami
Security Code
Please enter 6 digit security code.
Verify and Continue →

Please enter 6 digit code from your Google Authenticator or Microsoft Authenticator app.

Figure 20: Authenticator tab for authentication

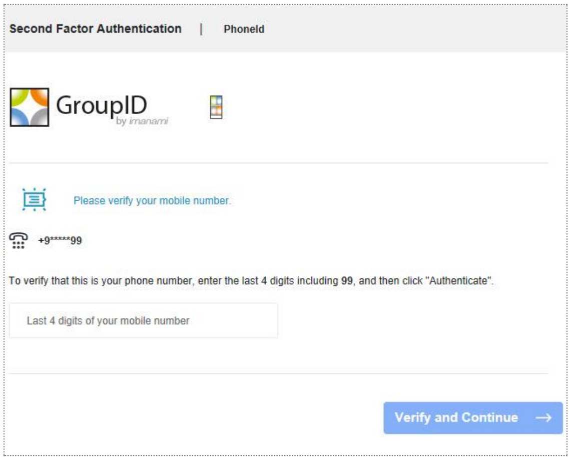
2. Launch the Google Authenticator or Microsoft Authenticator app on your smartphone. The app generates a verification code and displays it on your phone’s screen.

3. Enter the code in the **Security Code** box.
4. Click **Verify and Continue**.

Authenticator apps generate a new code every 30 seconds, so each code expires after 30 seconds.

Authenticate using PhoneID

1. On the **Authenticate Account** window (Figure 7), select and click **Continue**.



Second Factor Authentication | PhoneId

Please verify your mobile number.

☎ +9*****99

To verify that this is your phone number, enter the last 4 digits including 99, and then click "Authenticate".

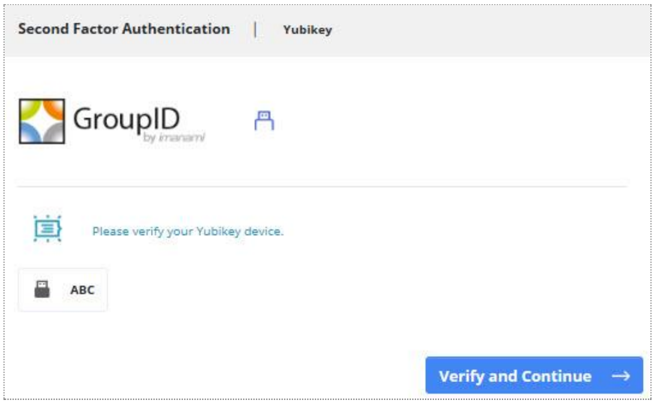
Last 4 digits of your mobile number

Figure 21: PhoneID tab for authentication

2. Type the last four digits of your mobile number and click **Verify and Continue**.
3. You will receive the PhoneID Login request notification on your mobile. Tapping ‘Yes’ on the notification authenticates you in GroupID.

Authenticate using YubiKey

1. Insert the YubiKey device in the USB slot of your computer.
2. On the **Authenticate Account** window (Figure 7), select **YubiKey Verification** and click **Continue**.

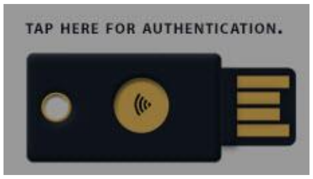


Second Factor Authentication | Yubikey

Please verify your Yubikey device.

Figure 22: YubiKey Verification tab for authentication

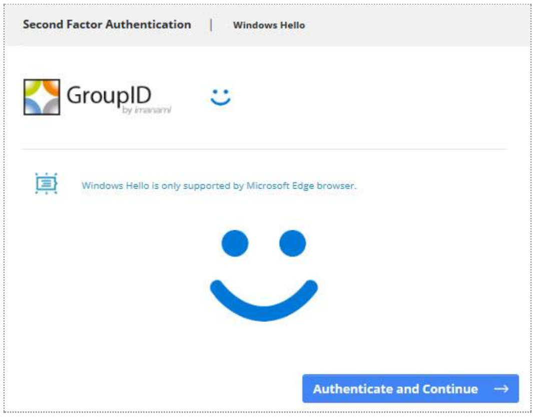
3. Click your YubiKey device name.
   GroupID directs you to tap on the device.



4. On tapping, you are authenticated in GroupID.

Authenticate using Windows Hello

1. On the **Authenticate Account** window (Figure 7), select **Windows Hello** and click **Continue**.



Second Factor Authentication | Windows Hello

Windows Hello is only supported by Microsoft Edge browser.

Figure 23: Windows Hello tab for authentication

2. Click **Authenticate and Continue**.

3. Provide the biometric information you enrolled your account with.

Chapter 4 - Creating Groups

Using Automate, you can create:

- A normal directory group, also called an unmanaged or static group

  An unmanaged group is a group you would normally create in a directory (for example, by using the Active Directory Users and Computers snap-in). Though such groups can be created using GroupID Automate and Self-Service portal, GroupID does not support dynamic updates to them. Any changes to the membership have to be updated manually.

- A Smart Group (normal Smart Group and Smart Group with a password expiry condition)

  A Smart Group is one that dynamically maintains its membership based on rules. These rules are applied in the form of a user-defined query, such as an LDAP query. This query is defined once and scheduled for membership update using a Smart Group Update job. When the Smart Group update job runs, it applies the defined rules to update the group's memberships.

  In this way, Smart Groups are automatically updated whenever the directory information changes. This automated group management allows administrators to easily maintain large distribution lists and security groups without having to manually add or remove members.

- A Dynasty

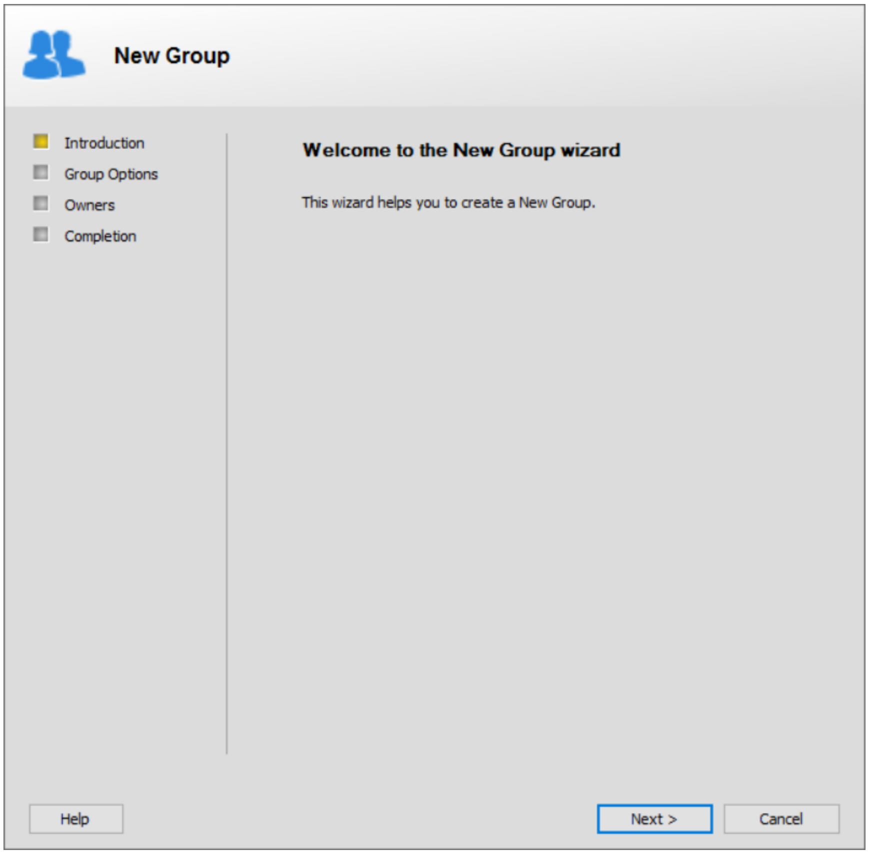
  A Dynasty is a Smart Group that creates and manages other Smart Groups using information in the directory. Dynasties help you manage large distribution lists by creating hierarchical group structures that represent your organization’s hierarchy.

  To create and manage dynasties, see Chapter 9 - Dynasties on page 113.

Create a static group in an Active Directory identity store

1. In GroupID Management Console, select **Automate** > right-click **All Groups** > **New** > **Group**.

   The **New Group** wizard opens to the **Welcome** page.

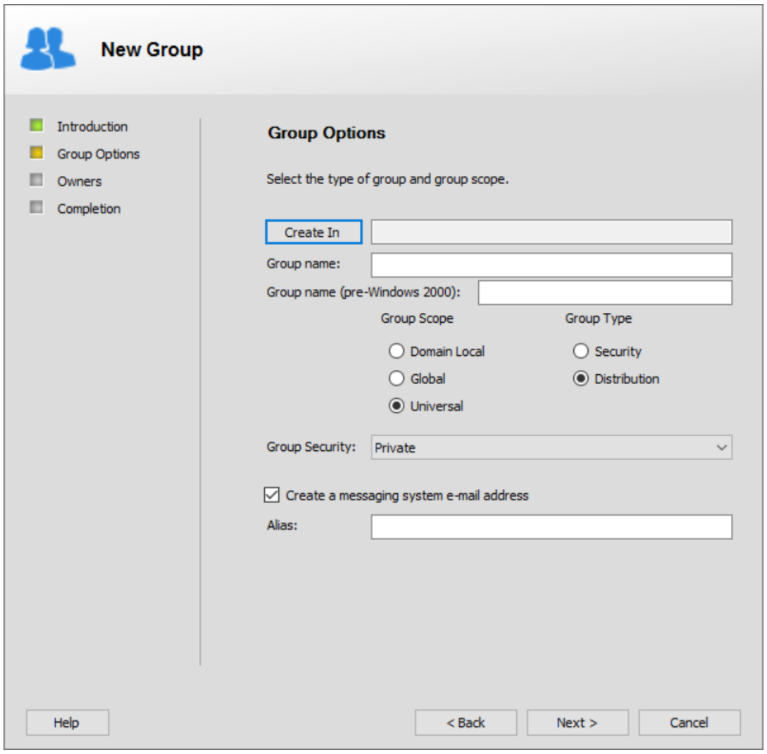
   

   Welcome to the New Group wizard

   This wizard helps you to create a New Group.

   Figure 24: Welcome page

2. Read the message and click **Next**.
   The **Group Options** page is displayed.



New Group

Group Options

Select the type of group and group scope.

Create In

Group name:

Group name (pre-Windows 2000):

Group Scope: ○ Domain Local ○ Global ● Universal

Group Type: ○ Security ● Distribution

Group Security: Private

☑ Create a messaging system e-mail address

Alias:

Figure 25: Group Options page

3. Click **Create in** to select a container to create the group in.
   On the **Select Container** dialog box, select the required container and click **OK**.

   You can create a group in a domain other than the logged-on domain, provided that the service account for the identity store has the required permissions on that domain.

4. In the **Prefix** box, which is displayed when prefixes are defined in identity store configurations, select a prefix to append the group name.

   See Group name prefixes on page 4.

5. In the **Group name** box, type a name for the group. In Active Directory, the group name is limited to 64 characters.

   If the administrator has defined a regular expression as a group naming convention in GroupID configurations, your group name must conform to it.

6. The group name you enter also appears in the **Group name (Pre-Windows 2000)** box. You can change it if required.

   In Active Directory, group name (Pre-Windows 2000) is limited to 20 characters.

7. In the **Group Scope** area, select an option to set a scope for this group. Group scope controls who or what can be a member of the group and what the group can be used for.

   - **Domain Local** - Can contain users in this domain.
   - **Global** - Can contain users from other domains but is visible only within its own domain.
   - **Universal** - Can contain users and groups from any domain and is visible in the Global Catalog.

   Click here for more information.

8. In the **Group Type** area, select an option to set the group's type.

   - **Security** - to use this group for securing public folders or other resources.
   - **Distribution** - to use this group for mail distribution.

9. From the **Group Security** list, select an option to set the group's security type. Security types determine the access level for a group.

   - **Private** - to restrict access to the group to members selected by the group owner. Only the owner can add or remove members from the group. Requests to join or leave the group cannot be submitted.
   - **Semi-Private** - to restrict access to the group to members selected by the group owner. However, requests to join or leave the group can be sent to the owner.
   - **Public** - to allow all users to access the group. Users can join or leave the group at will and do not require any permission to do so.

   NOTE Group security is licensed with GroupID Self-Service.

10. Select the **Create a messaging system e-mail address** check box to mail-enable the group and set an alias for it.

    Clear this check box to create the group as non-mail-enabled.

    This check box is available if a messaging system is configured for the identity store.

    NOTE With Exchange 2010/2013/2016/2019 configured as the messaging provider, you can only create this group as mail-enabled if the group scope is set to *Universal*.

11. In the **Alias** box, type an alias for the group.

If Exchange Server is the designated messaging system for the identity store, then the alias length is limited to 64 characters and must be unique to the forest. For other messaging systems, the alias length must not exceed the number of characters supported by the respective messaging system.

Also, the alias must not contain characters that are invalid for the configured messaging system. The following table lists the valid characters for the supported messaging systems:

<table>
<tr><th>Messaging System</th><th>Valid Characters</th></tr>
<tr><td>Exchange Server 2010/2013/2016/2019</td><td>• Uppercase letters (A - Z)
• Lowercase letters (a - z)
• Numeric digits (0 - 9)
• Special characters (#, $, %, &, ', *, +, -, /, =, ?, ^, _, `, {, |, } or ~). You can use one or more periods in an alias, but each must be preceded and followed by at least one of the other characters.</td></tr>
<tr><td>All other messaging systems</td><td>• Uppercase letters (A - Z)
• Lowercase letters (a - z)
• Numeric digits (0 - 9)</td></tr>
</table>

Table 2: Valid Characters for Aliases

12. Click **Next**.
    The **Owners** page is displayed.

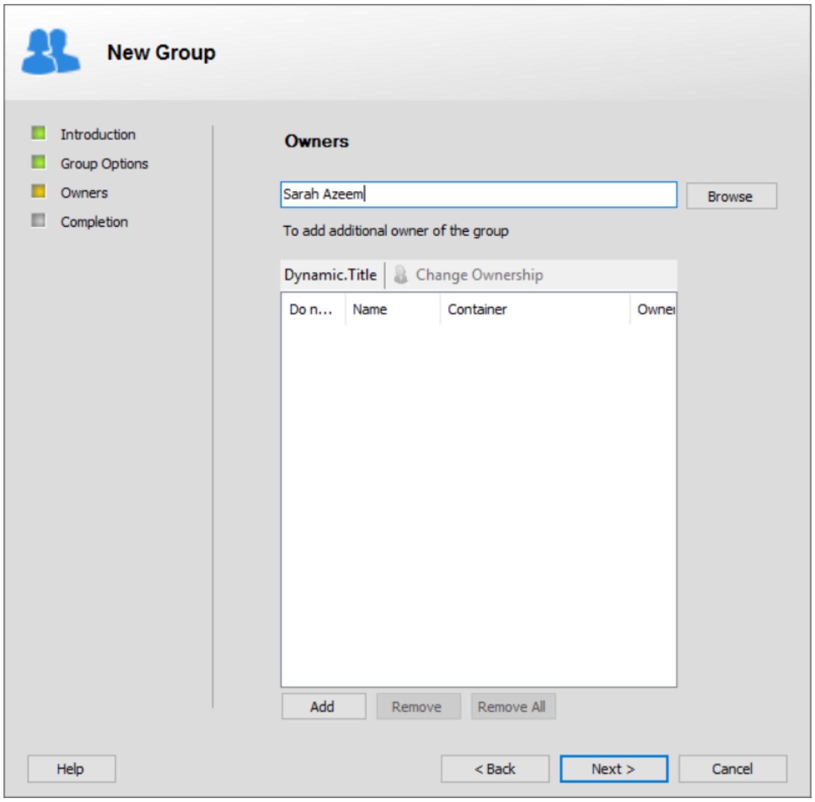


Figure 26: Owners page

When a group is created, Automate specifies the logged-on user as its primary owner. You can change the primary owner as well as specify temporary and permanent additional owners for the group.

Additional owners have the same privileges as the primary owner to manage the group. Like the primary owner, additional owners receive expiry, deletion and renewal notifications for the group and they can take the necessary actions indicated.

After a group is created, you can modify primary and additional owners using the **Managed By** tab (Figure 39) in group properties and the Transfer Ownership wizard.

NOTE Only users, contacts and security groups can be set as the primary and additional owners of a group. In case of a group, all its members are considered as owners.

13. The box displays the name of the logged-on user as the group’s primary owner.

    To change it, click **Browse**. On the **Find** dialog box (Figure 46), you can select another owner.

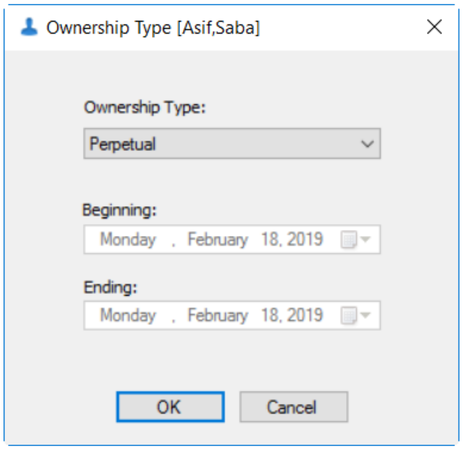
14. To specify additional owners for the group, click **Add**.

    Use the **Find** dialog box (Figure 46) to search and select groups, users, and contacts to set as additional owners of the group.

    - To remove an additional owner, select it in the list and click **Remove**.
    - To remove all additional owners, click **Remove All**.

15. By default, additional owners are added as permanent owners. However, you can change the ownership type (ownership type indicates whether an object is a temporary or permanent additional owner of a group).

    a. Select an additional owner and click **Change Ownership** to change its ownership type.



Ownership Type [Asif,Saba]

Ownership Type: Perpetual

Beginning: Monday , February 18, 2019

Ending: Monday , February 18, 2019

Figure 27: Ownership Type dialog box

    b. Select an option from the **Ownership Type** list:

Ownership Type	Description
Perpetual	To make the object a permanent additional owner of the group.
Temporary Owner	To make the object a temporary additional owner of the group for the period you specify in the **Beginning** and **Ending** boxes. At the end of the period, the object is removed from the group ownership.
Addition Pending	Indicates that the object will be a temporary additional owner of the group for a period in the future. Use the **Beginning** and **Ending** boxes to set a period. Before the beginning date, the object's *ownership type* is displayed as 'Addition Pending'.

	On the beginning date, the ownership type changes to 'Temporary Owner'. **Example:** You add Smith as a temporary additional owner of Group A on May 15, 2022 for future dates, May 20-30, 2022. Smith will be listed as Group A's additional owner with 'Addition Pending' as its ownership type from May 15 to 19, 2022. On May 20, Smith will become a temporary additional owner of Group A and its ownership type will change to 'Temporary Owner' from May 20 to 30, 2022. After May 30, Smith will be removed as Group A's additional owner.
Removal Pending	Indicates that the object will be temporarily removed from group ownership for a period in the future. Use the **Beginning** and **Ending** boxes to set a period. Before the beginning date, the object's ownership type is displayed as 'Removal Pending'. On the beginning date, the ownership type will change to 'Temporary Removed'. **Example:** You remove Smith as an additional owner of Group A on May 15, 2022 for future dates, May 20-30, 2022. Smith will be displayed as Group A's additional owner with 'Removal Pending' as ownership type from May 15 to 19, 2022. On May 20, Smith's ownership type in GroupID will change to 'Temporary Removed'; lasting till May 30, 2022. After May 30, Smith will be added back to Group A as a permanent additional owner.
Temporary Removed	Indicates that the object is temporarily removed from group ownership for the period specified in the **Beginning** and **Ending** boxes. At the end of the period, the object is added back to the group as a permanent additional owner.

Table 3: Ownership Type

c. Click **OK** to close the **Ownership Type** dialog box.

   The Managed By Life Cycle job updates the temporary ownership of groups by adding and removing temporary additional owners on the specified dates.

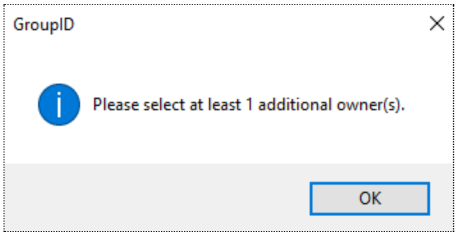
16. Like the primary owner, additional owners receive expiry, deletion and renewal notifications for the group and they can take the necessary actions indicated.

    To exclude an additional owner from receiving these email notifications, select the **Do not Notify** check box for it.

    NOTE For email notifications to be sent, an SMTP server must be configured for the identity store.

17. Click **Next**.

    You may observe a message, similar to the one shown below. It occurs because the Group Owners policy defined for your role in the identity store requires that the group must have at least x number of additional owners.

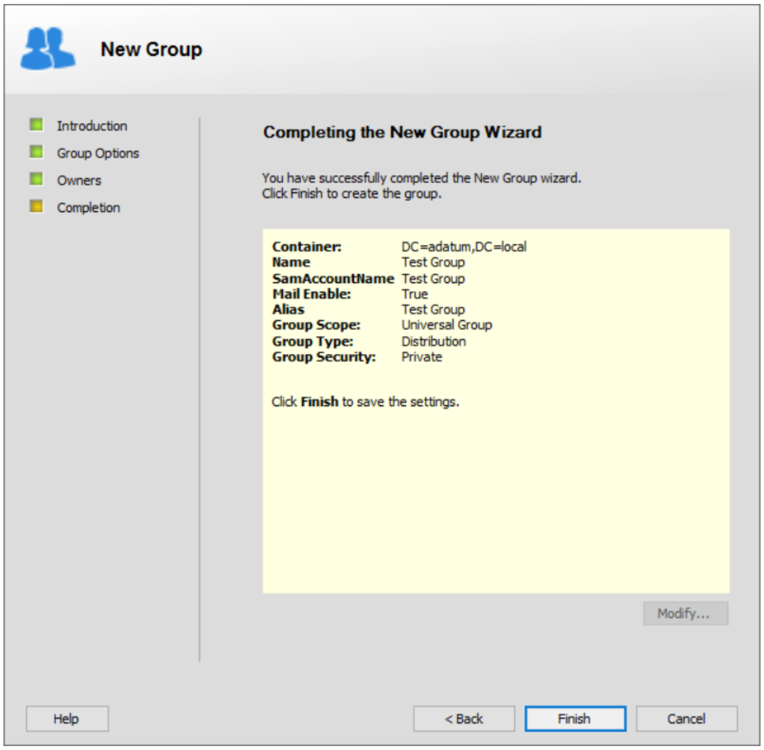
    GroupID

    Please select at least 1 additional owner(s).

    Figure 28: Owner required message

    Specify the said number of additional owners for the group and then click **Next**.

18. On the **Completion** page, review the settings that you have entered on the previous pages, using the **Back** button to access settings that you want to change.



Completing the New Group Wizard

You have successfully completed the New Group wizard.
Click Finish to create the group.

Container:	DC=adatum,DC=local
Name	Test Group
SamAccountName	Test Group
Mail Enable:	True
Alias	Test Group
Group Scope:	Universal Group
Group Type:	Distribution
Group Security:	Private

Click **Finish** to save the settings.

Figure 29: Completion page

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

20. When the group is created, the **Modify** and **Close** buttons get enabled.

    - Click **Modify** to open the group's properties.

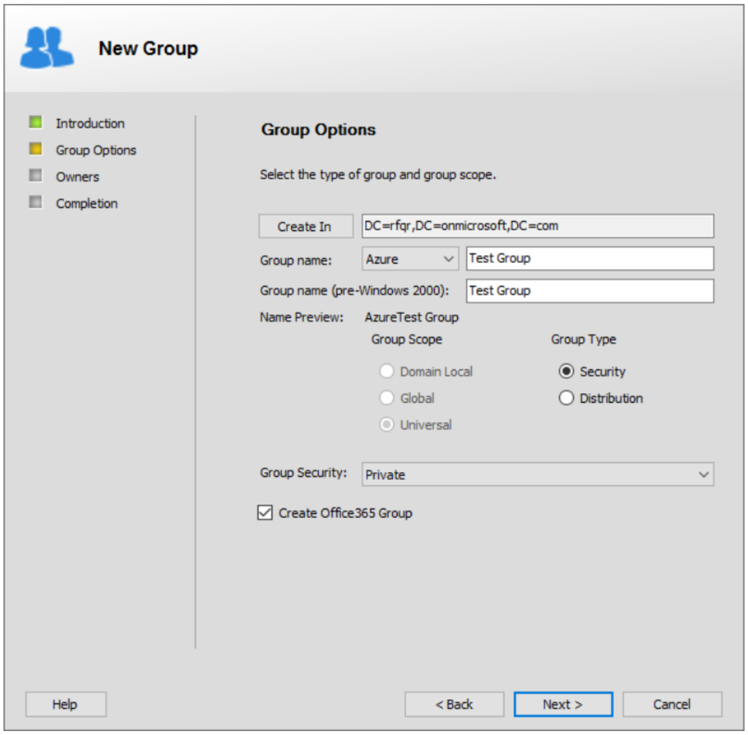
    - Click **Close** to close the **New Group** wizard.

Create a static group in an Azure identity store

1. In GroupID Management Console, select **Automate** > right-click **All Groups > New > Group**.

   The New Group wizard opens to the **Welcome** page (Figure 24).

2. Read the message and click **Next**.
   The **Group Options** page is displayed.



New Group

Group Options

Select the type of group and group scope.

Create In: DC=rfqr,DC=onmicrosoft,DC=com

Group name: Azure | Test Group

Group name (pre-Windows 2000): Test Group

Name Preview: AzureTest Group

Group Scope: ○ Domain Local ○ Global ○ Universal

Group Type: ● Security ○ Distribution

Group Security: Private

☑ Create Office365 Group

Figure 30: Group Options page

3. Click **Create in** to select a container to create the group in.
   On the **Select Container** dialog box, select the required container and click **OK**.

4. In the **Prefix** box, which is displayed when prefixes are defined in identity store configurations, select a prefix to append the group name.

   See Group name prefixes on page 4.

5. In the **Group name** box, type a name for the group. If the administrator has defined a regular expression as a group naming convention in GroupID configurations, your group name must conform to it.

6. The group name you enter also appears in the **Group name (Pre-Windows 2000)** box. Change it if required.

7. By default, groups in an Azure identity store have a universal scope. Since it cannot be changed, the **Group Scope** options are disabled.

8. In the **Group Type** area, select an option to set the group's type.

    - **Security** - to use this group for securing public folders or other resources.
    - **Distribution** - to use this group for mail distribution.

    ### To create a non mail-enabled security group:

    - Select Security as the group type.
    - Do not select the **Create Office 365 Group** check box.
      If you select it, an Office 365 group will be created instead of a security group.

    ### To create an Office 365 group:

    - Select *Security* as the group type.
    - Make sure you select the **Create Office 365 Group** check box to create an Office 365 group.

      If you do not select it, a security group will be created.

    ### To create a distribution list:

    - Select Distribution as the group type.
    - Whether or not you select the **Create Office 365 Group** check box, GroupID will create a distribution list.

    For a Dynasty, the **Create Office 365 Group** check box is not available because an Office 365 group cannot have groups as its members.

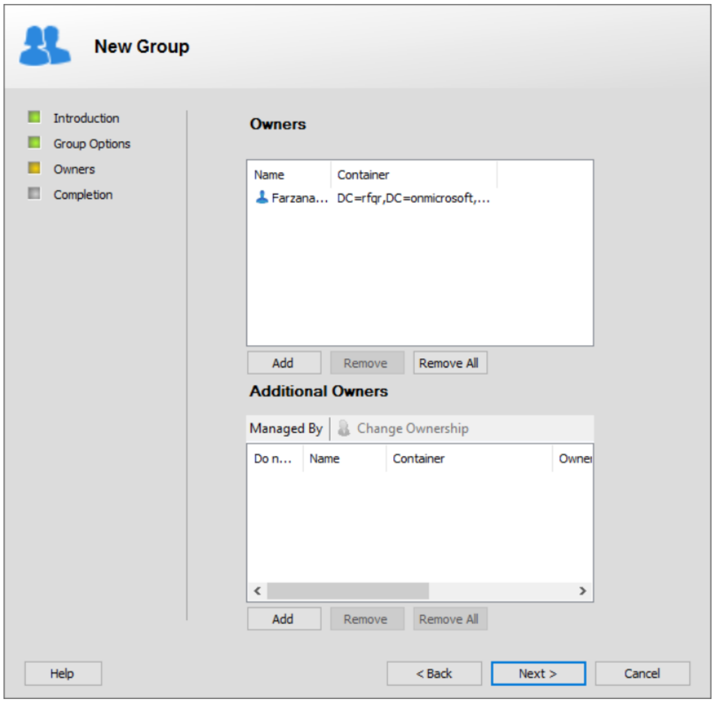
9. From the **Group Security** list, select an option to set the group's security type. Security types determine the access level for a group.

    - **Private** - to restrict access to the group to members selected by the group owner. Only the owner can add or remove members from the group. Requests to join or leave the group cannot be submitted.

- **Semi-Private** - to restrict access to the group to members selected by the group owner. However, requests to join or leave the group can be sent to the owner.

- **Public** - to allow all users to access the group. Users can join or leave the group at will and do not require any permissions to do so.

10. Click **Next**.
    The **Owners** page is displayed, which is similar to Figure 26, except that you can specify multiple primary owners for a group in an Azure identity store.



Name	Container
Farzana…	DC=rfqr,DC=onmicrosoft,…

Do n…	Name	Container	Owne

Figure 31: Owners Page

Follow the steps under Figure 26 to specify primary an additional owners for the group.

- You can only set users as primary owners in an Azure identity store.
- It is mandatory to have at least one primary owner to create a group in Azure identity store.

11. Click **Next**.

12. On the **Completion** page (Figure 29), click **Finish** to create the group.

Create a Smart Group

A Smart Group is one that dynamically maintains its membership based on the rules applied by a user-defined query, such as an LDAP query.

Rather than specifying static user memberships, you can use a query (for example, "All full-time employees in my company") to dynamically build membership in a Smart Group. Managing memberships with queries significantly reduces administrative costs.

Smart Groups in an Azure based identity store use a device structured query language while those in an Active Directory based identity store use LDAP queries to update group membership.

A Smart Group can also be created as a Password Expiry group. A Password Expiry group is a Smart Group whose membership contains users whose identity store account passwords are approaching their expiry dates. Members of this group are notified by email to reset their passwords. As soon as they do so, they are automatically removed from the group membership.

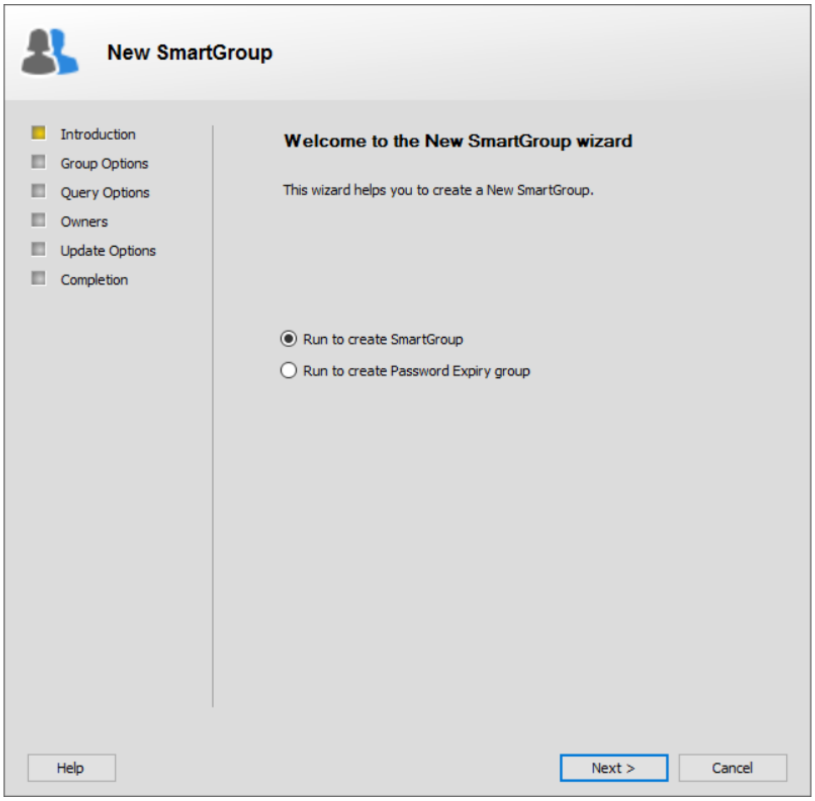
To create Password Expiry groups, you must have a password policy defined within the local security policy for your domain or directory server.

You should either apply a query to a group in the Azure portal or in GroupID. See Dynamic Groups in Azure in Appendix B.

To create a Smart Group:

1. In GroupID Management Console, select **Automate** > right-click **All Groups** > **New** > **Smart Group**.

   The **New Smart Group** wizard opens to the **Welcome** page.



Welcome to the New SmartGroup wizard

This wizard helps you to create a New SmartGroup.

● Run to create SmartGroup

○ Run to create Password Expiry group

Figure 32: Welcome page

2. Select one of the following options:

   - **Run to create Smart Group**, to create a new Smart Group.

     This option is selected by default and creates a conventional Smart Group with membership built and updated based on the query defined for it.

   - **Run to create Password Expiry group**, to create a Smart Group with a password expiry condition.

     A password expiry group is a Smart Group whose membership contains users whose identity store account passwords are approaching their expiry dates. Members of this group are notified by email to reset their passwords. When they do so, they are automatically removed from the group membership.

     The notification period and other relevant conditions for a password expiry group are set on the **Password Expiry Options** tab (Figure 93) of the **Query Designer** dialog box.

Password expiry groups cannot be created for an Azure-based identity store.

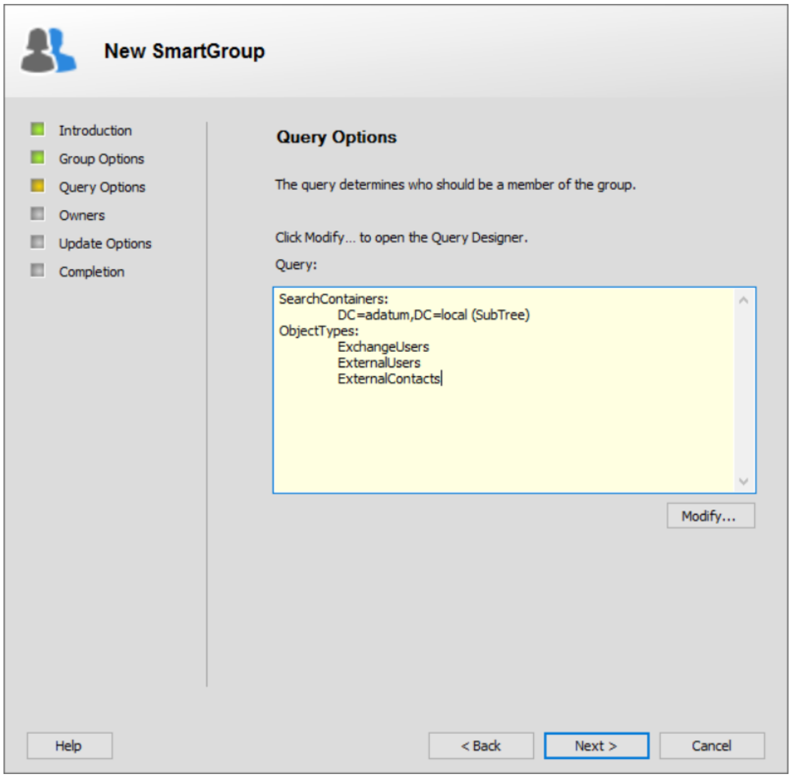
3. Click **Next**.
4. The **Group Options** page is displayed, which is similar to the **Group Options** page for a static group.

   - It is as shown in Figure 25 for a group in an Active Directory identity store.
   - It is as shown in Figure 30 for a group in an Azure identity store.

   Follow the instructions under the respective figure to specify group options for the Smart Group and click **Next**.
5. The **Query Options** page displays the default query that Automate will use to determine the members for this group

   - If a messaging provider is configured for the identity store, the default query returns messaging system recipients (users with mailboxes, users with external email addresses, and contacts with external email addresses).
   - Without a messaging provider, the default query returns all users, contacts, and groups in the identity store.
   - In case of an Azure identity store with a messaging provider configured, the default query returns messaging system recipients (users with mailboxes and users with external email addresses).
   - Without a messaging provider, the default query returns all users and groups. For an Office 365 group, however, only user objects are added to group membership.

   You can modify this query to limit the number of results, if required.



Query Options

The query determines who should be a member of the group.

Click Modify... to open the Query Designer.

Query:

```
SearchContainers:
        DC=adatum,DC=local (SubTree)
ObjectTypes:
        ExchangeUsers
        ExternalUsers
        ExternalContacts
```

Figure 33: Query Options page

6. To modify the query, click **Modify**; this launches the Query Designer dialog box, where you can edit the query.

   You can import or export a query from within the **Query Designer** dialog box using the **File > Import Query** or **File > Export Query** command on the main menu.

7. Click **Next**.

8. The **Owners** page is displayed, which is similar to the **Owners** page for a static group.

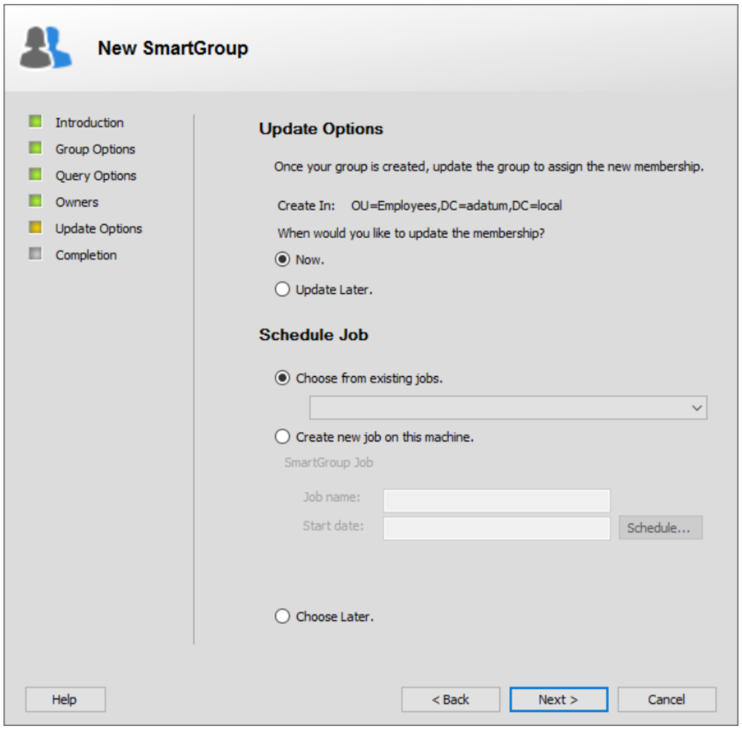
   - It is as shown in Figure 26 for a group in an Active Directory identity store.
   - It is as shown in Figure 31 for a group in an Azure identity store.

   Follow the instructions under the respective figure to assign primary and additional owners to the Smart Group as well as manage notifications for additional owners.

NOTE When a Smart Group Update job runs on a group, the notification behavior is as follows:

- If the **Do not Notify** check box is selected for an additional owner yet its email address is specified in the **To** box on the **Notification** tab (Figure 115) of the **Create/Edit Job** dialog box, the additional owner will receive the notifications.
- If the **Do not Notify** check box is selected for an additional owner yet the **Send Report to group owner(s)** check box is selected on the **Notification** tab (Figure 115) of the **Create/Edit Job** dialog box, the additional owner will not receive the notifications.

9. Click **Next**.
10. The **Update Options** page provides different options to update the group membership.



Update Options

Once your group is created, update the group to assign the new membership.

Create In: OU=Employees,DC=adatum,DC=local

When would you like to update the membership?

● Now.

○ Update Later.

Schedule Job

● Choose from existing jobs.

○ Create new job on this machine.

SmartGroup Job

Job name:

Start date:

○ Choose Later.

Figure 34: Update Options page

Automate provides multiple options to update the membership of Smart Groups. You can update the membership as soon as the Smart Group is created or you can define a scheduled Smart Group Update job to update the membership. The manual update option is also available, that you can use any time to update group membership.

Automate queries the directory (using the query on the **Query Options** page) to update the group membership. On the **Update Options** page, select when to update the membership of this Smart Group. You can also set a schedule for updating group membership.

The ‘out of bounds’ settings defined for the identity store also apply to membership update.

11. From the **When would you like to update the membership?** area, select when you want to update the group’s membership. Options are:

    - **Now**: to update the group membership as soon as you create the group.
    - **Update Later**: to update the group membership later. You can do so manually by right clicking the group in the groups list and clicking **Update**. You can also apply a Smart Group Update job to the group.

12. Use the **Schedule Job** area to link a Smart Group Update job with this group.

    A Smart Group Update job is runs on a set frequency (for example, daily, weekly, monthly) and at a specified time. When this job runs, it updates the group’s membership.

    Select one of the following options:

    - **Choose from existing jobs**: select this option button and then select a Smart Group Update job from the list to associate it with this Smart Group for membership update.

      The list contains all Smart Group Update jobs defined on your machine for the connected identity store.

    - **Create new job on this machine**: On selecting this option button, the **Smart Group Job** area gets enabled. Use it to create a new Smart Group Update job for the group’s membership update.

      Click the **Schedule** button to launch the **Create Job** dialog box (Figure 111), where you can create a new job.

      The **Job name** box displays the name of the Smart Group Update job. The **Start date** box displays *Monday, January 1, 0001* as the date, indicating that the job has never run before.

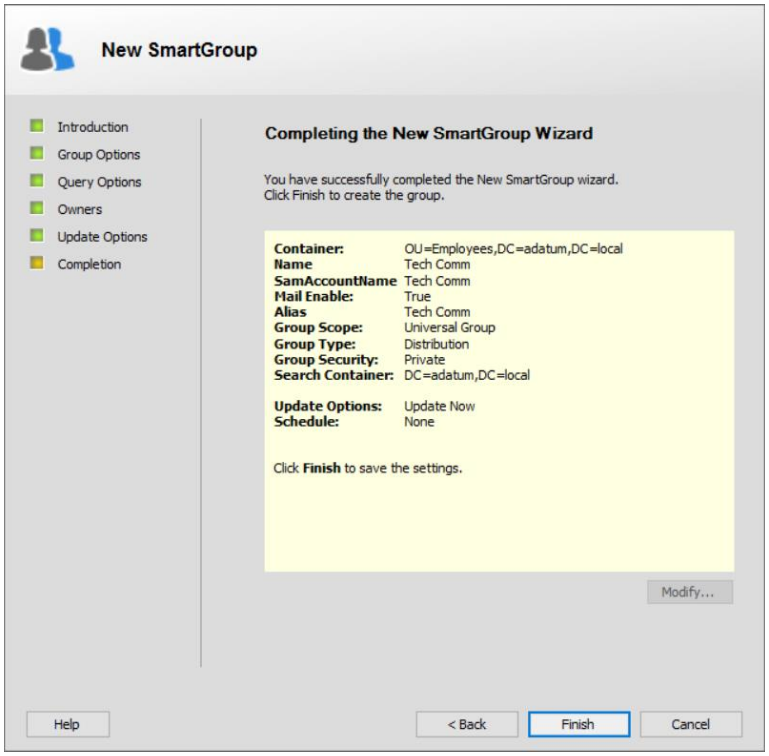
      The new job will also be listed under the **Smart Group Update** head on the **Scheduling** node in GroupID Management Console.

      NOTE To create a scheduled job, you must have the **Manage Scheduling** permission in the identity store.

    - **Choose Later**: to create the Smart Group without linking a Smart Group Update job with it. In this case, you will have to manually update the group membership.

NOTE If the GroupID administrator has enabled the ‘enforce job selection’ option in GroupID configurations, GroupID will not let you create this Smart Group unless you associate a Smart Group Update job with it. In this case, the **Choose Later** option will not be available.

13. Click **Next**.



Completing the New SmartGroup Wizard

You have successfully completed the New SmartGroup wizard.
Click Finish to create the group.

Container:	OU=Employees,DC=adatum,DC=local
Name	Tech Comm
SamAccountName	Tech Comm
Mail Enable:	True
Alias	Tech Comm
Group Scope:	Universal Group
Group Type:	Distribution
Group Security:	Private
Search Container:	DC=adatum,DC=local
Update Options:	Update Now
Schedule:	None

Click **Finish** to save the settings.

Figure 35: Completion page

On the Completion page, review the settings provided on the previous pages, using the **Back** button to access settings that you want to change.

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

15. When the group is created, the **Modify** and **Close** buttons get enabled.

- Click **Modify** to open the group properties.
- Click **Close** to close the **New Smart Group** wizard.

Chapter 5 - Group Properties

Group properties contains all settings associated with a group. Group properties vary by group type.

Modify a group's properties

Use the Group Properties dialog box to view and modify a group's properties.

1. In GroupID Management Console, select **Automate** > [required group node].
2. From the groups list, right-click the required group and select **Properties**. The **Group Properties** dialog box is displayed, with the **General** tab (Figure 36) in view.

A different set of tabs is available on the Properties dialog box for different kinds of groups.

- When you have an Azure identity store in GroupID that is synced with Active Directory using the AAD Sync schedule, then synced objects cannot be manipulated in the Azure identity store using GroupID.
- You cannot modify the properties of mail-enabled security groups (also called security-enabled distribution groups) in an Azure identity store.

Non-Mail-Enabled Static Group

- Group properties – General tab
- Group properties – Members tab
- Group properties – Member Of tab
- Group properties – Managed By tab
- Group properties – History tab

Mail-Enabled Static Group

- Group properties – General tab
- Group properties – Members tab

- Group properties – Member Of tab
- Group properties – Managed By tab
- Group properties – History tab
- Group properties – Exchange General tab
- Group properties – Email Addresses tab
- Group properties – Exchange Advanced tab

Non-Mail-Enabled Smart Group

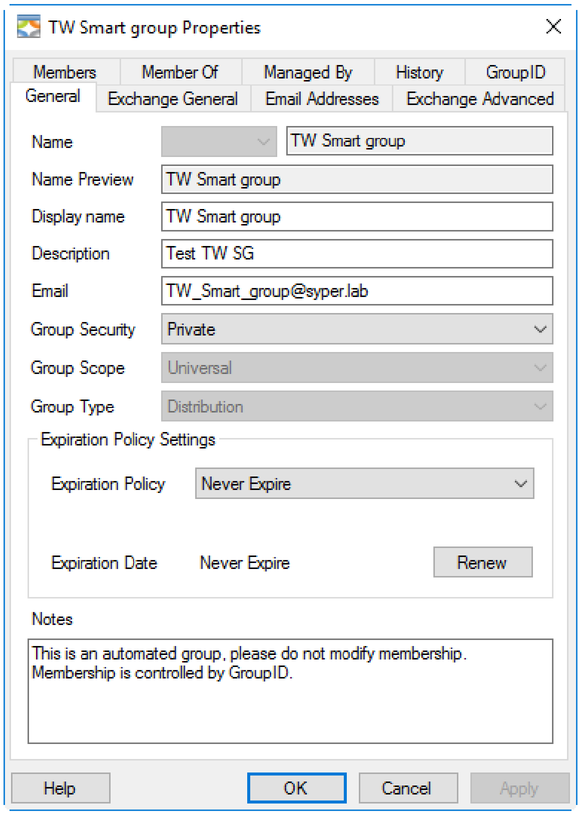
- Group properties – General tab
- Group properties – Members tab
- Group properties – Member Of tab
- Group properties – Managed By tab
- Group properties – History tab
- Group properties – GroupID tab

Mail-Enabled Smart Group

- Group properties – General tab
- Group properties – Members tab
- Group properties – Member Of tab
- Group properties – Managed By tab
- Group properties – History tab
- Group properties – Exchange General tab
- Group properties – Email Addresses tab
- Group properties – Exchange Advanced tab
- Group properties – GroupID tab

General tab

The **General** tab displays the general properties of the selected group, such as the group name, description, scope, type, security and other settings.



Name: TW Smart group
Name Preview: TW Smart group
Display name: TW Smart group
Description: Test TW SG
Email: TW_Smart_group@syper.lab
Group Security: Private
Group Scope: Universal
Group Type: Distribution

Expiration Policy Settings

Expiration Policy: Never Expire
Expiration Date: Never Expire

Notes

This is an automated group, please do not modify membership.
Membership is controlled by GroupID.

Figure 36: Group Properties dialog box - General tab

- The **Name** box displays the group's name. If prefixes are defined, a list appears for selecting a prefix for the group name.

  The prefixes list is available for static groups only. For Smart Groups and Dynasties, you cannot add or change the prefix here.

- The **Name Preview** box displays the complete name of the group with the prefix, if it is applied. See Group name prefixes on page 4.
- The **Display name** box displays the name by which this group is displayed in Automate.
- The **Description** box displays a user-provided description of the group.
- The **Email** box displays the email address of the group (for mail-enabled groups only).

- The **Group Security** list displays the group's security type. To change the security type, see Manage group access on page 74.
- The **Group Scope** list displays the group’s scope as domain local, global or universal.
- The **Group Type** list displays the group’s type as either a security group or a distribution list.

  NOTE The Group Scope and Group Type options are disabled for mail-enabled groups since it is not allowed to modify these in Exchange 2007 and later. For non mail-enabled groups, these options can be modified after group creation.

- The **Expiration Policy** list displays the expiry policy for this group. It specifies the duration the group remains active for, and expires when the period ends.

  If you select the *Other* option from the list, two boxes are displayed. First, select an option (Days, Months, or Years) from the second list. Then enter a value for the selected option in the first box. The group will remain active for the duration specified here.

  NOTE The **Expiration Policy** list is not available for Dynasty children since they inherit the expiry policy of their parents.

  For details about group expiry, see Expire groups on page 75.

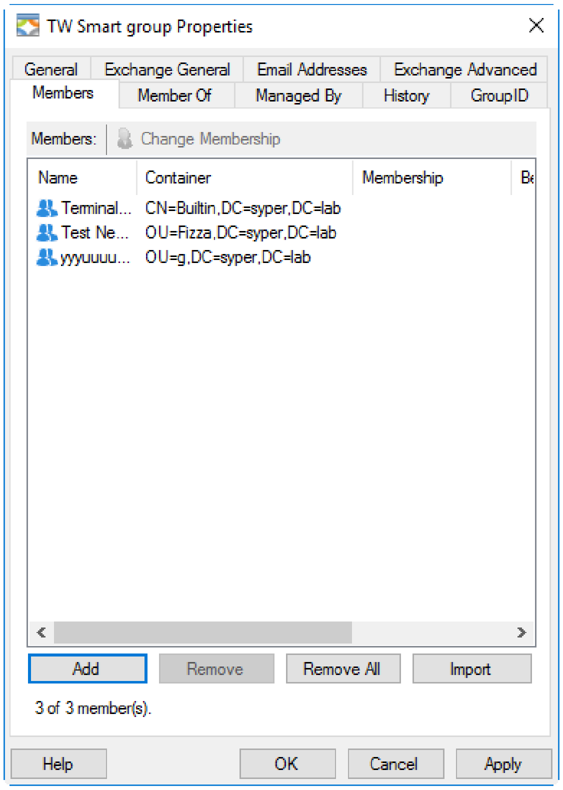
- **Expiration Date** displays the expiry date for the group.
- Use the **Renew** button to re-apply the selected expiry policy to the group, starting from the current date.

  Suppose the group's expiry policy is set to 30 days and the group expires in 2 days. Clicking this button would renew the expiry policy, with the 30-day countdown starting from the current date.

- Use the **Notes** box to type any notes for the group. If this group is a Smart Group or Dynasty, a reminder message will be included.

Members tab

Use this tab to view or modify the membership of a group.



Name	Container	Membership	Be
Terminal...	CN=Builtin,DC=syper,DC=lab		
Test Ne...	OU=Fizza,DC=syper,DC=lab		
yyyuuuu...	OU=g,DC=syper,DC=lab		

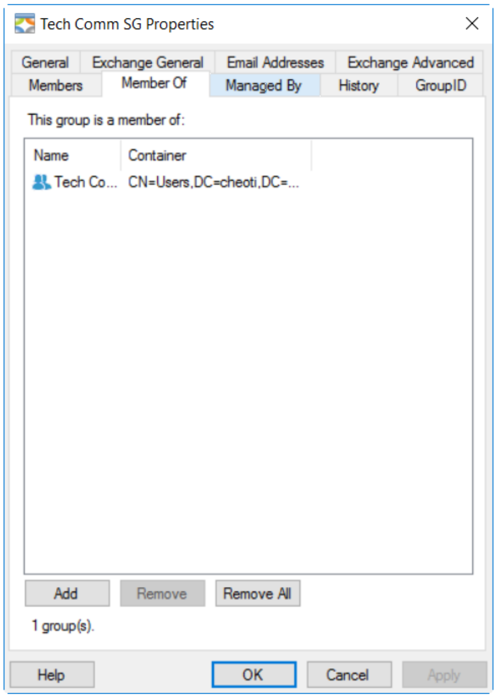
3 of 3 member(s).

Figure 37: Group Properties dialog box – Members tab

Group membership is discussed in detail in Chapter 7 - Group Memberships on page 89.

Member Of tab

Use the **Member Of** tab to view the groups that this group is a member of. You can add and remove this group from the membership of other groups.



This group is a member of:

Name	Container
Tech Co...	CN=Users,DC=cheoti,DC=...

1 group(s).

Figure 38: Group Properties dialog box – Member Of tab

- The **This group is a member of** area displays a list of all the groups this group is a member of.
- Use the **Add** button to add this group to the membership of another group.
- Use the **Remove** button to remove this group from the membership of the selected group.
- Use the **Remove All** button to remove this group from the memberships of all groups listed.

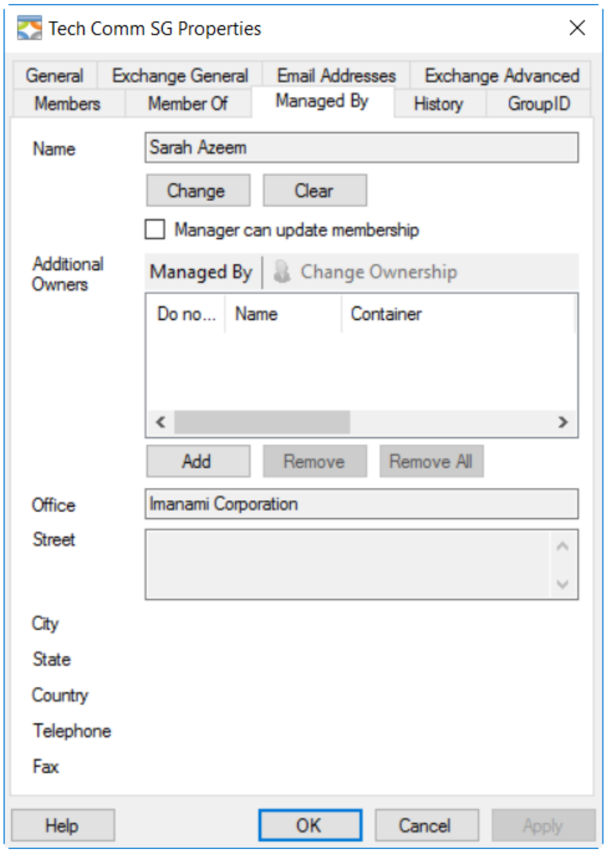
Managed By tab

Use the **Managed By** tab to view or modify the group's managers. The group's primary owner, additional owners, and Exchange additional owners are considered as the group's managers.

The group's primary and additional owners are defined on this tab; Exchange additional owners are defined on the **Exchange General** tab (Figure 41).

NOTE Only users, contacts and security groups can be set as the primary and additional owners of a group. Moreover, only mail-enabled users can be set as Exchange additional owners.

For groups in an Azure based identity store, only users can be set as primary owners. Moreover, Azure supports multiple primary owners for a group. Exchange additional owners are not supported.



Tech Comm SG Properties

Name: Sarah Azeem

☐ Manager can update membership

Office: Imanami Corporation

Figure 39: Group Properties dialog box – Managed By tab

For a group in a Microsoft Azure based identity store, this tab only displays the options to add and remove primary owners and additional owners.

Moreover, a group in an Azure based identity store must have a primary owner.

- The **Name** box displays the name of the group's primary owner, if the group has one.

  Use the **Clear** button to remove the primary owner. The group would have no primary owner if you do not select another owner.

  Use the **Change** button to specify or change the group's primary owner.

- The **Office** and **Street** boxes display the office and street address of the group's primary owner. You can also view the city, state and country the primary owner belongs to. Contact information includes the telephone and fax number of the primary owner.

- Select the **Manager can update membership** check box to enable the group owners (primary owner and Exchange additional owners) to update this group's membership directly on the directory server.

  For details, see Allow group owners to modify membership on the directory server on page 92.

- The **Additional Owners** area displays the additional owners for this group (if any).

  Click **Add** to specify a new additional owner for this group.

  Click **Remove** to remove the selected additional owner or **Remove All** to remove all additional owners.

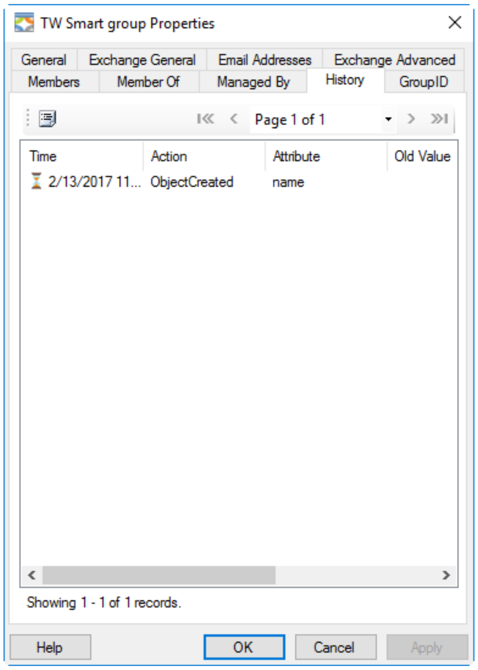
For detailed information on managing a group's owners, see Manage group owners on page 64.

History tab

The **History** tab displays a log of actions performed on the group, if history tracking is enabled for the identity store.

The actions to be tracked are also specified at the identity store level.

See Group history on page 84 for details about the logged actions and for adding notes to actions.



Time	Action	Attribute	Old Value
2/13/2017 11...	ObjectCreated	name	

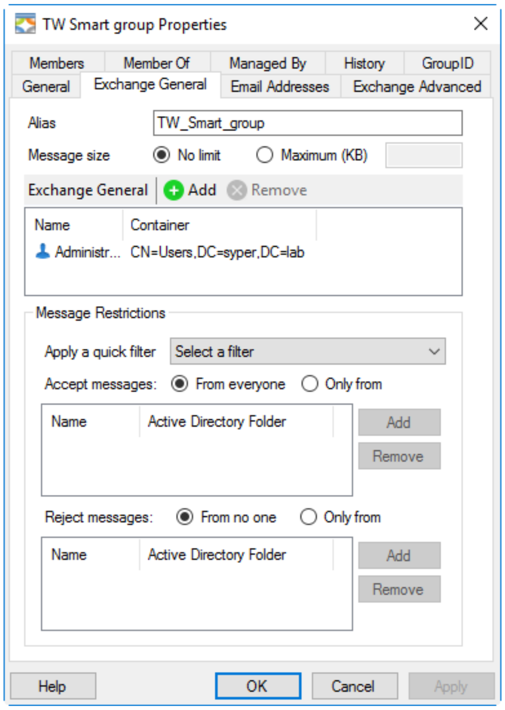
Showing 1 - 1 of 1 records.

Figure 40: Group Properties dialog box – History tab

Exchange General tab

Use the **Exchange General** tab to set message restrictions for a mail-enabled group. You can change the alias, limit the size of individual messages sent to the group, and restrict the group from receiving messages from certain recipients. This helps control email traffic for the group.

This tab is only available if you have configured Microsoft Exchange as the messaging provider for the connected identity store.



Alias: TW_Smart_group

Message size: ● No limit ○ Maximum (KB)

Exchange General

Name	Container
Administr...	CN=Users,DC=syper,DC=lab

Message Restrictions

Apply a quick filter: Select a filter

Accept messages: ● From everyone ○ Only from

Name	Active Directory Folder

Reject messages: ● From no one ○ Only from

Name	Active Directory Folder

Figure 41: Group Properties dialog box – Exchange General tab

- The **Alias** box displays the Exchange alias for this group. To change it, see Specify the Exchange alias for a group on page 108.
- The **Message size** setting specifies the size limit for the messages sent to this group. For details, see Apply size limit to incoming on page 105.
- Use the **Exchange General** area to set Microsoft Exchange additional owners for this group. Only mail-enabled users can be set as Exchange additional owners.

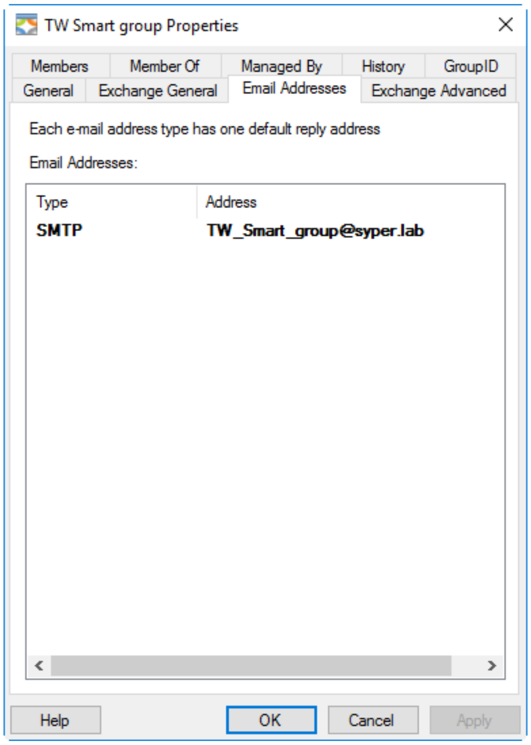
  For details, see Specify Exchange additional owners on page 69.
- Settings in the **Message Restrictions** section control who can and cannot send messages to this group. For details, see Restrict recipients for sending emails to a group on page 105.

- Use the **Accept messages** setting to specify the users and groups (mail-enabled only) who can send emails to this group.
  - **From everyone**: Indicates that everyone can send emails to this group.
  - **Only from**: Indicates that only the users and groups in this list can send emails to this group. Use the **Add** and **Remove** buttons to add or remove users and groups from this list.
- Use the **Reject messages** setting to specify the users and groups (mail-enabled only) who cannot send emails to this group.
  - **From no one**: Indicates that no email should be rejected.
  - **Only from**: Indicates that emails from the users and groups in the given list will be rejected. Use the **Add** and **Remove** buttons to add or remove users and groups from this list.

Email Addresses tab

In case of a mail-enabled group, Microsoft Exchange assigns different addresses to it for communication with different repositories (such as Address Book, SIP, Outlook). These addresses are displayed on the **Email Addresses** tab.

The **Email Addresses** tab is only available if you have configured Microsoft Exchange as the messaging provider for the connected identity store.



Each e-mail address type has one default reply address

Email Addresses:

Type	Address
SMTP	TW_Smart_group@syper.lab

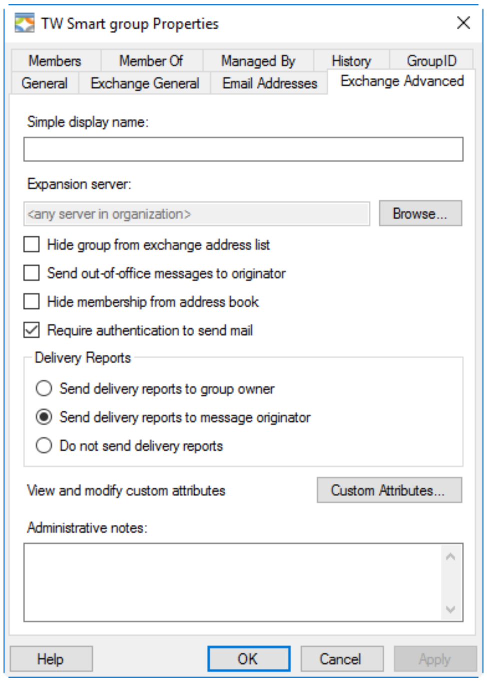
Figure 42: Group Properties dialog box – Email Addresses tab

Email addresses listed in the **Email Addresses** area can be of different types; for example, SMTP X400, and so on. You cannot add or remove addresses in the list.

Exchange Advanced tab

Use the **Exchange Advanced** tab to configure advanced Exchange settings. You can set the expansion server, hide the group in Exchange address lists, set recipients for non-delivery reports, specify custom Exchange attributes, and so on.

The **Exchange Advanced** tab is only available if you have configured Microsoft Exchange as the messaging provider for the connected identity store.



TW Smart group Properties

Simple display name:

Expansion server: <any server in organization>

□ Hide group from exchange address list

□ Send out-of-office messages to originator

□ Hide membership from address book

☑ Require authentication to send mail

Delivery Reports

○ Send delivery reports to group owner

● Send delivery reports to message originator

○ Do not send delivery reports

View and modify custom attributes

Administrative notes:

Figure 43: Group Properties dialog box – Exchange Advanced tab

- The **Simple display name** box displays the simple display name for this group, if any. This name is used by systems that cannot interpret all characters in a normal display name.
- By default, the Exchange Server specified as the messaging provider for the connected identity store acts as the expansion server. However, you can specify a different expansion server in the **Expansion server** box.

  To specify a different expansion server, see Select expansion server on page 109.
- Select the **Hide group from Exchange address list** check box to prevent the group’s email address from appearing in Exchange address lists, such as Global Address List (GAL).

See Hide a group in Exchange address lists on page 109 for details.

- Select the **Send out-of-office messages to originator** check box to send out-of-office (OOO) email notifications to the message originator (sender).

  See Set group to send ‘out-of-office’ messages on page 110 for details.
- Select the **Hide membership from address book** check box to hide the membership of mail-enabled groups in the Exchange address book (such as the Outlook address book).
- The **Require authentication to send mail** check box indicates whether to authenticate the users who send emails to the group. Selecting this check box blocks incoming emails from users on other domains or networks that cannot be authenticated on the domain where the group exists.
- In the **Delivery Reports** area, you can set non-delivery report (NDR) recipients when an email sent to this group is not delivered. The non-delivery report lets the recipient know that the email was not delivered.

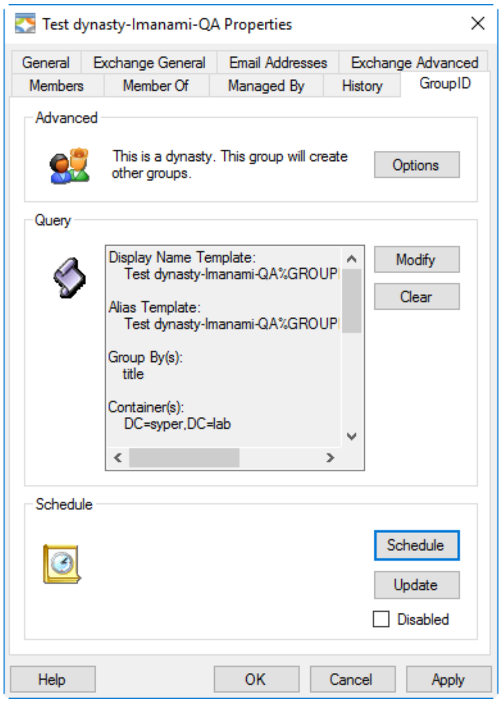
  See Set recipient for non-delivery reports on page 111 for details.
- Click **Custom Attributes** to launch the **Exchange Custom Attributes** dialog box so you can view and modify the values of custom Exchange attributes.

  See Assign values to custom attributes of a group on page 112 for details.
- In the **Administrative notes** box, view and enter useful information about the group.

GroupID tab

The **GroupID** tab is only available for Smart Groups and Dynasties. Use it to view the query you have defined to update group membership and details of the Smart Group Update job associated with the group for scheduled membership update.

The tab is organized into three sections: **Advanced**, **Query**, and **Schedule**.



This is a dynasty. This group will create other groups.

```
Display Name Template:
   Test dynasty-Imanami-QA%GROUP

Alias Template:
   Test dynasty-Imanami-QA%GROUP

Group By(s):
   title

Container(s):
   DC=syper,DC=lab
```

☐ Disabled

Figure 44: Group Properties dialog box – GroupID tab

- The **Advanced** area is available for Dynasties of the parent and middle level. Click **Options** to launch the **Dynasty Options** dialog box, where you can modify the Dynasty options.

  See Dynasty options on page 131 for details.

- The **Query** area displays the query used to update group membership.

  Click **Modify** to launch the Query Designer dialog box, where you can change the query.

  Click **Clear** to clear the query and downgrade this group to a normal, static group.

- The **Schedule** area displays the date and time when the group was last updated, as well as the machine name that performed the update.

  Click **Update** to manually update the group.

  Click **Schedule** to create/modify a Smart Group Update job that updates the group. See Update Smart Groups and Dynasties using a scheduled job on page 62 for details.

- Select the **Disable** check box to disable membership updates to the group, either by a scheduled job or using the **Update** command.

Chapter 6 - Managing Groups

Automate provides comprehensive options to manage directory groups. Using these options, you can:

- Update Smart Groups and Dynasties: Use different methods to update the membership of Smart Groups and Dynasties.
- Move groups to a different container.
- Manage group owners: Manage a group’s primary owner, additional owners, and Exchange additional owners.
- Transfer group ownership: Assign owners to orphan groups and transfer group ownership.
- Manage group access.
- Expire groups: Learn about different ways to expire groups manually and automatically.
- Renew expired groups.
- Group Deletion: explains how groups are deleted in Automate and how a deleted group can be restored.
- Group history: provides information on viewing a group's history.

Update Smart Groups and Dynasties

When a Smart Group or Dynasty is updated, it involves the following:

- Each Smart Group and Dynasty has a query, such as an LDAP query, defined for it. On update, the query retrieves records from the directory and group membership is updated with these records.

  Whatever the records returned by the query, the membership of an Office 365 group is updated with user objects only.

- The values of certain attribute(s) can be updated.
  - For a Smart Group, for example, the value of the managedBy attribute is updated for nested groups. See Membership settings on page 89 for information on nested groups.

- For Dynasties, the administrator can specify certain attributes at the identity store level, whose values are passed on from parent to child Dynasties. These attributes' values are updated for child Dynasties on update, depending on the inheritance option set for each Dynasty.

Automate provides different methods to update Smart Groups and Dynasties, namely:

- Manual update
- Scheduled update

In both methods, the query defined for the group is executed to update membership; the difference being that in manual update, you can execute the query manually any time while scheduled updates run automatically at a specified frequency.

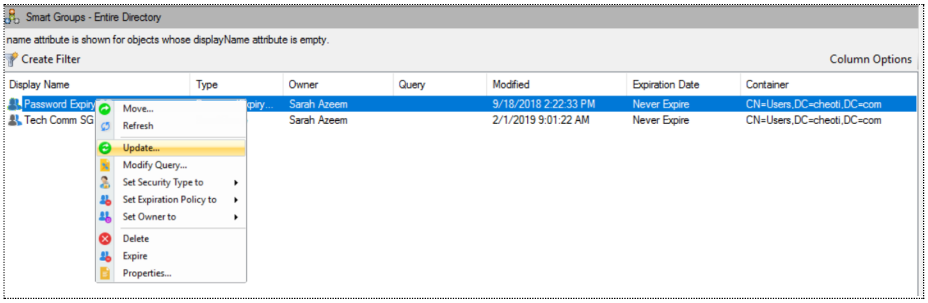
The 'out of bounds' settings defined for an identity store also impact the group membership update process.

Update Smart Groups and Dynasties using the Update command

You can manually update a Smart Group any time by right-clicking the group and clicking **Update** on the shortcut menu. This executes the query defined for the group and updates its membership

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, select one or more groups. These should be Smart Groups or Dynasties or both.

   To select multiple groups, hold down the **CTRL** key and select individual groups or hold down the **SHIFT** key and select a range of groups.
3. Right-click the selection and select **Update**.



Smart Groups - Entire Directory

name attribute is shown for objects whose displayName attribute is empty.

Display Name	Type	Owner	Query	Modified	Expiration Date	Container
Password Expiry	piry...	Sarah Azeem		9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech Comm SG		Sarah Azeem		2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com

Figure 45: Update command on the shortcut menu

If the selection includes expired groups, Automate skips them while updating.

4. When the update is complete, click **OK**.

Update Smart Groups and Dynasties using a scheduled job

GroupID provides a scheduled update feature to keep the memberships of Smart Groups and Dynasties current, and to update values of certain attributes. You can define scheduled jobs for Smart Group Update and apply them to Smart Groups and Dynasties. The Task Scheduler keep checking scheduled jobs and initiating scheduled job runs.

You can associate a Smart Group Update job with a group in any of the following ways:

- Method 1: In Automate, select a group and associate a Smart Group Update job with it.
- Method 2: In the Scheduling node, open a Smart Group Update job and add the required group to its targets list.

Method 1: Associate a Smart Group Update job with a group

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, right-click the required Smart Group or Dynasty and select **Properties**.
3. On the **GroupID** tab (Figure 44), click **Schedule**.
   - If no Smart Group Update job is associated with the group, the **Create Job** dialog box (Figure 111) is displayed, where you can create a new Smart Group Update job.
   - If a Smart Group Update job is already associated with the group, the **Edit Job** dialog box is displayed, where you can edit job details.

   In either case, the associated job runs according to the schedule you specify for it and updates the target group.
4. Click **OK** to close the Properties dialog box.

Method 2: Add a group to the targets list of a Smart Group Update job

1. In GroupID Management Console, select the **Scheduling** node.
2. Expand the **Smart Group Update** head and select an existing job or create a new job.
3. On the **Create Job** dialog box (Figure 111) or **Edit Job** dialog box, add the

required group to the job's **Targets** list.

4. Add/edit the required information and click **OK**.

When the job runs, it updates the membership of all target groups on the basis of each group's respective query. It also updates the required attributes' values.

Disable updates to a group

You can disable updates, either by a scheduled job or using the **Update** command, for a Smart Group or Dynasty.

In this way, you can suspend updates to a group for an indefinite period and resume them when needed.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, right-click the required Smart Group or Dynasty and select **Properties**.
3. On the **GroupID** tab (Figure 44), select the **Disabled** check box to disable updates for the group.

   Clear the **Disabled** check box to enable updates.
4. Click **OK**.

You can also define, edit, disable and delete a Smart Group Update job using the **Scheduling** node in GroupID Management Console.

Move groups to a different container

You can move one or more groups to another container or domain in the connected identity store.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, select one or more groups.
   - To select consecutive groups, click the first group in the list, press and hold down the **SHIFT** key and then click the last group.
   - To select non-consecutive groups, press and hold down the **CTRL** key and then click each group that you want to select.
3. Right-click the selection and click **Move** on the shortcut menu.
   The **Select Container** dialog box (Figure 108) is displayed.
4. Select the domain or container you want to move the group(s) to, and click

OK.

5. When the process is complete, click **OK** on the **Move Group** dialog box.

Manage group owners

When a new group is created; by default, the group creator is set as its primary owner. However, you can change the primary owner or even remove it, leaving the group orphan.

NOTE You cannot remove a group's primary owner if the Owners policy for your role does not allow it. See **Group Owners** policy in Role policies.

Additional owners

You can also specify temporary and permanent additional owners for a group. These can be users, contacts and even security groups. In case of a group, all its members will be considered as additional owners.

You can change the ownership type of an additional owner from temporary to permanent and vice versa.

Additional owners have the same privileges as the primary owner to manage the group. Group expiry, deletion, and renewal notifications are sent to the additional owners along with the primary owner. However, you can exclude some or all additional owners from receiving email notifications.

By default, there is no restriction on the number of additional owners a group can have. However, if the administrator has specified a maximum and minimum value for additional owners in the **Group Owners** policy for your role in the identity store, you cannot create a group or save modifications to it unless it has the specified number of additional owners.

Exchange 2010/2013/2016/2019 additional owners

Microsoft Exchange 2010/2013/2016/2019 offers the co-managed by feature that enables you to specify Exchange additional owners for a group, provided that Exchange 2010/2013/2016/2019 is configured as the messaging provider for the identity store. Exchange additional owners are stored in the msExchangecoManagedby attribute.

Automate sends group expiry, deletion, and renewal notifications to all Exchange additional owners along with the group's primary owner and additional owners.

NOTE For email notifications to be sent, an SMTP server must be configured for the identity store.

Only users, contacts and security groups can be set as the primary and additional owners of a group. Moreover, only mail-enabled users can be set as Exchange additional owners.

Note the following for a Microsoft Azure based identity store:

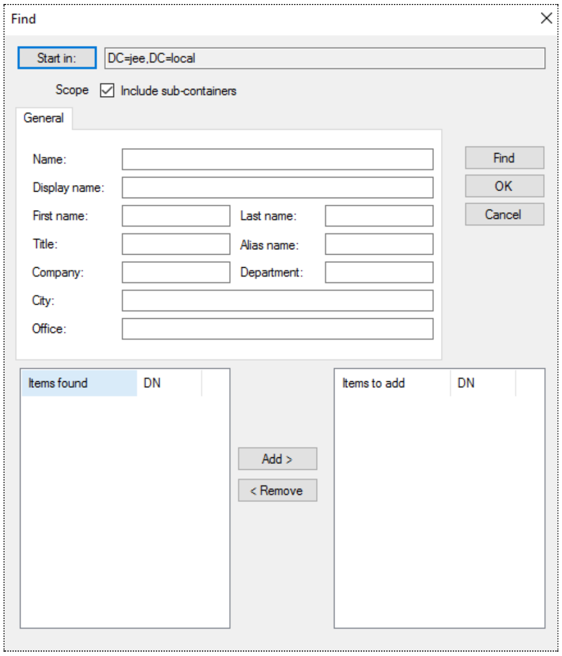
- Only users can be set as primary owners.
- Azure supports multiple primary owners for a group.
- At least one primary owner is mandatory.
- Exchange additional owners are not supported.

Change the primary owner for a group

When a new group is created, the group creator is set as its primary owner. However, you can change the primary owner.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Managed By** tab (Figure 39), the **Name** box displays the name of the group's primary owner.

   To change the primary owner, click **Change**; the **Find** dialog box is displayed, where you can locate and select the recipient to set as the group's primary owner.


Start in: DC=jee,DC=local

Scope ☑ Include sub-containers

Figure 46: Find dialog box

Enter a criterion and click **Find** to return the results; then add the required objects from the **Items found list** to the **Items to add** list.

- Click **Start in** to select the top level container to start the search in.

  If the administrator has applied a search policy at the identity store level to restrict the search scope to a container, the container name is displayed here and you cannot change it.

- Select the **Include sub-containers** check box to expand the search scope to sub-containers in the selected container.

- The **General** area lists the general attributes for searching an object. All these fields are optional. However, the more fields you specify a value for, the more specific your search.

  You can search an object by its name, display name, first name, last name, title, alias, company, department, city, and office

- Click **Find** button to return the search results.
  The **Items found** box lists all objects that match your search criteria.

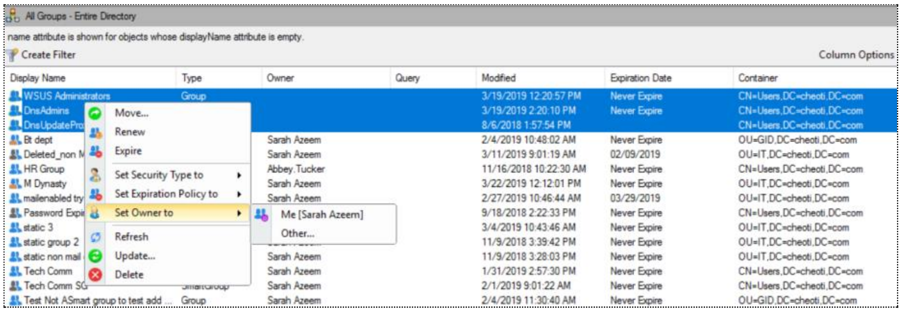
- Select your required object(s) and click add to move them to the **Items to add** box.
  To remove an object from the **Items to add** box, select it and click **Remove**.

- Click **OK** to close the **Find** dialog box.

4. The object selected on the **Find** dialog box is displayed in the **Name** box on the **Managed By** tab. Click **OK**.

Change the primary owner for multiple groups

1. In GroupID Management Console, select **Automate > [required group node]**.
2. Select one or more groups in the groups list.
   - To select consecutive groups, click the first group in the list, press and hold down the **SHIFT** key and then click the last group.
   - To select non-consecutive groups, press and hold down the **CTRL** key and then click each group that you want to select.
3. Right-click the selected groups, point to **Set Owner** and select one of the following options:



All Groups - Entire Directory

name attribute is shown for objects whose displayName attribute is empty.

Display Name	Type	Owner	Query	Modified	Expiration Date	Container
WSUS Administrators	Group			3/19/2019 12:20:57 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsAdmins				3/19/2019 2:20:10 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsUpdatePro				8/6/2018 1:57:54 PM		CN=Users,DC=cheoti,DC=com
Bt dept		Sarah Azeem		2/4/2019 10:48:02 AM	Never Expire	OU=GID,DC=cheoti,DC=com
Deleted_non M		Sarah Azeem		3/11/2019 9:01:19 AM	02/09/2019	OU=IT,DC=cheoti,DC=com
HR Group		Abbey.Tucker		11/16/2018 10:22:30 AM	Never Expire	CN=Users,DC=cheoti,DC=com
M Dynasty		Sarah Azeem		3/22/2019 12:12:01 PM	Never Expire	OU=IT,DC=cheoti,DC=com
mailenabled try		Sarah Azeem		2/27/2019 10:46:44 AM	03/29/2019	OU=IT,DC=cheoti,DC=com
Password Expi				9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
static 3				3/4/2019 10:43:46 AM	Never Expire	OU=IT,DC=cheoti,DC=com
static group 2				11/9/2018 3:39:42 PM	Never Expire	OU=IT,DC=cheoti,DC=com
static non mail		Sarah Azeem		11/9/2018 3:28:03 PM	Never Expire	OU=IT,DC=cheoti,DC=com
Tech Comm		Sarah Azeem		1/31/2019 2:57:30 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech Comm SG	SmartGroup	Sarah Azeem		2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com
Test Not ASmart group to test add ...	Group	Sarah Azeem		2/4/2019 11:30:40 AM	Never Expire	OU=GID,DC=cheoti,DC=com

Figure 47: Set Owner options

- **Me [your logged-on user name]**, to set yourself as the primary owner for the selected groups.
- **[Most recently used recipient set as primary owner (if any)]**, to set this recipient as the primary owner for the selected groups.
- **Other...**, to select a different recipient as the primary owner. Clicking this option displays the **Set Owner** dialog box where you can locate and select the required recipient.

Set primary owners for an Azure group

Using GroupID, you can specify multiple primary owners for groups in an Azure based identity store.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
   On the **Managed By** tab (Figure 39), the **Owners** area is for specifying the group’s primary owners.
3. Click **Add**. On the **Find** dialog box (Figure 46), locate and select the recipients to set as the group's primary owners, and click **OK**.

   These recipients can be user objects only.

   - To remove an owner, select it and click **Remove**.
   - To remove all primary owners, click **Remove All**.
     However, you must add at least one primary owner; else, you would not be able to save the information.
4. Click **OK** to close the group properties dialog box.

Set additional owners for a group

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Managed By** tab (Figure 39), the **Additional Owners** area is for specifying the group’s additional owners.

   - To specify additional owner(s), click **Add**. The **Find** dialog box (Figure 46) is displayed. Locate and select the recipients to set as the group's additional owners. These can be users, contacts and even groups. In case of a group, all its members will be considered as additional owners. Like primary owners, additional owners have full rights to manage the group.
   - By default; all expiry, deletion and renewal notifications for the group are sent to all additional owners (in addition to the primary owner) and they can take the necessary actions accordingly.

     However, to exclude an additional owner from receiving email notifications, select the **Do not Notify** check box for it.

   NOTE When a Smart Group Update job runs on a group, the notification behavior is as follows:

     - If the **Do not Notify** check box is selected for an additional owner but its email address is specified in the **To** box on the **Notification** tab (Figure 115) of the **Create/Edit Job** dialog box, the additional owner will receive the notifications.
     - If the **Do not Notify** check box is selected for an additional owner but the **Send Report to group owner(s)** check box is selected on the **Notification** tab (Figure 115) of the **Create/Edit Job** dialog box, the additional owner will not receive the notifications.

   - To remove an additional owner, select it and click **Remove**.
   - To remove all additional owners, click **Remove All**.
4. Click **OK** to close the group properties dialog box.

   You may observe a message that the group does not adhere to a requirement for additional owner. It occurs because the Group Owners policy defined for your role at the identity store level requires that the group must have at least x number of additional owners.

   Specify the required number of additional owners and then click **OK**.

Change an additional owner's ownership type

Ownership type indicates whether an object is a temporary or permanent additional owner of a group. The Managed By Life Cycle job updates the temporary ownership of groups by adding and removing temporary additional owners on the specified dates.

Consider a scenario where the Managed By Life Cycle job is scheduled to run once a week, say Mondays. If an object is to be added as a group's temporary additional owner for three days - Wednesday till Friday, it will not be added. This happens because the Managed By Life Cycle job did not run on the particular days for temporary ownership update.

Make sure that the Managed By Life Cycle job is scheduled to run at a frequency that meets your temporary ownership requirements.

To change ownership type:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Managed By** tab (Figure 39), select an additional owner and click **Change Ownership**.
4. On the **Ownership Type** dialog box (Figure 27), select an option from the **Ownership Type** list to specify the additional owner's ownership type. See Table 3 for the available options.
5. Click **OK** to close the **Ownership Type** dialog box.
6. Click **OK** to close group properties.

Specify Exchange additional owners

If Exchange Server 2010/2013/2016/2019 is configured as the messaging provider for the connected identity store, you can specify Exchange additional owners for a group. Only mail-enabled users can be designated as Exchange additional owners.

Automate sends group expiry, deletion, and renewal notifications to these owners along with the group's primary and additional owners.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange General** tab (Figure 41), click **Add** in the **Exchange General** area. The **Find** dialog box (Figure 46) is displayed, where you can locate and select the recipient to set as an Exchange additional owner for the group.

4. You can also remove an Exchange additional owner by selecting it and clicking **Remove**.
5. Click **OK**.

Transfer group ownership

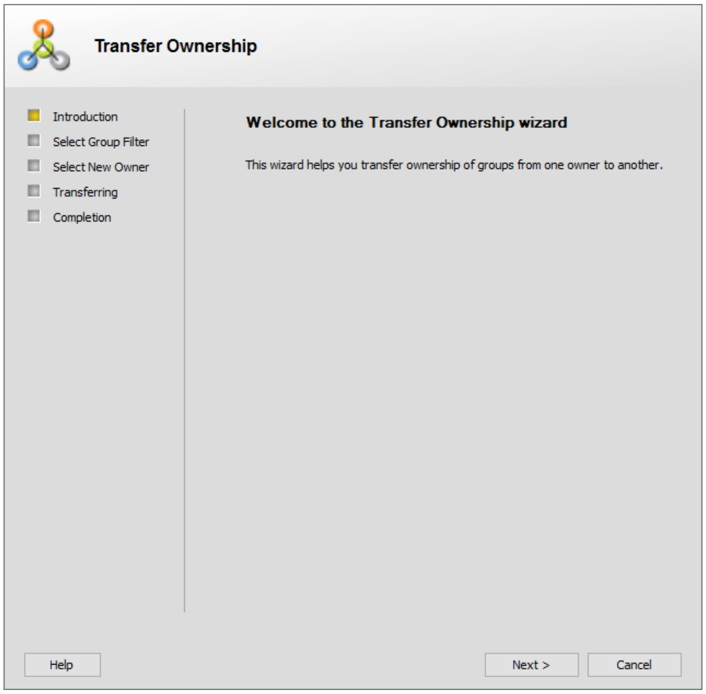
The **Transfer Ownership** wizard in Automate provides a convenient way to:

- assign ownership to orphan groups in the connected identity store, and
- transfer primary and additional group ownerships (including Exchange 2010/2013/2016/2019 additional ownerships) from one recipient to another.

Depending on the number of groups and the amount of available bandwidth between GroupID and the messaging provider server (such as Exchange Server) or directory server, this process may take several minutes.

1. In GroupID Management Console, select **Automate**, right-click **All Groups** and select **Transfer Ownership Wizard**.

   The wizard opens to the **Welcome** page.

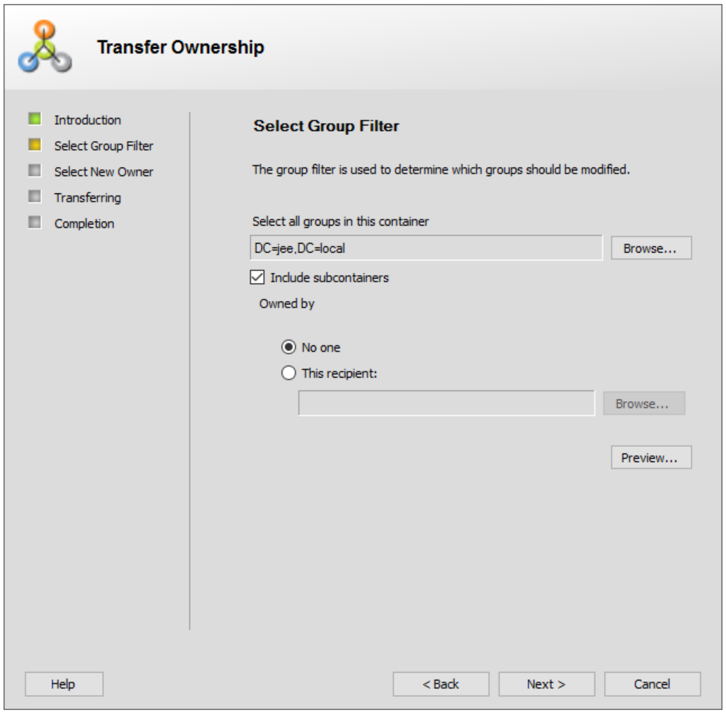


Welcome to the Transfer Ownership wizard

This wizard helps you transfer ownership of groups from one owner to another.

Figure 48: Welcome page

2. Read the welcome message and click **Next**.
   The **Select Group Filter** page is displayed.



Transfer Ownership

Select Group Filter

The group filter is used to determine which groups should be modified.

Select all groups in this container: DC=jee,DC=local

☑ Include subcontainers

Owned by

● No one

○ This recipient:

Figure 49: Select Group Filter page

Use this page to set the criteria for filtering groups that have to be transferred to a new owner.

3. The **Select all groups in this container** box displays the distinguished name of the container that the wizard searches for the groups to transfer their ownership. The default selection is the domain of the connected identity store.

   Click **Browse** and select a different organizational unit, domain, or the entire directory.

   Your selection determines where the wizard searches for the groups to transfer their ownership. The smaller the selection, the less time it takes to carry out the transfer.

4. Specify whether to search for groups in sub-containers by selecting or clearing the **Include sub-containers** check box.

   The scope of this setting varies, depending on the container you selected in the previous step. The following table explains the actual structures searched when you select the **Include sub-containers** option:

Selected Container	Selecting Include sub-containers
Organizational Unit	Includes the sub-organizational units in the search for required groups.

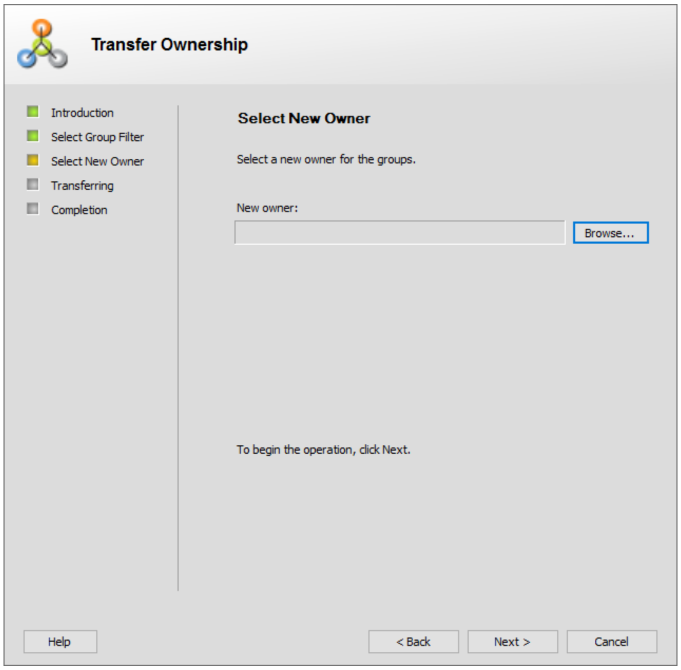
Domain	Includes all organizational units and their sub-trees in the search for required groups.
Entire Directory	Searches the entire identity store; the **Include sub-containers** setting has no effect.

Table 4: Impact of the Include sub-containers option

For Active Directory, if the search container is set to Global Catalog and ExtensionData is not replicated to the Global Catalog, additional ownership of the groups will not be transferred.

5. In the **Owned by** area, specify whether to select groups having no owner or groups having a specific owner for transferring ownership.
   - **No one** –to change the ownership of groups having no owner.
   - **This recipient** – to change the ownership of groups managed by a recipient. This option includes all groups for which the recipient is the primary owner, additional owner, or Exchange 2010/2013/2016/2019 additional owner.

     After selecting this option, click **Browse** and use the **Find** dialog box (Figure 46) to select the required recipient.
6. Click the **Preview** button to view the list of groups that match the given criteria for ownership transfer.
7. Click **Next**.
   The **Select New Owner** page is displayed.



Select New Owner

Select a new owner for the groups.

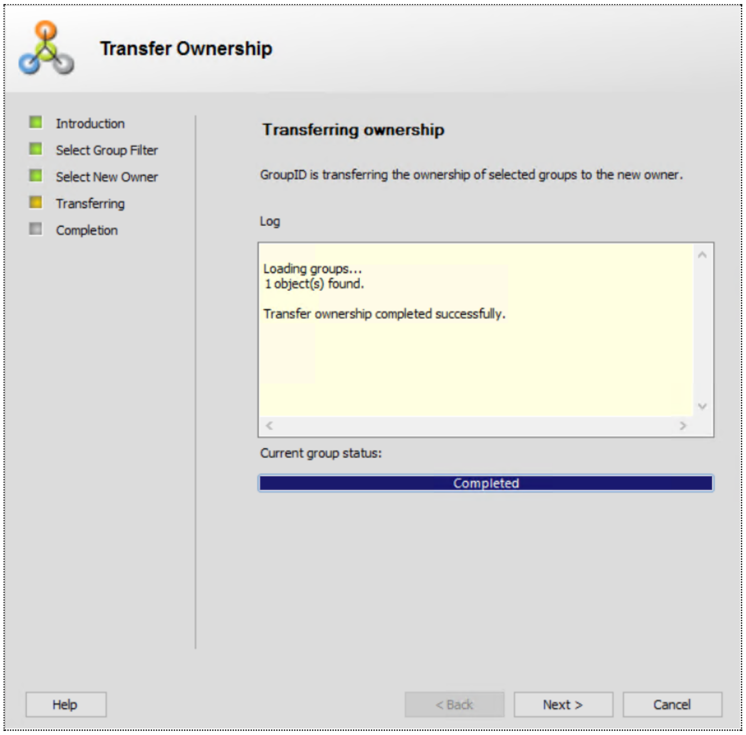
New owner:

To begin the operation, click Next.

Figure 50: Select New Owner page

8. Click **Browse** to select a new owner for the group(s).
   You can only select a contact, user, or a security group as an owner.

9. Click **Next**.
   The **Transferring ownership** page is displayed:



Transferring ownership

GroupID is transferring the ownership of selected groups to the new owner.

Log

```
Loading groups...
 1 object(s) found.

Transfer ownership completed successfully.
```

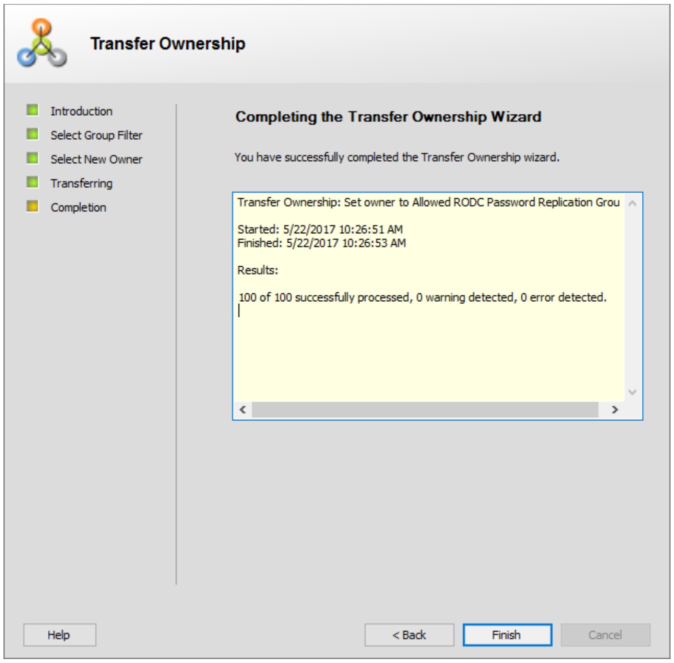
Current group status:

Completed

Figure 51: Transferring Ownership page

The **Transferring ownership** page displays the transfer progress while it transfers the ownership of each group to the new owner.

10. Click **Next**.
    The **Completion** page is displayed:



Transfer Ownership

Completing the Transfer Ownership Wizard

You have successfully completed the Transfer Ownership wizard.

```
Transfer Ownership: Set owner to Allowed RODC Password Replication Grou

Started: 5/22/2017 10:26:51 AM
Finished: 5/22/2017 10:26:53 AM

Results:

100 of 100 successfully processed, 0 warning detected, 0 error detected.
```

Figure 52: Completion page

This page displays the distinguished names of all groups that have been successfully processed and transferred to the new owner. It also displays any errors that were encountered during the process.

11. Click **Finish** to close the wizard.

Manage group access

A group’s security type determines how non-members can access the group and become its members. GroupID provides three security types:

- **Private** - to restrict access to the group to members selected by the group owner. Only the owner can add or remove members from the group. Requests to join or leave the group cannot be submitted.
- **Semi-Private** - to restrict access to the group to members selected by the group owner. However, requests to join or leave the group can be sent to the owner.
- **Public** - to allow all users to access the group. Users can join or leave the group at will and do not require any permissions to do so.

A security type is assigned to the group when it is created. However, you can change it later, if required.

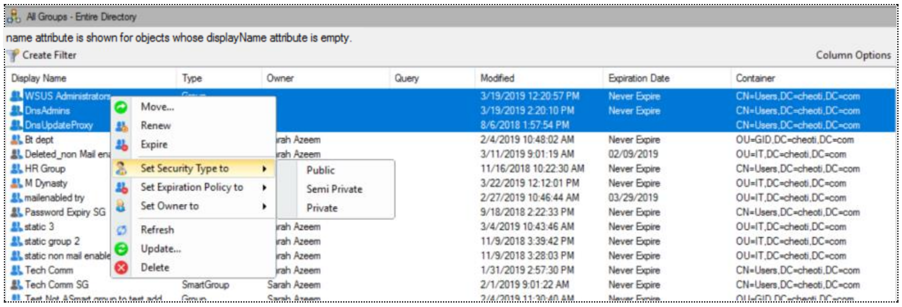
NOTE The group security option is available with a GroupID Self-Service license.

Change the security type for a group

1. In GroupID Management Console, select **Automate > [required group node].**
2. From the groups list, right-click the required group and select **Properties**.
3. On the **General** tab (Figure 36) of the group properties dialog box, select a different security type from the **Group Security** list and click **Apply**.
4. Click **OK**.

Change the security type for multiple groups

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, select one or more groups.
3. Right-click the selected groups, point to **Set Security Type to** and click the required security type.



name attribute is shown for objects whose displayName attribute is empty.

Display Name	Type	Owner	Query	Modified	Expiration Date	Container
WSUS Administrators	Group			3/19/2019 12:20:57 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsAdmins				3/19/2019 2:20:10 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsUpdateProxy				8/6/2018 1:57:54 PM		CN=Users,DC=cheoti,DC=com
Bt dept		rah Azeem		2/4/2019 10:48:02 AM	Never Expire	OU=GID,DC=cheoti,DC=com
Deleted_non Mail ena		rah Azeem		3/11/2019 9:01:19 AM	02/09/2019	OU=IT,DC=cheoti,DC=com
HR Group				11/16/2018 10:22:30 AM	Never Expire	CN=Users,DC=cheoti,DC=com
M Dynasty				3/22/2019 12:12:01 PM	Never Expire	OU=IT,DC=cheoti,DC=com
mailenabled try				2/27/2019 10:46:44 AM	03/29/2019	OU=IT,DC=cheoti,DC=com
Password Expiry SG				9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
static 3		rah Azeem		3/4/2019 10:43:46 AM	Never Expire	OU=IT,DC=cheoti,DC=com
static group 2		rah Azeem		11/9/2018 3:39:42 PM	Never Expire	OU=IT,DC=cheoti,DC=com
static non mail enable		rah Azeem		11/9/2018 3:28:03 PM	Never Expire	OU=IT,DC=cheoti,DC=com
Tech Comm		rah Azeem		1/31/2019 2:57:30 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech Comm SG	SmartGroup	Sarah Azeem		2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com
Test Not ASmart group to test add	Group	Sarah Azeem		2/4/2019 11:30:40 AM	Never Expire	OU=GID,DC=cheoti,DC=com

Figure 53: Set Security Type To options

Expire groups

Automate provides two ways to expire a group:

- Use the Expire command on the Actions menu or shortcut menu to expire a group manually.
- The Group Life Cycle job expires groups automatically based on the expiry policy specified for each group.

The expiry policy for a group specifies the period for which the group remains active. At the end of the period, the group expires.

The following events take place when a group expires:

- The group becomes inactive and is locked for all activities.
- "EXPIRED_" is added as a prefix to the group name.
- A mail-enabled distribution group is mail-disabled, which means that any emails sent to the group are bounced back with an expiry message.

  When you expire an Office 365 group using GroupID, its member list is backed up in the database and cleared from Office 365.

- For a security group, its member list is cleared and any permissions set for that group no longer apply. However, GroupID keeps a backup of its membership in the database.

In case of an Active Directory identity store with Office 365 as messaging provider:

In case of an Active Directory identity store with Office 365 as the messaging provider, the following happens when a distribution group is expired manually or via the Group Life Cycle job:

- The group’s email address is removed in Active Directory.
- "EXPIRED_" is added as a prefix to the group name.
- The group is removed from Office 365 when the AAD Sync schedule runs.

On renewing an expired distribution group, the following happens:

- The group’s email address is added in Active Directory.
- The "EXPIRED_" prefix is removed from the group’s name.
- The group is created with members in Office 365 when the AAD Sync schedule runs.

In case of an Azure AD identity store with Office 365 as messaging provider:

In case of an Azure AD identity store with Office 365 as the messaging provider, the following happens when a distribution group is expired manually or via the Group Life Cycle job:

- GroupID takes a backup of the group’s membership.
- It empties out the group’s membership in Office 365.

On renewing an expired distribution group, the following happens:

- The group’s membership is repopulated in Azure AD and Office 365.

Automate moves expired groups to the **Expired Groups** node. To make an expired group active again, you can renew it. See Renew expired groups on page 81.

Group Life Cycle policy

All settings related to group expiry are specified in the Group Lifecycle policy. This policy is defined at the identity store level and controls the following:

- The default expiry policy for groups
  This policy specifies the period for which a group remains active. When the period ends, the group expires.

  Groups with a 'Never Expire' policy are not expired by the Group Lifecycle job.
- Wait period for deleting expired groups
  The administrator can specify X number of days after which an expired group would be deleted, starting from the expiry date. This also applies to manually expired groups.
- Security groups expiry
  If the administrator has enabled the security groups expiry option, you will be able to expire security groups; else security groups cannot be expired manually or by the Group Life Cycle job.

  This feature also applies to Office 365 groups in an Azure based identity store.
- Filter groups for expiration and deletion
  By default, the Group Life Cycle job processes all groups in the identity store. However, the administrator can filter organizational units to include or exclude from the job.
- Group usage lifecycle
  The administrator can set the expiry of mail-enabled distribution groups based on their usage.

  If an expiring group is used in the last X number of days, it will be renewed by reapplying the expiry policy to it. However, if a group in not used in the last X number of days, its life will be reduced to 7 days.
- Enable group attestation
  The administrator can enforce group owners to review and validate the attributes and membership of an expiring group before renewing it. Group owners must use the Self-Service portal for group attestation.

- Notifications for expiring groups
  The administrator can specify whether to send notifications 1 day, 7 days, or 30 days before the group expires, to inform the group owners (or the default approver if the group has no primary or additional owners) about the approaching expiry.

  If no option is selected for expiry notifications, no notifications will be sent. In this case, the Group Life Cycle job expires the group without notifying anyone.
- Set default approver for notifications
  The administrator can designate a recipient as the default approver for group expiry notifications.
  .
  By default, group expiry notifications are addressed to the group's owners. For groups without owners, the notification is sent to the default approver.

  If notifications are enabled but no notification recipient is available, the job does not expire the group.

Of these, only the first setting, i.e., the group expiry policy, can be changed for individual groups. The remaining settings apply to all groups in the identity store and cannot be changed for individual groups.

The Group Life Cycle job executes the Group Lifecycle policy as defined for the identity store, but monitors group expiry dates as determined by each group's expiry policy.

The administrator may choose to apply the group expiry policy on the Azure portal rather than GroupID's Group Life Cycle policy. See Group expiration policy in Appendix B for more info.

Group Expiry Notifications

The Group Lifecycle job monitors the expiry policy of all groups. When a group approaches its expiry, the job does the following:

- When notifications are not enabled, the Group Life Cycle job expires the group without notifying anyone.
- When notifications are enabled in the Group Life Cycle policy, the job notifies the primary and additional owners or the default approver (in case no owner is set for the group) about the approaching expiry.

  In case the notification could not be sent or no recipient is available, the Group Life Cycle job extends the expiry date of the group by 7 days on the group's expiry day. The job continues this process until the notification is sent.

- When the *1 day before expiration* option is selected for sending notifications, GroupID extends the group's expiry date by 7 days, starting from the expiry date.

  Suppose a group has its expiry date set to July 1. With the notification sent one day before expiry (i.e., June 30), GroupID extends the group's expiry date to +7 days (i.e., July 8). The group will expire when it reaches its extended expiry date (i.e., July 8).

NOTE Notifications are sent if an SMTP server is configured for the identity store.

Expire a group manually

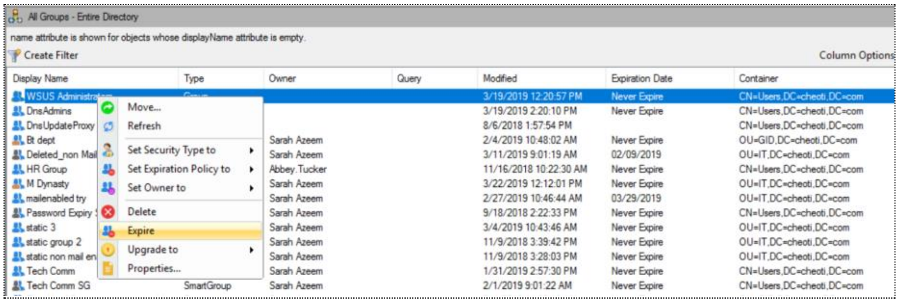
You can manually expire a group, overlooking its expiry policy. Even groups with a "Never expire" policy can be manually expired.

However, you cannot expire a group when any of the following conditions is met:

- When the expiry of security groups is disabled in group lifecycle settings.
- When a group resides in a container the group lifecycle policy does not apply to.

To expire a group manually:

1. In GroupID Management Console, select **Automate > [required group node].**
2. In the groups list, select one or more groups.
3. Right-click the selection and select **Expire**.



All Groups - Entire Directory

name attribute is shown for objects whose displayName attribute is empty.

Display Name	Type	Owner	Query	Modified	Expiration Date	Container
WSUS Administrators	Group			3/19/2019 12:20:57 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsAdmins				3/19/2019 2:20:10 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsUpdateProxy				8/6/2018 1:57:54 PM		CN=Users,DC=cheoti,DC=com
Bt dept		Sarah Azeem		2/4/2019 10:48:02 AM	Never Expire	OU=GID,DC=cheoti,DC=com
Deleted_non Mail		Sarah Azeem		3/11/2019 9:01:19 AM	02/09/2019	OU=IT,DC=cheoti,DC=com
HR Group		Abbey.Tucker		11/16/2018 10:22:30 AM	Never Expire	CN=Users,DC=cheoti,DC=com
M Dynasty		Sarah Azeem		3/22/2019 12:12:01 PM	Never Expire	OU=IT,DC=cheoti,DC=com
mailenabled try		Sarah Azeem		2/27/2019 10:46:44 AM	03/29/2019	OU=IT,DC=cheoti,DC=com
Password Expiry		Sarah Azeem		9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
static 3		Sarah Azeem		3/4/2019 10:43:46 AM	Never Expire	OU=IT,DC=cheoti,DC=com
static group 2		Sarah Azeem		11/9/2018 3:39:42 PM	Never Expire	OU=IT,DC=cheoti,DC=com
static non mail en		Sarah Azeem		11/9/2018 3:28:03 PM	Never Expire	OU=IT,DC=cheoti,DC=com
Tech Comm		Sarah Azeem		1/31/2019 2:57:30 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech Comm SG	SmartGroup	Sarah Azeem		2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com

Figure 54: Expire command on the shortcut menu

Expire a group using an expiry policy

You can change the default expiry policy for a group.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. In the **Expiration Policy Settings** area on the **General** tab (Figure 36), select a new expiry criterion from the **Expiration Policy** list. Options are:
    - Never Expire
    - Expire Every 30 Days
    - Expire Every 60 Days
    - Expire Every 90 Days
    - Expire Every 120 Days
    - Expire Every 6 Months
    - Expire Every Year
    - Other
      On selecting this option, a text box and a list box is displayed. From the list box, select **Days**, **Months** or **Years** and in the text box, type the desired number of days/months/years. Below is the range of values that can be entered in the text box:
        - 1 - 999 for days
        - 1 - 99 for months
        - 1 - 99 for years
4. On selecting an expiry option, a confirmation message is displayed. Click **Yes**.

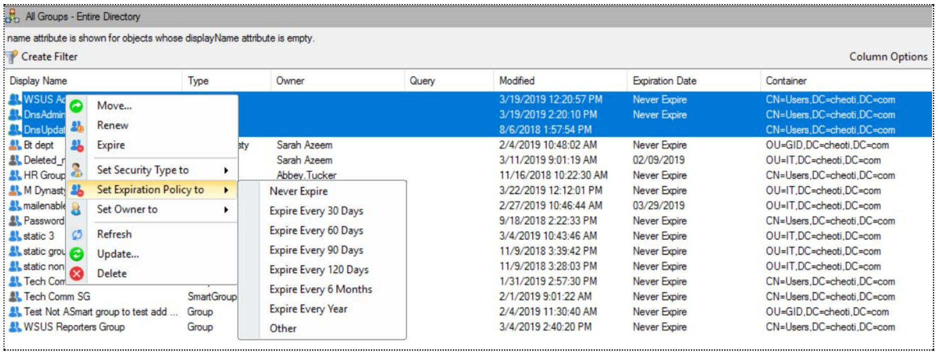
   The group's expiry date, as determined by the selected expiry policy, is displayed next to **Expiration Date**.

   NOTE The **Expiration Policy** list is disabled for Dynasty children since they inherit the expiry policy from their parent.
5. Click **OK** to close the dialog box.

NOTE If expiry notifications are enabled in the Group Life Cycle policy but the group has no owner or default approver, the group will not expire.

Modify the expiry policy of multiple groups

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, select one or more groups.
3. Right-click the selection, click **Set Expiration Policy to** and select an expiry policy.



Display Name	Type	Owner	Query	Modified	Expiration Date	Container
WSUS Ac				3/19/2019 12:20:57 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsAdmir				3/19/2019 2:20:10 PM	Never Expire	CN=Users,DC=cheoti,DC=com
DnsUpdat				8/6/2018 1:57:54 PM		CN=Users,DC=cheoti,DC=com
Bt dept	ty	Sarah Azeem		2/4/2019 10:48:02 AM	Never Expire	OU=GID,DC=cheoti,DC=com
Deleted_r		Sarah Azeem		3/11/2019 9:01:19 AM	02/09/2019	OU=IT,DC=cheoti,DC=com
HR Group		Abbey.Tucker		11/16/2018 10:22:30 AM	Never Expire	CN=Users,DC=cheoti,DC=com
M Dynasty				3/22/2019 12:12:01 PM	Never Expire	OU=IT,DC=cheoti,DC=com
mailenable				2/27/2019 10:46:44 AM	03/29/2019	OU=IT,DC=cheoti,DC=com
Password				9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
static 3				3/4/2019 10:43:46 AM	Never Expire	OU=IT,DC=cheoti,DC=com
static grou				11/9/2018 3:39:42 PM	Never Expire	OU=IT,DC=cheoti,DC=com
static non				11/9/2018 3:28:03 PM	Never Expire	OU=IT,DC=cheoti,DC=com
Tech Com				1/31/2019 2:57:30 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech Comm SG	SmartGroup			2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com
Test Not ASmart group to test add ...	Group			2/4/2019 11:30:40 AM	Never Expire	OU=GID,DC=cheoti,DC=com
WSUS Reporters Group	Group			3/4/2019 2:40:20 PM	Never Expire	CN=Users,DC=cheoti,DC=com

Figure 55: Set Expiration Policy to command on the shortcut menu

4. Click **Yes** on the confirmation dialog box.

NOTE

If your selection includes Dynasty children, their expiry policy will not be updated.

Renew expired groups

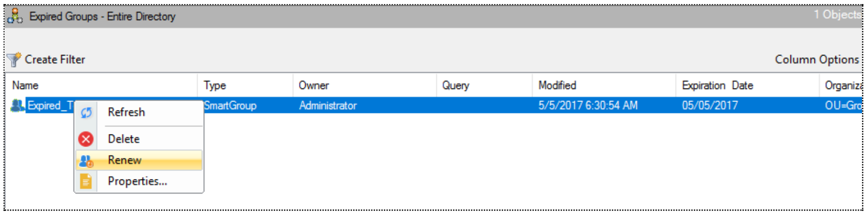
If a group has expired and you still need it, you can renew it. Upon renewal, the group becomes active again and its expiry policy is re-applied to it, starting from the date of renewal.

In the Group Life Cycle policy, the administrator can specify a period for which expired groups are not deleted from the directory. If a group is not renewed within this period, the Group Life Cycle job automatically deletes it from the directory.

For information about deleted groups, see Group Deletion.

To renew an expired group:

1. In GroupID Management Console, select **Automate** > **All Groups** > **Expired Groups**.
2. From the groups list, select one or more groups.
3. Right-click the selection and click **Renew**.



Name	Type	Owner	Query	Modified	Expiration Date	Organiza
Expired_T	SmartGroup	Administrator		5/5/2017 6:30:54 AM	05/05/2017	OU=Gro

Figure 56: Renew command on the shortcut menu

Dynasty children automatically renew with their parent. Renewing them individually is not allowed.

Group Deletion

GroupID handles group deletion as either physical or logical.

In the **Recycle Bin**, you can distinguish physically deleted groups from logically deleted groups by their type.

- Physically deleted groups have *Tombstone* as type.
- Logically deleted groups are of the *Logically Deleted Group* type. They also have **Deleted_** prefixed to their display names. However, groups in the Recycle Bin are displayed by their names, not their display names.

Both types are locked for further operations until restored.

While all searches in GroupID are catered through Elasticsearch, the Recycle Bin is an exception, as it fetches data from the directory.

The Recycle Bin does not display data for an Azure based identity store.

Physical Deletion

Physical group deletion refers to manually deleting groups using the *Delete* command on the *Actions* menu or shortcut menu. GroupID moves a physically deleted it to the **Recycle Bin** node while stripping it of most of its properties. You cannot delete a group from the Recycle Bin; however, you can restore it. The restoration process not only restores the group to its original container, but it also reinstates the home container for the group, if deleted.

When restored, a physically deleted group is restored with limited attributes; its membership is not restored.

A Smart Group and Dynasty is restored as a static group with no members and no query.

Logical Deletion

Groups that are deleted by the Group Life cycle job are considered to be logically deleted. The job deletes expired groups X number of days after group expiry, as specified in the Group Life Cycle policy.

Upon deletion, logically deleted groups are moved to the **Recycle Bin** node, with all their attributes intact. As a result, a logically deleted group, when restored, returns to its state it had at the time of deletion. The restoration process not only restores the group to the container from where it was deleted but it also reinstates the home container for the group, if deleted.

You can also manually delete a logically deleted group in the **Recycle Bin**, making it physically deleted. Simply right-click the required group and select **Delete** on the shortcut menu.

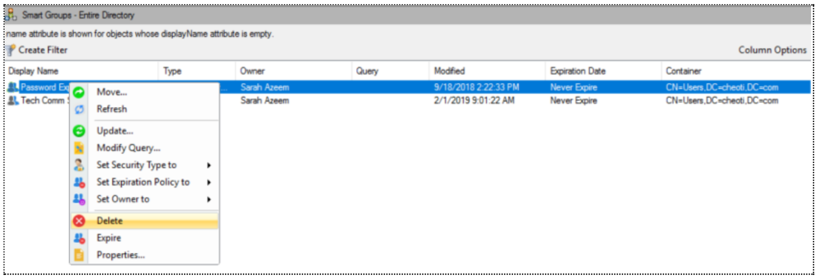
Deletion Notifications

When the Group Life Cycle job deletes a group, it notifies the group owners or, if there is no owner, the default approver specified in the Group Life Cycle policy.

The job does not delete a group that neither has an owner nor a default approver.

Physically delete a group

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, select one or more groups.
3. Right-click the selection and click **Delete** on the shortcut menu.



Smart Groups - Entire Directory

name attribute is shown for objects whose displayName attribute is empty.

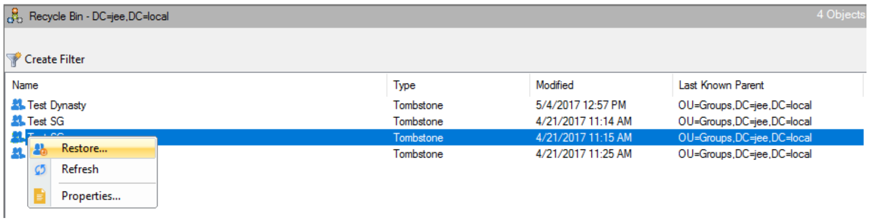
Display Name	Type	Owner	Query	Modified	Expiration Date	Container
Password Ex		Sarah Azeem		9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech Comm		Sarah Azeem		2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com

Figure 57: Delete command on the shortcut menu

Restore a deleted group

1. In GroupID Management Console, select **Automate** > **Recycle Bin**.
2. From the groups list, select one or more groups, as required.

3. Right-click the selection and click **Restore**.



Recycle Bin - DC=jee,DC=local — 4 Objects

Name	Type	Modified	Last Known Parent
Test Dynasty	Tombstone	5/4/2017 12:57 PM	OU=Groups,DC=jee,DC=local
Test SG	Tombstone	4/21/2017 11:14 AM	OU=Groups,DC=jee,DC=local
	Tombstone	4/21/2017 11:15 AM	OU=Groups,DC=jee,DC=local
	Tombstone	4/21/2017 11:25 AM	OU=Groups,DC=jee,DC=local

Figure 58: Restore command on the shortcut menu

NOTE You can only restore a physically deleted group from the Recycle Bin if the service account for the connected identity store has the 'Reanimate Tombstone' permissions.

Group history

Automate can maintain a complete track of actions performed on a group since its creation, if history tracking is enabled for the identity store. The actions to be tracked by Automate are also specified in history setting.

GroupID offers two views of history logging for a group:

- Normal view
- Detailed view

To view a group's history:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. From the groups list, right-click the required group and select **Properties**.
3. On the group properties dialog box, select the **History** tab (Figure 40).
   By default, this tab display history in normal view.
4. Select a history record and click the **View Details** icon (☰) to switch to detailed view.
5. Click **OK** to close the dialog box.

Normal view

The normal history view is what you see on the **History** tab (Figure 40) in group properties. It displays:

- **Time**, the date and time that the action was performed.
- **Action**, the type of action performed.

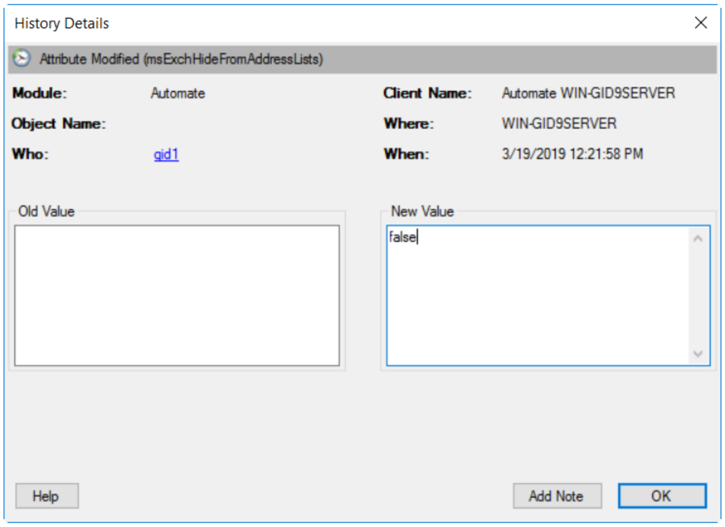
- **Attribute**, the schema attribute that was changed due to the action.
- **Old Value**, the value before the change was applied.
- **New Value**, the changed value.

If the history record spans multiple pages, you can page through the records using the navigation buttons available at the top of the tab.

Detailed view

You can view the details of each history record displayed in the normal view.

Select a history record in the normal view and click the **View Details** icon (📋).



History Details

Attribute Modified (msExchHideFromAddressLists)

Module: Automate

Object Name:

Who: gid1

Client Name: Automate WIN-GID9SERVER

Where: WIN-GID9SERVER

When: 3/19/2019 12:21:58 PM

Old Value

New Value: false

Figure 59: History Details dialog box

For single-valued attributes, the dialog box displays the old and new values. For multi-valued attributes, the lists of added items and removed items are displayed. Information comprises of:

- **Module**, the name of the GroupID module that performed the action.
- **Client Name**, the module and machine name on which the action was performed.
- **Object Name**, the name of the group the action was performed on.
- **Where**, the machine name from where the action was performed.
- **Who**, the name of the user who performed the action.
- **When**, the date and time of action.

The following lists are available when the target attribute is single-valued.

- **Old Values**, the list of values before the action was performed.
- **New Values**, the list of values after the action was performed.

The following lists are available when the target attribute is multi-valued.

- **Added Items**, the list of items that were added to the multi-value attribute.
- **Removed Items**, the list of items that were removed from the multi-value attribute.

Notes on history items

GroupID enables a user to add notes to history items that were logged as a result of any change he or she made. A note may explain the reason for making a certain change, such as the reason for changing the expiry policy of a group.

Only the user who added the note can update it. Other users can only view this note; they cannot edit it or add comments.

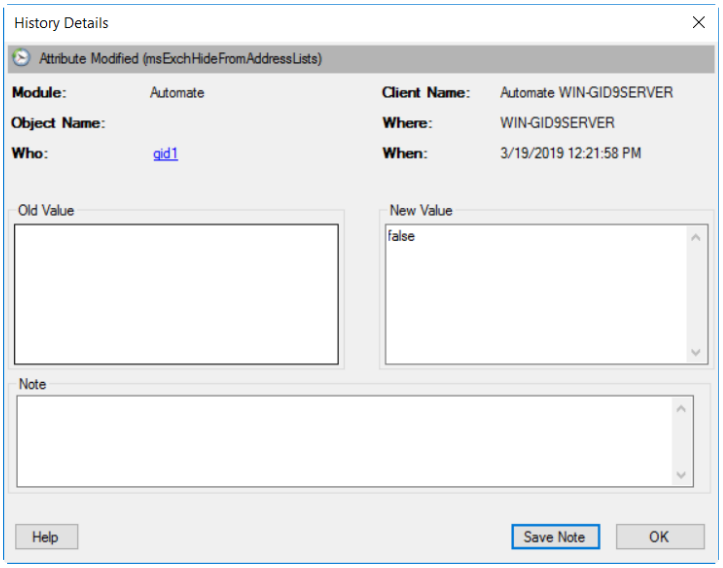
On the **History Detail** dialog box (Figure 59), one of these is available to you:

- The Add Note button
  When you are the user who performed the action that logged this history item and you haven’t added any note yet.
- The Edit Note button
  When you are the user who performed the action that logged this history item and you have already added a note.
- The note text
  When the user who performed the action has added a note. If you are not this user, you can only view this note.
- None of these buttons
  When you are not the user who performed the action and the user performing the action has not added any note.

A history note added or updated for an item using Automate is visible in the Self-Service portal and vice versa.

Add a note

1. On the **History Detail** dialog box ((Figure 59), click the **Add Note** button to add a note to the history item. The **Note** textbox is displayed.



History Details

Attribute Modified (msExchHideFromAddressLists)

Module: Automate
Object Name:
Who: gid1
Client Name: Automate WIN-GID9SERVER
Where: WIN-GID9SERVER
When: 3/19/2019 12:21:58 PM

Old Value:

New Value: false

Note:

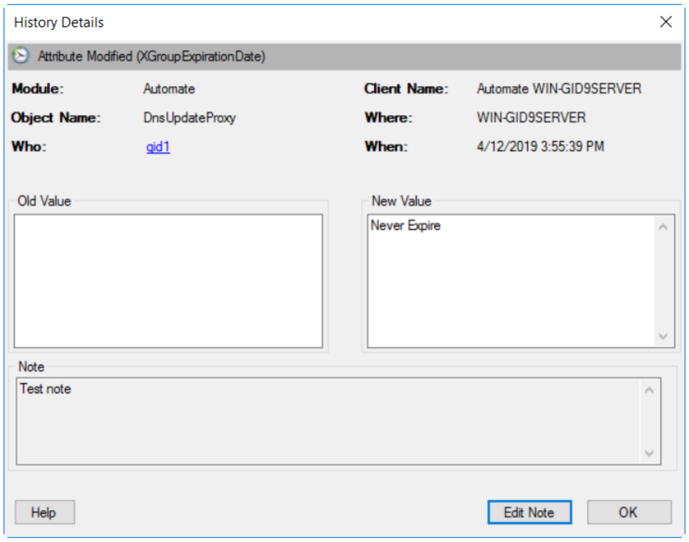
Figure 60: Note textbox on the History Detail dialog box

2. Write a note and click **Save Note** to save it.
   Your note can have a maximum of 500 characters.

   Once a note is added, the **Edit Note** button is available. Use it to update your note.
3. Click **OK**.

Edit a note

On the **History Detail** dialog box (Figure 59), the **Note** box displays your note for the history item.



History Details

Attribute Modified (XGroupExpirationDate)

Module: Automate
Object Name: DnsUpdateProxy
Who: gid1
Client Name: Automate WIN-GID9SERVER
Where: WIN-GID9SERVER
When: 4/12/2019 3:55:39 PM

Old Value:

New Value: Never Expire

Note: Test note

Figure 61: History Detail dialog box with the Edit Note button

1. Click the **Edit Note** button and update the note.
2. Save the changes and click **OK**.

View a note

Once a note is added, other users can view it, but they cannot edit it or add comments to it.

On the **History Detail** dialog box (Figure 59), the **Note** box displays the note. Read it and click **OK**.

Remove a note

On the **History Detail** dialog box (Figure 59), the **Note** box displays your note for the history item.

1. Click the **Edit Note** button and remove the note.
2. Click **Save Note** and then **OK**.

Chapter 7 - Group Memberships

Groups let you apply a common set of policies to multiple users. Groups also guarantee consistency of permissions and privileges across the membership. Using Automate, you can do the following with regards to group membership:

- Add and remove group members
- Change the membership type of a member
- View a group member's properties
- Fundamentals for nesting

Membership settings

To avoid large, unusual changes to Smart Group and Dynasty memberships, the administrator can configure the 'Out of Bounds' setting for an identity store.

The administrator can:

- Specify the maximum number of members for a Smart Group and Dynasty
- Determine actions to take if the limit is exceeded, such as not updating group membership or breaking the membership into smaller nested groups.

Example:

Let's assume the administrator sets the maximum membership limit to 500 and opts for nested groups when membership exceeds this limit.

Scenario 1: On update, 485 objects are fetched to be added to Group A's membership. Since the count is less than 500, the objects are directly added as group members.

Scenario 2: On the next update, 620 objects are fetched to be added to Group A's membership. Since the count exceeds 500, it breaks the membership into 2 child groups (Group 1 with 500 members and Group 2 with 120 members) and nests them into Group A. Hence, GroupID checks the member count and takes necessary action before adding members to the group.

In case of an Office 365 group the option to break the membership into child groups would have the following impact:

An Office 365 group (Group A) will be updated according to the Smart Group update process. However, when the maximum membership limit is hit, the update process will create child group(s) and try to add them as members of Group A. Since an Office 365 group cannot have groups as members, Group A's membership will be empty. The child groups will continue to exist but without any link to Group A.

Modify group membership

You can add and remove members to groups in any of these ways:

- Add and remove members manually
- Permit group owners to modify group membership on the directory server
- Auto-update group membership using a Smart Group Update job
- Import members using an external data source

Manually update group membership

You can manually add and remove members to a group any time when required.

This method is recommended for static (unmanaged) groups only. For Smart Groups and Dynasties, Automate will discard any manual membership changes when it updates groups through the Smart Group Update job.

Static group membership is also affected by the membership lifecycle policies defined for the identity store.

To add members manually:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. Right-click the required group and select **Properties**.
3. On the **Members** tab (Figure 37), click **Add**; the **Find** dialog box (Figure 46) is displayed. Locate the directory objects that you want to add to this group's membership. The selected objects get listed in the **Members** area of the **Members** tab.
4. Click **Apply** and then **OK** to save the changes.

When adding groups to the membership of this group, you must be familiar with the basic nesting principals. See Nesting fundamentals on page 102 for reference.

Only user objects can be added as members of an Office 365 group.

Remove members manually

1. In GroupID Management Console, select **Automate > [required group node]**.
2. Right-click the required group and select **Properties**.
3. Click the **Members** tab (Figure 37).
4. In the **Members** list, select the member to remove and click **Remove**.
   To select multiple members, press and hold the CTRL key while clicking the members in the list.

   Use **Remove All** to remove all members of the group.

Allow group owners to modify membership on the directory server

For a group, you can authorize its owners (primary owner and Exchange additional owners) to update the group's membership directly on the directory server. Additional owners are not included.

This is a provider-end permission and does not impact role-based permissions assigned at the identity store level in GroupID. Nor do role-based permissions assigned at the identity store level have any impact on this feature.

Enabling this setting auto-grants the required permissions to the managers. For Active Directory, for example, the following permissions are granted:

- Create, delete, and manage user accounts
- Reset user password and force password change at next logon
- Create, delete and manage groups
- Modify the membership of a group

It is not recommended to update Smart Group and Dynasty membership manually; changes might be reversed when a Smart Group Update job runs.

To grant permission on the directory server:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. Right-click the required group and select **Properties**.
3. Click the **Managed By** tab (Figure 39).
4. Select the **Manager can update membership** check box to enable the group's primary owner and Exchange additional owners to update this group's membership directly on the directory server.
5. Click **OK**.

The *manager can update membership* feature is not available for groups in an Azure based identity store.

Scheduled membership update

You can associate a scheduled job with Smart Groups and Dynasties for scheduled membership update. This job should be of the' Smart Group Update' type.

Each Smart Group and Dynasty has a user-defined query specified for it. When the scheduled job runs, it updates group membership with the records fetched by the query.

Static groups cannot be updated automatically because they do not have a query defined for them.

For more information on updating Smart Group and Dynasty membership, see Update Smart Groups and Dynasties on page 60.

Import group members using a wizard

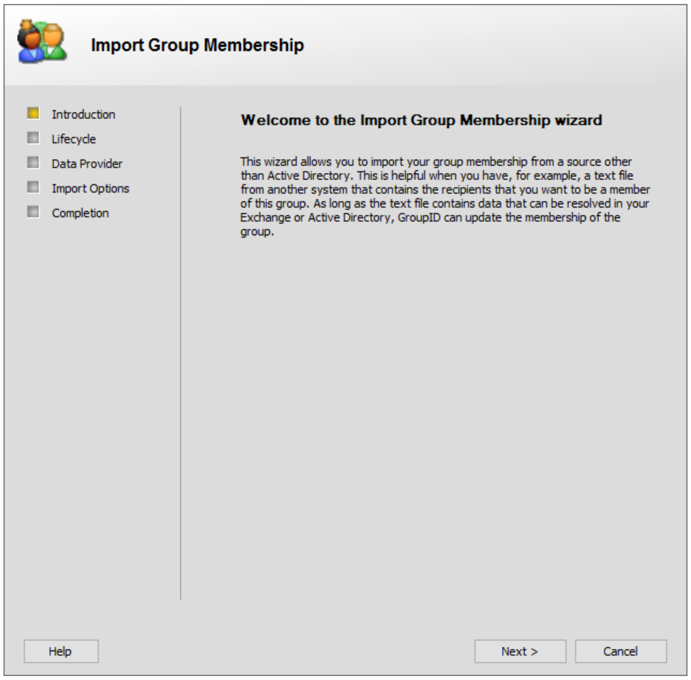
In this method, you specify an external data source containing the list of objects to add as members to the selected group. When importing, Automate compares the data in the external data source with the directory using a key field, and then adds matching objects to the group membership.

For example, you have a list of employee-IDs in a text file and you want to add all employees from the directory, whose IDs match with those present in the text file, to the membership of the group. Simply select the text file and map its field name with the employeeID attribute of the directory. The wizard will search the directory for objects having those values for employeeID as present in the text file, and add those to the membership of the group.

Only user objects can be imported as members for an Office 365 group.

To import group members:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Members** tab (Figure 37), click **Import**.
   The **Import Group Membership** wizard opens to the **Welcome** page.



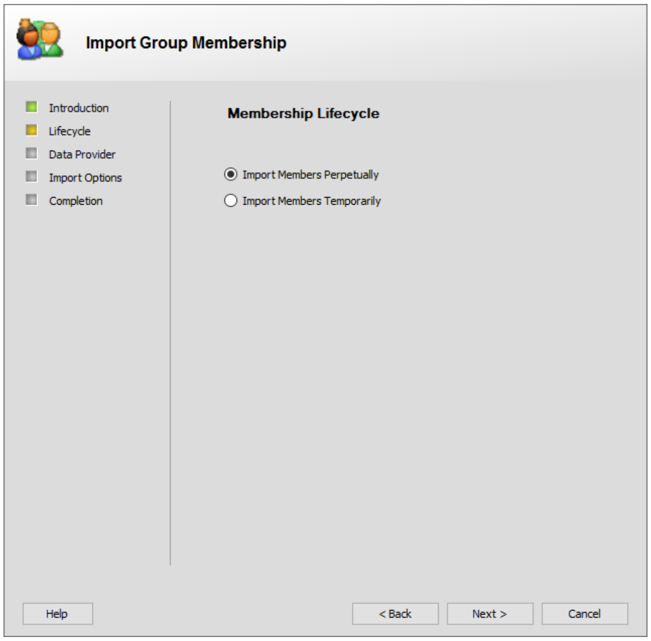
Import Group Membership

Welcome to the Import Group Membership wizard

This wizard allows you to import your group membership from a source other than Active Directory. This is helpful when you have, for example, a text file from another system that contains the recipients that you want to be a member of this group. As long as the text file contains data that can be resolved in your Exchange or Active Directory, GroupID can update the membership of the group.

Figure 62: Welcome page

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



Import Group Membership

Membership Lifecycle

● Import Members Perpetually
○ Import Members Temporarily

Figure 63: Membership Lifecycle page

5. Select whether the imported members should be added permanently or temporarily to the group membership.

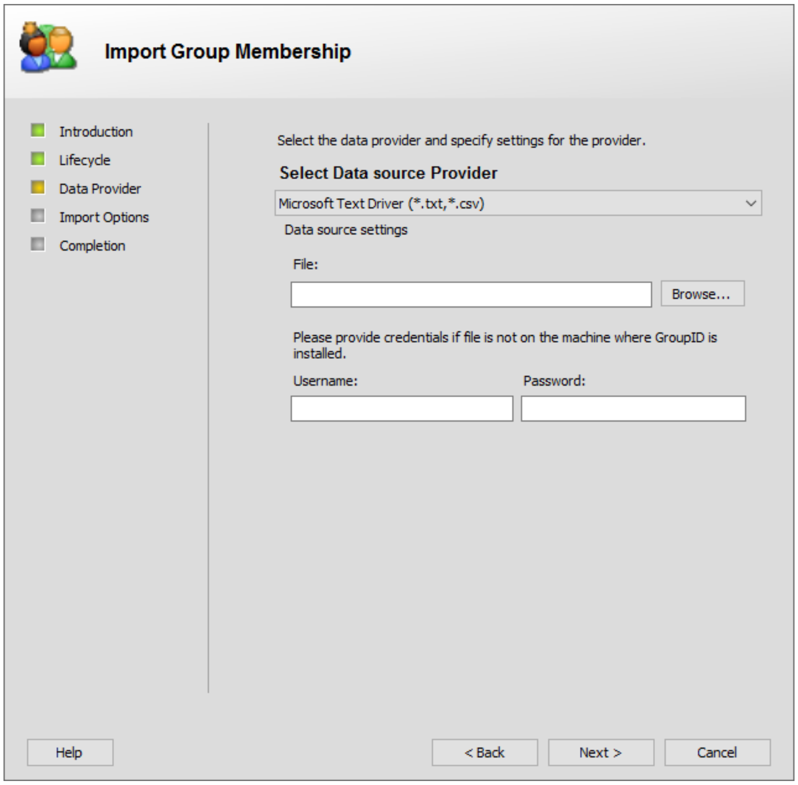
   - **Select Members Perpetually**: to add imported members permanently to the group membership.

- **Import Members Temporarily:** to add imported members to the group membership for a specific period. At end of the period, these members are automatically removed from membership.

6. In case of temporary membership, use the **Duration** list to specify the membership duration of the imported members. Options are:

    - **7 Days**, to add members to the group for 7 days starting today.
    - **30 Days**, to add members to the group for 30 days starting today.
    - **90 Days**, to add members to the group for 90 days starting today.
    - **Custom**, to add members to the group for the period you specify in the **From** and **To** boxes. Members are added to the group on the date in the **From** box and removed from membership on the date in the **To** box.

7. Click **Next**.



Select the data provider and specify settings for the provider.

Select Data source Provider

Microsoft Text Driver (*.txt,*.csv)

Data source settings

File:

Please provide credentials if file is not on the machine where GroupID is installed.

Username:

Password:

Figure 64: Data Provider page

On the **Data Provider** page, select and configure the data source that contains the objects for import. Automate compares the data in the external data source with the directory using a key field, and then adds matching objects to the group membership.

8. From the **Select Data Source Provider** list, select one of the following options:

- **Microsoft Text Driver (*.txt, *.csv)**

  Use the Microsoft Text Driver (*.txt; *.csv) to connect to Comma Separated Value (CSV) text files or Tab Separated Value (TSV) text files. This provider supports automatic schema detection if a header row is included in the file.

  a. Click **Browse** to select the required CSV or TSV file.

  b. In the **User name** and **Password** boxes, provide a user name and password to connect to the machine where the file is placed.
     This is required only when the file is placed on a machine other than the GroupID machine.

- **ODBC Data Source**

  The ODBC provider can be used to connect to any ODBC compatible data source. This can be any data source including databases, directories, or even files.

  a. Click the **ODBC** button to launch the Windows **ODBC Data Source Administrator** dialog box to select the System DSN to use.

  b. In the **Table or view** box, specify the name of the table or view to use.

  c. In the **User name** and **Password** boxes, provide a user name and password to access the directory server.

- **Sun ONE iPlanet Driver**

  Use the Sun ONE Directory Server (iPlanet) provider to connect to a Sun ONE directory. This provider does not support dynamic schema.

  a. In the **Server** box, specify the name or the IP address of the directory server to connect to.

  b. In the **Port** box, provide the port on which LDAP is running. If this box is left blank, the default port (389) is used.

  c. In the **Container** box, specify the path to use as a start location. Only objects that exist in the LDAP path specified and all sub-containers are considered for extracting matching records from the directory. If this box is left empty, all objects in the data source are checked for matches in the connected identity store.

  d. In the **User DN** box, provide a user name to connect to the directory. Leave this box blank to connect anonymously.

  e. In the **Password** box, provide a password for the specified user name (if required).

- **Lotus Notes**

  Use the Lotus Notes provider to connect to a Lotus Notes directory. This provider does not support dynamic schema detection. A schema file is included with the most commonly used fields. You may add fields to this schema using the **Advance Connection Properties** dialog box.

  The fields available for this data provider are the same as for Sun ONE iPlanet Driver.

- **Microsoft SQL Driver**

  Use this driver to connect with Microsoft SQL Server database systems.

  a. By default, GroupID uses the SQL authentication mode to connect to SQL Server. Select the **Windows Authentication** check box to enable the Windows Authentication mode to connect to SQL Server. GroupID works with this mode in context of the account configured in GroupIDAppPool10 (both when SQL Server is available locally or remotely.

     Selecting this check box disables the **Username** and **Password** boxes.

  b. In the **Server** box, specify the name or IP address of SQL Server on your network.

  c. In the **Database** box, specify the name of the database you want to access on SQL Server.

  d. In the **Table or view** box, provide the name of the table or view in the specified database that you want to connect to.

  e. In the **Username** and **Password** boxes, provide the user name and password required to access SQL Server.

- **Oracle**

  Use this driver to connect with Oracle database systems.

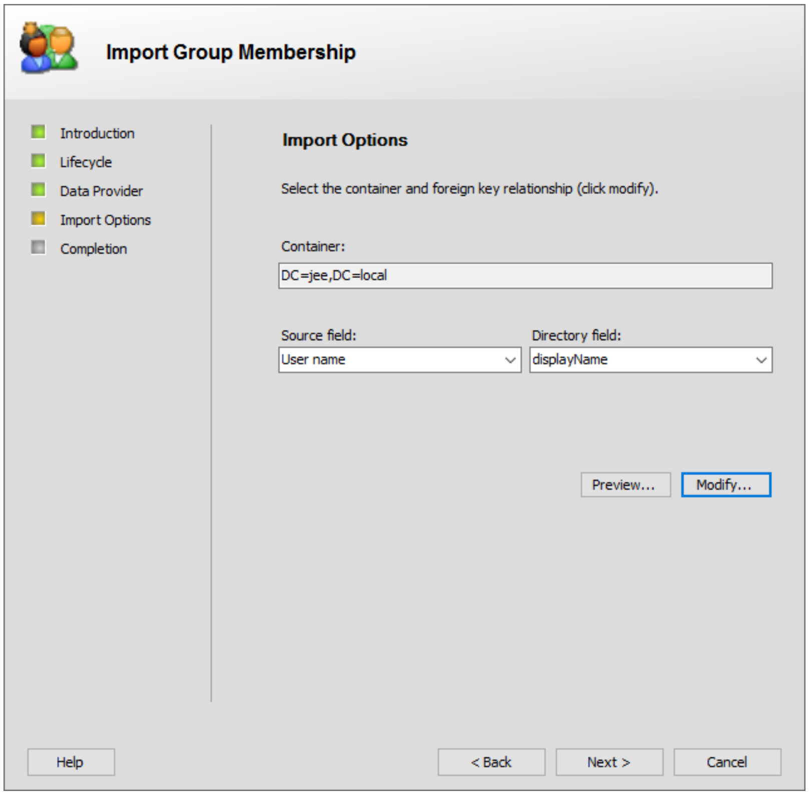
  a. In the **Server** box, specify the name or IP address of the Oracle server on your network.

  b. In the **Database** box, specify the name of the database you want to access on the Oracle server.

  c. In the **Table or view** box, provide the name of the table or view in the specified database that you want to connect to.

  d. In the **Username** and **Password** boxes, provide the user name and password required to access the Oracle server.

9. Click **Next**.



Import Group Membership

Import Options

Select the container and foreign key relationship (click modify).

Container: DC=jee,DC=local

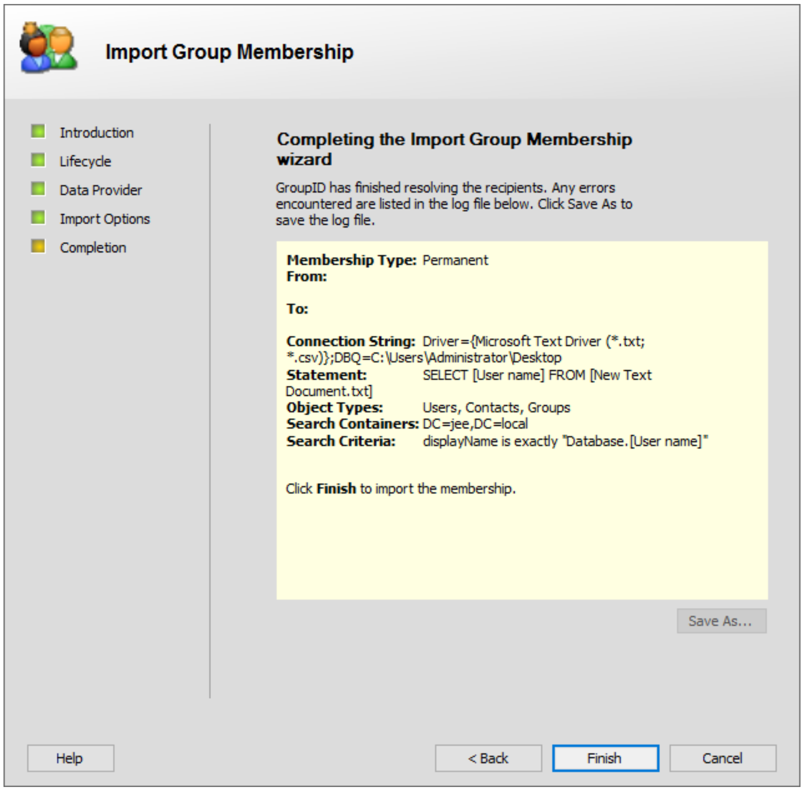
Source field: User name

Directory field: displayName

Figure 65: Import Options page

On the **Import Options** page, select the source container and map the fields for the data source and the directory. The wizard matches the values of the mapped fields to determine what objects to import to the group's membership.

10. The **Container** box displays the top-level container in the connected identity store to locate members for import.
11. From the **Source field** list, select the name of the field in the data source to map to its equivalent directory field.
12. From the **Directory field** list, select the name of the directory field to map to the selected source field.
    The wizard imports memberships where values for both fields match.
13. Click **Preview** to view the values returned as a result of the mapped fields.
14. Click **Modify** to launch the [Query Designer dialog box]() for specifying advanced queries.
15. Click **Next**.



Completing the Import Group Membership wizard

GroupID has finished resolving the recipients. Any errors encountered are listed in the log file below. Click Save As to save the log file.

Membership Type: Permanent
From:

To:

Connection String: Driver={Microsoft Text Driver (*.txt; *.csv)};DBQ=C:\Users\Administrator\Desktop
Statement: SELECT [User name] FROM [New Text Document.txt]
Object Types: Users, Contacts, Groups
Search Containers: DC=jee,DC=local
Search Criteria: displayName is exactly "Database.[User name]"

Click **Finish** to import the membership.

Figure 66: Completion page

16. This page displays a summary of the settings specified on the previous pages. It also displays a log of the errors encountered during the object matching process, if any.
    Click **Save As** to save the log details to a file.

17. Click **Finish** to import members to the group.

Change a member’s membership type

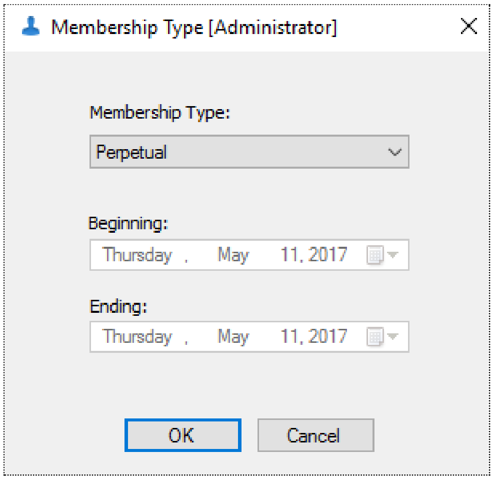
Membership type indicates whether an object is a temporary or permanent member of a group. The Membership Life Cycle job updates the temporary membership of groups. It adds and removes temporary members from group membership on the specified dates.

Consider a scenario where the Membership Life Cycle job is scheduled to run once a week, say Mondays. If an object is to be added to group membership for three days - Wednesday till Friday, it will not be added. This happens because the Membership Life Cycle job did not run on the particular days for temporary membership update.

The Membership Life Cycle job must be scheduled to run at a frequency that meets your temporary membership requirements.

To change membership type:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Members** tab (Figure 37), select a member and click **Change Membership** to change its membership type.



Membership Type [Administrator]

Membership Type: Perpetual

Beginning: Thursday , May 11, 2017

Ending: Thursday , May 11, 2017

Figure 67: Membership Type dialog box

4. Select an option from the **Membership Type** list to specify the member's membership type:

Membership Type	Description
Perpetual	To make the object a permanent member of the group.
Temporary Member	To make the object a temporary member of the group for the period you specify in the **Beginning** and **Ending** boxes. At the end of the period, the object is removed from the group membership.
Addition Pending	Indicates that the object will be a temporary member of the group for a period in the future. Use the **Beginning** and **Ending** boxes to set a period. Before the beginning date, the object’s membership type is displayed as ‘Addition Pending’. On the beginning date, the membership type changes to ‘Temporary Member’. **Example:** You add Smith as a temporary member to Group A on May 15, 2019 for future dates, May 20-30, 2019.

	Smith will be displayed in Group A's membership with 'Addition Pending' as its membership type from May 15 to 19, 2019. However, Smith would not be added to group membership in the provider. On May 20, Smith will become a temporary member of Group A and its membership type will change to 'Temporary Member' from May 20 to 30, 2019. Smith will also be added to group membership in the provider. After May 30, Smith will be removed from Group A as a member in GroupID and in the provider.
Removal Pending	Indicates that the object will be temporarily removed from group membership for a period in the future. Use the **Beginning** and **Ending** boxes to set a period. Before the beginning date, the object's membership type is displayed as 'Removal Pending'. On the beginning date, the membership type will change to 'Temporary Removed'. **Example:** You remove Smith from Group A on May 15, 2019 for future dates, May 20-30, 2019. Smith will be displayed in Group A's membership with 'Removal Pending' as membership type from May 15 to 19, 2019. On May 20, Smith's membership type in GroupID will change to 'Temporary Removed'; lasting till May 30, 2019. However, Smith will be removed from Group A's membership in the provider. After May 30, Smith will be added back to Group A as a permanent member in GroupID and in the provider.
Temporary Removed	Indicates that the object is temporarily removed from group membership for the period specified in the **Beginning** and **Ending** boxes. At the end of the period, the object is added back to the group membership as a permanent member.

Table 5: Membership Type

5. Click **OK** to close the **Membership Type** dialog box.
6. Click **OK** to close group properties.

View a member's properties

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. Click the **Members** tab (Figure 37).
4. In the **Members** area, double-click a member to view or modify its properties.
   - If the member is a ‘user’ or ‘contact’ object, the **User Properties** dialog box is displayed, where you can view the member's name, address, contact number, organization, the groups the user is a member of, and more.
   - If the member is a ‘group’ object, the **Group Properties** dialog box is displayed. See Chapter 5 - Group Properties on page 47.

Nesting fundamentals

Adding a group as a member of another group is called nesting. The nesting option depends on the domain functionality mode (native or mixed) of your Windows server and the group type.

- For distribution groups, nesting is supported in both mixed mode and native mode.
- For security groups, nesting is supported only for domains running in native mode.

Before nesting groups, be aware that depending on the scope of the group, the group can contain only specific types and scopes of other groups.

The following list describes what a group in native-mode domain can contain. The same applies to distribution groups in mixed-mode domains:

- A universal group can contain other universal groups, global groups and accounts from any domain in any forest. A universal group cannot contain any domain local groups.
- A global group can contain other global groups and accounts from the same domain that the group belongs to. A global group cannot contain any universal groups, or any global group or account from another domain.
- A domain local group can contain universal groups, global groups and accounts from any domain or forest. A domain local group can also contain other domain local groups from the same domain that the group belongs to.

A domain local group cannot contain other domain local groups from any other domain or forest.

Security groups in a mixed-mode domain have the following restrictions:

- Universal groups cannot be created in mixed-mode domains because the universal scope is supported only in Windows 2000 native-mode domains.
- A global group can contain accounts from the same domain to which the group belongs. A global group cannot contain any universal groups, any global group, or an account from another domain.
- A domain local group can contain global groups and accounts from any domain or forest. A domain local group cannot contain any other domain local group.

Chapter 8 - Exchange Settings

If your GroupID Management Console is connected to an Active Directory-based identity store with Microsoft Exchange configured as the messaging provider, you will find three additional tabs on the Group Properties dialog box for mail-enabled groups.

- Exchange General tab (Figure 41)
- Exchange Advanced tab (Figure 43)
- Email Addresses tab (Figure 42)

Use these tabs to manage Exchange-specific settings for a mail-enabled group, such as:

- Apply size limit to incoming , explains how you can specify a size limit that applies to each email sent to the group.
- Restrict recipients for sending emails to a group, explains how you can restrict the group to accept messages from certain recipients.
- Specify the Exchange alias for a group.
- Set a simple display name for a group.
- Select expansion server, provides instructions on selecting the Expansion Server for a group.
- Hide a group in Exchange address lists, describes how you can prevent a group from appearing in Exchange address lists.
- Hide membership from address book, explains the process of hiding group members from the Outlook address book.
- Set group to send ‘out-of-office’ messages, explains how you can configure out-of-office auto-replies.
- Authenticate users who send email to a group.
- Set recipient for non-delivery reports, instructs you about setting the recipient to whom the delivery failure report will be sent when a message is not delivered to the group.
- Assign values to custom attributes of a group, explains how you can utilize custom attribute fields to save additional information about the group.

Apply size limit to incoming messages

The default Exchange settings apply no restriction on the size of incoming messages a mail-enabled group can receive. You can specify a limit that applies to each incoming message.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. Click the **Exchange General** tab (Figure 41).
4. With respect to incoming messages, you can:
   - **Set a message size limit**
     In the **Message size** area, select **Maximum (KB)** and specify the maximum allowable size (in kilobytes) for incoming messages.
     Any message exceeding this is bounced back to the sender.
   - **Set no size limit**
     Select the **No limit** option for the **Message Size** setting.
     This indicates that there is no limit on the size of the incoming message.
5. Click **Apply** and then **OK**.

Restrict recipients for sending emails to a group

By default, a mailbox-enabled group can accept emails from everyone in an Exchange organization. You can apply restrictions so that the group can accept emails from a specific list of users and groups (mail-enabled only); or you can allow the group to accept emails from everyone except a specific list of users and groups.

A scenario can be as follows:
If you want the group to receive emails from all except one member (Member A) of a group (Group A), add Group A to the *Accept messages* list and then add Member A to the *Reject messages* list.

Allow group to receive emails from everyone

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange General** tab (Figure 41), locate the **Message Restrictions** area.

4. Select *None* in the **Apply a quick filter** list and make sure that *From everyone* is selected as the **Accept messages** setting.

5. Click **Apply** and then **OK**.

Allow emails only from group owners or members, or both

1. In GroupID Management Console, select **Automate > [required group node]**.

2. In the groups list, right-click the required group and select **Properties**.

3. On the **Exchange General** tab (Figure 41), locate the **Message Restrictions** area.

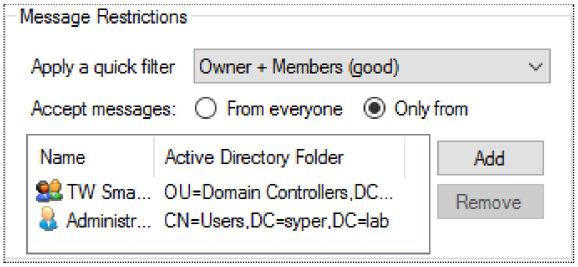
4. From the **Apply a quick filter** list, select one of the following:

   - **Owner only (best)** – the group can receive emails only from the primary owner, additional owner(s), and Exchange additional owner(s).

   - **Owner + Members (good)** – the group can receive emails from the primary owner, additional owner(s), Exchange additional owner(s), and all group members.

   You can view this group's members on the **Members** tab (Figure 37) and the group’s primary and additional owners on the **Managed By** tab (Figure 39).

5. When you select an option from the **Apply a quick filter** list, the respective users and groups are displayed in the **Accept messages** area accordingly. The group can receive emails from these objects only. You can add or remove users and groups (mail-enabled only) from the list using the **Add** and **Remove** buttons.



Message Restrictions

Apply a quick filter: Owner + Members (good)

Accept messages: ○ From everyone ● Only from

Name	Active Directory Folder
TW Sma...	OU=Domain Controllers,DC...
Administr...	CN=Users,DC=syper,DC=lab

Figure 68: Accept Messages area

6. Click **Apply** and then **OK**.

Allow emails from specific users or groups

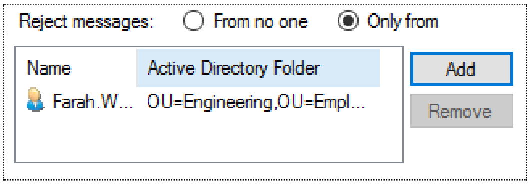
1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange General** tab (Figure 41), locate the **Message Restrictions** area.
4. For the **Accept messages** setting, select **Only from**.
5. To specify the users and groups (mail-enabled only) this group can receive emails from, click **Add**.
   The **Find** dialog box (Figure 46) is displayed, where you can search and select the required users and groups.

   The selected users and groups are displayed in the **Accept messages** area, as shown in Figure 68.
6. Click **Apply** and then **OK**.

Reject emails from specific users or groups

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange General** tab (Figure 41), locate the **Message Restrictions** area.
4. For the **Reject messages** setting, select **Only from**.
5. To specify the users and groups (mail-enabled only) this group cannot receive emails from, click **Add**.
   The **Find** dialog box (Figure 46) is displayed, where you can search and select the required users and groups.

   The selected objects are displayed in the **Reject messages** area, as shown below:



Reject messages: ○ From no one ● Only from

Name	Active Directory Folder
Farah.W...	OU=Engineering,OU=Empl...

Figure 69: Reject Messages area

6. Click **Apply** and then **OK**.

Specify the Exchange alias for a group

You can change the alias for a mail-enabled group.

With Microsoft Exchange as the messaging provider, the alias length is limited to 64 characters and it must be unique in the forest. The alias should also not contain characters that are considered invalid by Exchange.

The following table lists the valid characters for aliases for Microsoft Exchange Servers supported by GroupID:

<table>
<tr><th>Messaging System</th><th>Valid Characters</th></tr>
<tr><td>Exchange Server 2010/2013/2016/2019</td><td>• Uppercase letters (A-Z)
• Lowercase letters (a-z)
• Numeric digits (0-9)
• Special characters (#, $, %, &, ', *, +, -, /, =, ?, ^, _, `, {, |, } or ~). You can use one or more periods in an alias, but each one should be preceded and followed by at least one of the other characters.</td></tr>
</table>

Table 6: Valid characters for Exchange alias

To change the alias:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange General** tab (Figure 41), the **Alias** box displays the current alias for the group. Modify it as required.
4. Click **Apply** and then **OK**.

Set a simple display name for a group

The simple display name of a mail-enabled group is used by systems that cannot interpret all characters in a normal display name.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. Click the **Exchange Advanced** tab (Figure 43).
4. In the **Simple display name** box, specify a simple display name for this group.

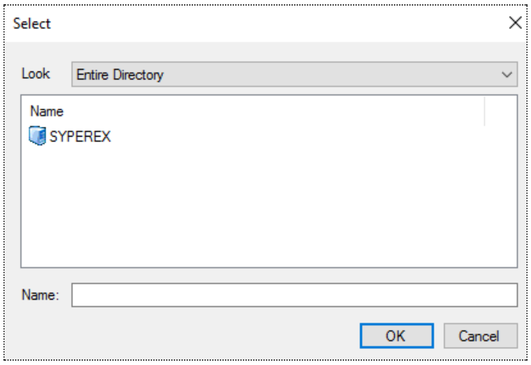
5. Click **Apply** and then **OK**.

Select expansion server

An expansion server is an Exchange Server responsible for expanding the membership list of a distribution group, resolving the names of all recipients in that group and determining the most efficient path for routing the message.

By default, the Exchange Server specified as the messaging provider for the connected identity store acts as the expansion server. However, you can specify a different expansion server for the group.

1. In GroupID Management Console, select **Automate** > **[required group node].**
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange Advanced** tab (Figure 43), click the **Browse** button next to the **Expansion server** box to select an expansion server.



Select

Look: Entire Directory

Name

SYPEREX

Name:

Figure 70: Select dialog box

4. Select the Exchange server to use to expand this distribution group.

   To revert to the default setting (that is, any server in the organization), click **Browse** and then click **OK** without selecting a server.

5. Click **Apply** and then **OK**.

Hide a group in Exchange address lists

You can prevent a mail-enabled group from appearing in the Global Address List (GAL) and other address lists that are defined in your Exchange organization.

Even when you apply this setting, users in your Exchange organization can still send messages to the group by using the group’s email address.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange Advanced** tab (Figure 43), select the **Hide group from Exchange address list** check box if you do not want the group to appear in Exchange address lists.
4. Click **Apply** and then **OK**.

Hide membership from address book

You can hide the members of a mail-enabled group from the Outlook address book.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange Advanced** tab (Figure 43), select the **Hide membership from address book** check box if you do not want group members to be displayed in the Outlook address book.
4. Click **Apply** and then **OK**.

Set group to send 'out-of-office' messages

You can set a mail-enabled group (Group A) to send out-of-office auto-replies to the message originator (sender), when the group (Group A) receives a message and one or more group members have *out-of-office* status.

1. In GroupID Management Console, select **Automate** > **[required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. Click the **Exchange Advanced** tab (Figure 43).
4. Select the **Set out-of-office messages to originator** check box to send out-of-office messages to the originator (sender) if any of the group members has the required settings in place.
5. Click **Apply**.

NOTE

Visit this link to configure out-of-office messages for Microsoft Exchange 2010 using Exchange Management Console.

Authenticate users who send email to a group

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. Click the **Exchange Advanced** tab (Figure 43).
4. Select the **Require authentication to send mail** check box to block incoming emails from users that cannot be authenticated on the domain where the group exists.
5. Click **Apply** and then **OK**.

Set recipient for non-delivery reports (NDR)

If a message sent to a group is not delivered, nobody is informed about the delivery failure, by default. You can change this setting to notify either the group owner or the message originator (sender) about the delivery failure by sending a non-delivery report.

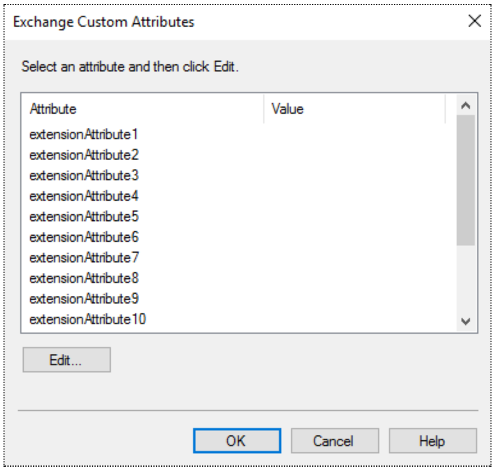
1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. Click the **Exchange Advanced** tab (Figure 43).
4. In the **Delivery Reports** area, select whether to notify the group owner or the message originator when a message sent to this group is not delivered to group members. You can also choose not to notify anyone.
   - **Send delivery reports to group owner** - The non-delivery report is sent to the group owner to inform him or her that a message sent to the group was not delivered to group members.
   - **Send delivery reports to message originator** - The non-delivery report is sent to the sender to inform him or her that the message was not delivered to the target group.
   - **Do not send delivery reports** – Non-delivery reports are not sent to anyone.
5. Click **Apply** and then **OK**.

NOTE Non-delivery reports are sent if an SMTP server is configured for the identity store.

Assign values to custom attributes of a group

Exchange provides 15 custom attribute fields that you can use to add additional information about a mail-enabled group. For example, you can use custom attributes to save health insurance data of the group's manager.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required group and select **Properties**.
3. On the **Exchange Advanced** tab (Figure 43), click **Custom Attributes**; the **Exchange Custom Attributes** dialog box is displayed, showing the list of all custom attributes.



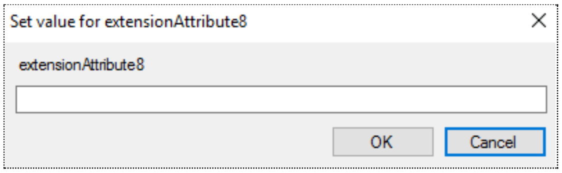
Exchange Custom Attributes

Select an attribute and then click Edit.

Attribute	Value
extensionAttribute1	
extensionAttribute2	
extensionAttribute3	
extensionAttribute4	
extensionAttribute5	
extensionAttribute6	
extensionAttribute7	
extensionAttribute8	
extensionAttribute9	
extensionAttribute10	

Figure 71: Exchange Custom Attributes dialog box

4. Select an attribute and click **Edit**.



Set value for extensionAttribute8

extensionAttribute8

Figure 72: Set value dialog box

5. Type a value for the custom attribute and click **OK**.
6. Repeat steps 5 and 6 to specify a value for another custom attribute.
7. Click **OK** to close the **Exchange Custom Attributes** dialog box.
8. Click **Apply** and then **OK** on the group properties dialog box.

Chapter 9 - Dynasties

A Dynasty is a Smart Group that creates and manages other Smart Groups using information in the directory. Dynasties help you manage large distribution lists by creating hierarchical group structures that represent your organization. The Smart Groups that the Dynasty creates are called child groups and become members of their respective parent Dynasty.

A Dynasty retrieves data from the directory on the same pattern as a Smart Group does, but it has its own mechanism of dividing the query results into child groups.

The group-by field determines child groups

When you create a Dynasty, you specify a query and a field, referred to as the *group-by* field. The group-by field is used to divide the query results into groups.

For example, if you set ‘department’ as the group-by field, then each distinct value for the ‘department’ field is returned, for instance, Sales, Marketing, and Human Resources. Thus, a Dynasty with the group-by field set to ‘department’ creates child groups for each distinct value: Sales, Marketing, and Human Resources.

Built-in updates

Automate keeps the Dynasty active in two ways:

- By adding new child groups as new values are returned for the group-by field.
- By removing existing child groups as previous values of the group-by field no longer exist in the directory.

Thus, as new values of the ‘department’ field appear, new groups are created, and as old values disappear, the corresponding child groups are deleted.

The same process occurs with the membership of each child group. When a user’s department changes from Sales to Marketing, for example, the user is removed from the Sales child group and added to the Marketing child group.

The child-parent relationship

Dynasty children inherit their parent's characteristics and properties, such as group type, group security, expiry policy, owner, delivery restrictions, message size restrictions and more. Inheritance saves administrators incalculable time through the systematic application of pre-defined properties to new groups.

You can modify the values of all inherited attributes for a child, except the expiry policy. Child Dynasties always inherit the expiry policy from the parent Dynasty and it can only be modified at the parent level.

Depending on the inheritance option selected for the parent Dynasty on the **Dynasty Options** dialog box (Figure 86) the modified values of inherited attributes may or may not persist.

Multi-level Dynasties

Automate can create multi-level Dynasties. For example, you can create one Dynasty that groups first by country, then state, and then city. When updated, the Dynasty creates a group for every country, then it creates a group for every state in a country, and finally it creates a group for each city within each state. Thus, each user in the organization belongs to a country group, a state group, and a city group, and because the groups are updated through their multi-level structure, you do not need to worry that they will go out-of-date.

Create a Dynasty

Automate provides the following templates for creating Dynasties:

- Organizational
  To create a Smart Group for every distinct company, then for each department within a company, and finally for each title in a department.
- Geographical
  To create a Smart Group for every distinct country, then for each state within a country, and finally for each city within a state.
- Managerial
  To either create separate Smart Groups for the direct reports of each manager or add all direct reports of the top manager and sub-level managers to a single group.
- Custom
  To begin with a blank Dynasty and select your own group-by attributes.

These templates provide pre-defined group-by attributes for creating Dynasty levels. You can also define custom group-by attributes to expand the Dynasty levels to suit your organizational model. You can also combine an external data source with the templates to provide extended criteria for determining group membership.

NOTE Settings related to Dynasty membership are configured at the identity store level. See Membership settings on page 89 and Dynasty settings on page 138.

NOTE Do not move a Dynasty from one domain to another. Child Dynasties would get orphaned and subsequently deleted.

You cannot create mail-enabled Dynasties of the Office 365 group type in a Microsoft Azure based identity store, since an Office 365 group cannot have groups as its members. Only non mail-enabled Dynasties of the security group type are supported.

Naming conventions for child Dynasties

Dynasty names help you group a parent Dynasty with its respective child Dynasties.

- For an organizational/geographical/custom Dynasty:
  The name of a child Dynasty starts with the name of its parent Dynasty (unless you change the naming template for Dynasty children).
- For a managerial Dynasty:
  By default, the naming template for its child Dynasties starts with "Direct reports of <manager>".

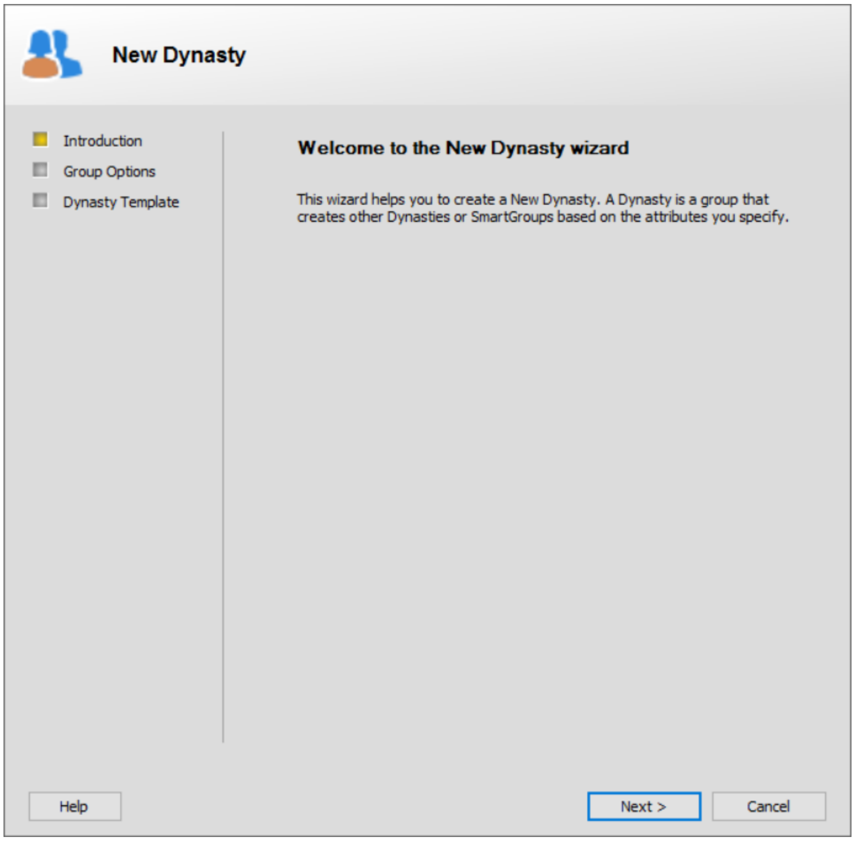
To modify the display name template for child Dynasties, see Modify alias and display name structure on page 136.

NOTE In the Dynasty creation/update process, a child Dynasty will not be created if it bears the same name as that of an existing object in the directory. For example, when you create a custom Dynasty, test1, on only one attribute, SamAccountName, it’s child Dynasties would be named as test1-Robert, test1-John, and so on. However, if test1-Robert already exists as a user object, GroupID will skip the test1-Robert child Dynasty and continue to create the rest of the Dynasty.

Create a Organization/Geographical/Custom Dynasty

1. In GroupID Management Console, select **Automate** > right-click **All Groups** > **New** > **Dynasty**.

   The **New Dynasty** wizard opens to the **Welcome** page.



Welcome to the New Dynasty wizard

This wizard helps you to create a New Dynasty. A Dynasty is a group that creates other Dynasties or SmartGroups based on the attributes you specify.

Figure 73: Welcome page

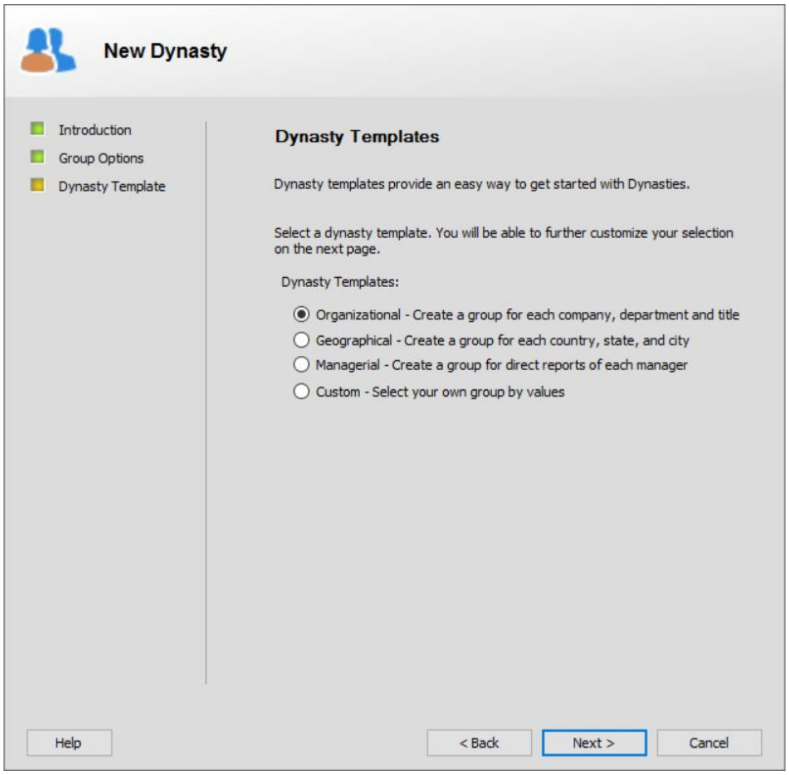
2. Read the welcome message and click **Next**.

3. The **Group Options** page is similar to the **Group Options** page for a static group (Figure 25).

   For an Azure based identity store, the **Group Options** page is as shown in **Error! Reference source not found.**. For a Dynasty, however, the **Create O ffice 365 Group** check box is not available because an Office 365 group cannot have groups as its members.

   Follow the instructions under the figures to specify group options for the Dynasty and click **Next**.

4. Automate provides several Dynasty templates to help kick-start the Dynasty. On the **Dynasty Templates** page, select a template for the Dynasty. Regardless of the template you select, you will still be able to modify the Dynasty structure to best suit your organization’s requirements.



Dynasty Templates

Dynasty templates provide an easy way to get started with Dynasties.

Select a dynasty template. You will be able to further customize your selection on the next page.

Dynasty Templates:

- ● Organizational - Create a group for each company, department and title
- ○ Geographical - Create a group for each country, state, and city
- ○ Managerial - Create a group for direct reports of each manager
- ○ Custom - Select your own group by values

Figure 74: Dynasty Templates page

5. Select the **Organizational**, **Geographical**, or **Custom** template to create the Dynasty.

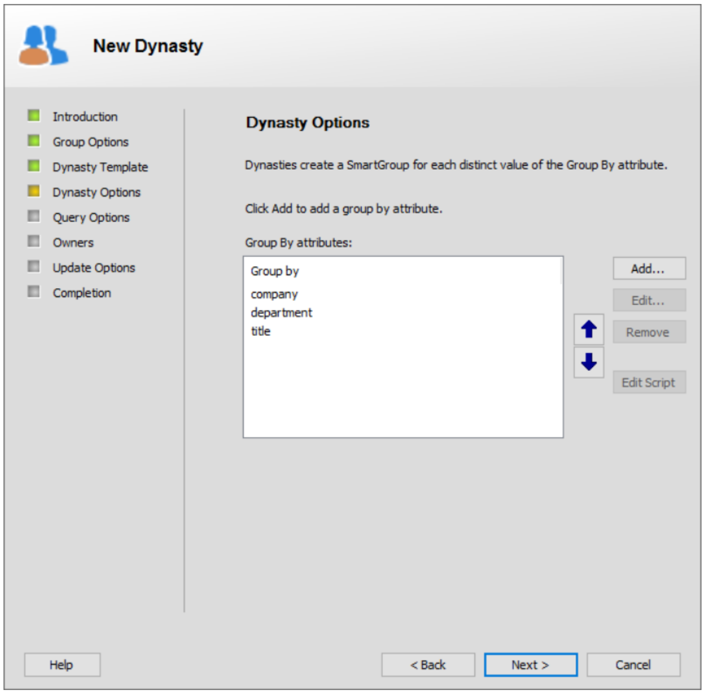
   - Select **Organizational** to create a group for every distinct company, then for each department within a company, and finally for each title in a department.

     In a Microsoft Azure based identity store, an organizational Dynasty creates a group for every distinct company location, then for each department within a company location, and finally for each job title in a department.

   - Select **Geographical** to create a group for every distinct country, then for each state within a country, and finally for each city within a state.

   - Select **Custom** to begin with a blank group and select your own group-by attributes.

6. Click **Next**.
   The **Dynasty Options** page is displayed:



Dynasty Options

Dynasties create a SmartGroup for each distinct value of the Group By attribute.

Click Add to add a group by attribute.

Group By attributes:

Group by
company
department
title

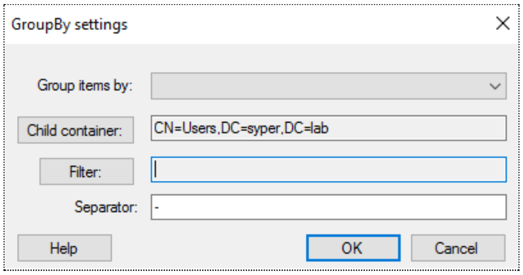
Figure 75: Dynasty Options page

Dynasties create Smart Groups for each distinct value of each Group-By attribute. Depending on the Dynasty template selected, the **Group-By attributes** area displays the list of default group-by attributes for the template; however, you can add and remove attributes. For the **Custom** template, no attribute is displayed.

For example, if you specify the Country, State, and City attributes, Automate creates a group for every distinct country value, then for each state within a country, and finally for each city in a state.

- Click **Add** to specify a group-by attribute.
- Click **Edit** to edit the selected group-by attribute options.
- Click **Remove** to remove the selected group-by attribute.

7. To add more group-by attributes to those displayed in the **Group By attributes** list, click **Add**.



Group items by:

Child container: CN=Users,DC=syper,DC=lab

Filter:

Separator: -

Figure 76: Group-by Settings dialog box

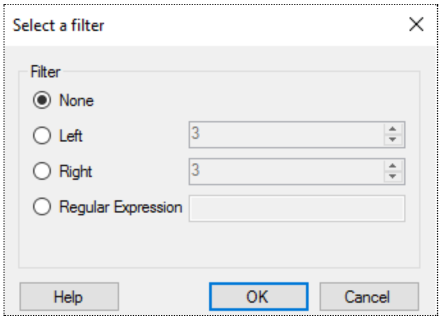
a. In the **Group items by** list, type or select the field (attribute) to use for expanding the Dynasty. Automate creates a child group for each unique value of this field.

b. The **Child container** box displays the container where new child groups will be created. If this setting is blank, the container in which the parent Dynasty resides is used for creating child groups.

   To change the container, click the **Child container** button and select a new container.

c. You can select additional group-by filters for greater control over the values used to create children.

   Click **Filter**; the **Select a filter** dialog box is displayed:



Left: 3

Right: 3

Figure 77: Select a filter dialog box

The Group-By filter is used to strip out values from Dynasties by allowing you to collapse several values into one.

An example is populating the Office field with the building/office number, thus conveniently storing two items of related data in the same field. Now, suppose you need a distribution list for each building. If the building name was in its own field (custom attribute 1), you could create a Dynasty that groups by the custom attribute 1 field and Automate would then create a group for each building value.

Attribute value:
Custom Attribute 1 = MacArthur Plaza

Sample groups created by Automate Dynasty:
Everyone in MacArthur Plaza

However, if you were to create a Dynasty that groups by the Office field (which contains both the building name and office number), Automate will create a group for each distinct building/office value. This strategy gives you a group for every office number, rather than for each building.

Attribute value:
Office = MacArthur Plaza/1256C

Sample groups created by Automate Dynasty:
Everyone in MacArthur Plaza/1256C

The Group-By filter solves this problem by allowing you to filter out unwanted permutations of values.

On the **Select a filter** dialog box (Figure 77), select one of the following filters and click **OK**:

- **None** – Do not apply any filter. Simply create a group for each distinct value of the attribute selected in the **Group items by** list. For example, distinct values for the 'department' attribute might be *Engineering*, *Marketing*, and *Finance*.
- **Left** – Select a portion of the group-by attribute starting from the left for the number of characters specified in the **Left** box, and create a group for each distinct value of the portion of the attribute selected.
- **Right** – Select a portion of the group-by attribute, starting from the right for the number of characters specified in the **Right** box, and create a group for each distinct value of the portion of the attribute selected.
- **Regular Expression** - A group is created for each distinct value as per the given regular expression.

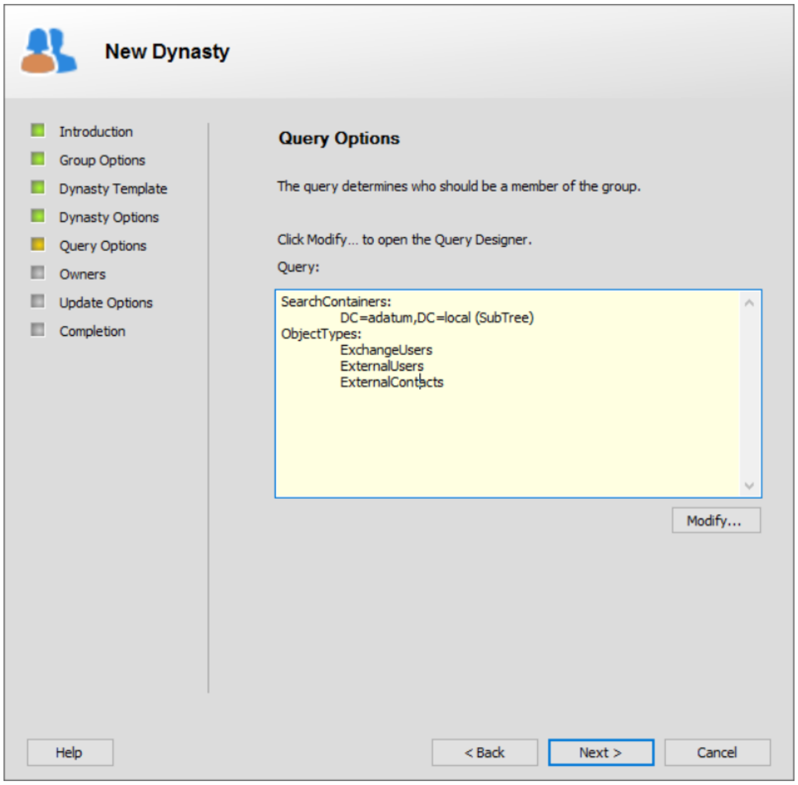
d. Each group-by level can have a separator. In the **Separator** box, enter a separator character to use in both the display name and alias of child groups to separate the group-by values.

e. Click **OK** to close the **Group-by Settings** dialog box.

8. The **Edit Script** button is disabled on the **Dynasty Options** page (Figure 75), so you cannot write a script to customize the behavior of the options on this page. After the Dynasty is created, use the **GroupID** tab (Figure 44) in group properties to access the **Dynasty Options** dialog box (Figure 84), where you can write a script.

   NOTE This scripting feature is only available for parent Dynasties. Child Dynasties inherit the script.

9. Click **Next**.
   The **Query Options** page is displayed.



Query Options

The query determines who should be a member of the group.

Click Modify... to open the Query Designer.

Query:

```
SearchContainers:
        DC=adatum,DC=local (SubTree)
ObjectTypes:
        ExchangeUsers
        ExternalUsers
        ExternalContacts
```

Figure 78: Query Options page

This page displays the default query that Automate will use to determine the Dynasty membership. The default query returns all users with Exchange mailboxes, along with users and contacts with external email addresses, which are then grouped by the specified group-by attributes. You can modify this query to limit the number of results, if required.

For a Dynasty in an Azure based identity store, the default query returns all users and groups.

Dynasties in an Azure based identity store use a device structured query language while those in an Active Directory based identity store use LDAP queries to retrieve group membership.

You can combine an external data source with the group-by attributes to add an extra filter, so that the query filters objects matching the values of the data source while determining the membership of child groups. For example, if you want to create an organizational Dynasty for all employees whose first names and last names are present in an external data source, you can select that data source and map a key field with a directory field. When Dynasty membership is updated, it will filter only those users from the directory whose first names and last names match with the data source.

Use the **Advanced** tab (Figure 98) of the **Query Designer** dialog box to select the data source and configure the connection settings.

10. To modify the query, click **Modify**; this launches the **Query Designer** dialog box (Figure 88), where you can edit the query.

    You can import or export a query from within the **Query Designer** dialog box using the **File > Import Query** or **File > Export Query** command on the main menu.

11. Click **Next**.

12. The **Owners** page is similar to the **Owners** page for a static group (Figure 26). Follow the instructions under the figure to assign primary and additional owners to the Dynasty and click **Next**.

    NOTE Additional owners are only set for the parent and are not inherited by child Dynasties during update.

13. The **Update Options** page is similar to the **Update Options** page for a Smart Group (Figure 34). Follow the instructions under the figure to specify when you want to update the membership of the Dynasty and click **Next**.

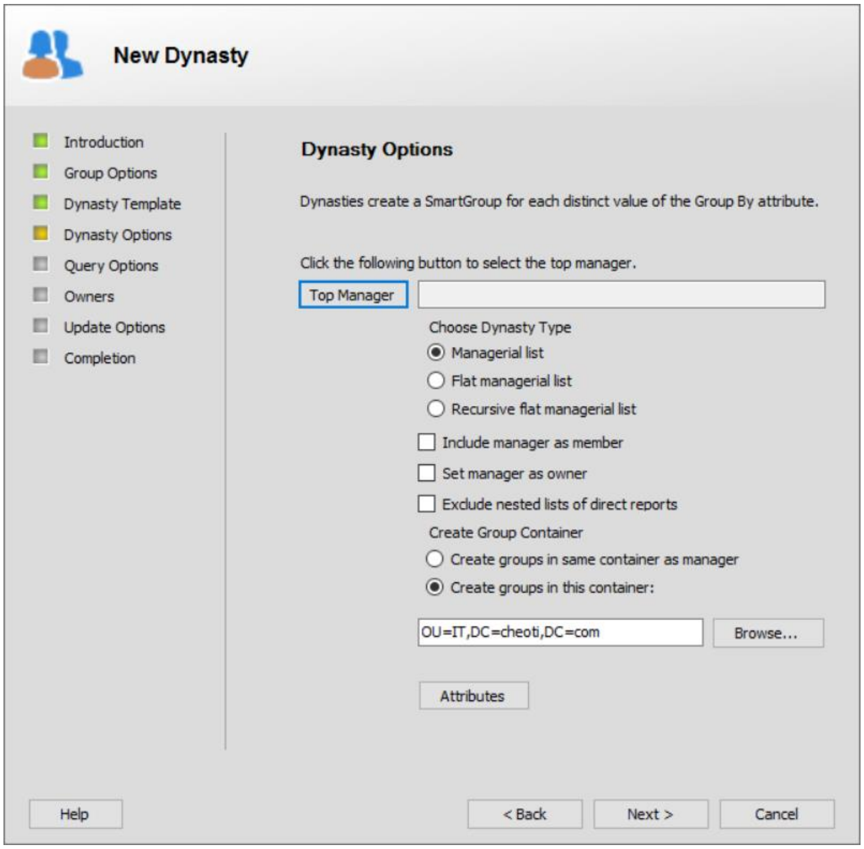
14. The **Completion** page is similar to the **Completion** page for a Smart Group (Figure 35). Follow the instructions under the figure to create the Dynasty.

Create a Managerial Dynasty

1. To create a Dynasty using the Managerial template, follow the instructions under Create a Organization/Geographical/Custom on page 115, until you reach the **Dynasty Templates** page (Figure 74) of the wizard.

2. Select the **Managerial** option to create a managerial Dynasty.

3. Click **Next**.
   The **Dynasty Options** page is displayed:



Dynasty Options

Dynasties create a SmartGroup for each distinct value of the Group By attribute.

Click the following button to select the top manager.

Top Manager

Choose Dynasty Type

● Managerial list
○ Flat managerial list
○ Recursive flat managerial list

□ Include manager as member
□ Set manager as owner
□ Exclude nested lists of direct reports

Create Group Container

○ Create groups in same container as manager
● Create groups in this container:

OU=IT,DC=cheoti,DC=com   Browse...

Attributes

Figure 79: Dynasty Options page for Managerial Dynasty

4. Click the **Top Manager** button; the **Find** dialog box (Figure 46) is displayed, where you can search and select the top-level manager, and thus, the starting point for the Dynasty.

5. Select an option button for **Choose Dynasty Type** to specify the type of managerial Dynasty you want to create.

   - **Managerial List**

     Construct a managerial Dynasty structure by first creating a Smart Group containing all direct reports of the top-level manager as members, then creating separate Smart Groups for the direct reports (with their respective direct reports as members). This Dynasty structure continues till a Smart Group is created for all managers and sub-managers with their respective direct reports as members.

     Example:

     Take the following data set:

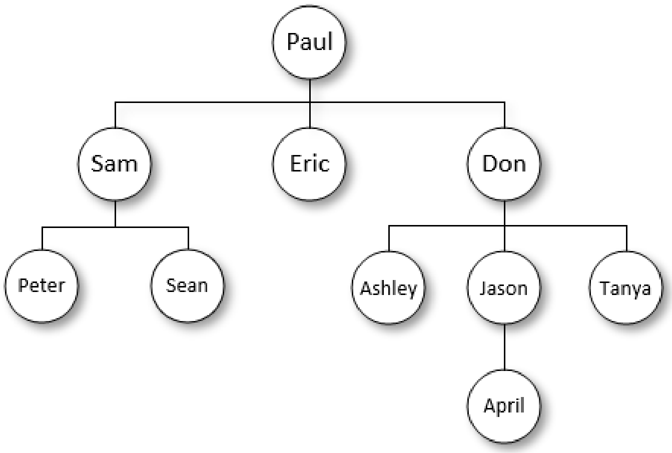


Figure 80: Data Set for Managerial Dynasty

- Paul is the top manager with three direct reports: Sam, Eric and Don.
- Sam has two direct reports, Peter and Sean.
- Eric has no direct report.
- Don has three direct reports: Ashley, Jason and Tanya.
- Jason has a direct report, April.

Automate would create a Dynasty with the following child groups:

- Direct reports of Paul
  Members: Sam, Eric, Don
- Direct reports of Sam
  Members: Peter, Sean
- Direct reports of Don
  Members: Ashley, Jason, Tanya
- Direct reports of Jason
  Members: April

- **Flat managerial list**

  A flat managerial list is one in which all direct reports of the top manager and sub-level managers are added as members of a single group; no separate groups are created for different levels of managers.

  With the data set shown in Figure 80, a flat managerial list would consist of one Smart Group for Paul, with all users as members.

  On selecting this option button, some options on this page get disabled since they do not apply to a flat managerial list.

- **Recursive flat managerial list**

  Use a recursive flat managerial list to create a Smart Group for each manager and sub-manager. For members, each group would contain the respective manager's direct reports, the direct reports of those direct reports, thus continuing till the nth level.

  With the data set shown in Figure 80, the following child groups will be created:

  - Direct reports of Paul
    Members: Sam, Eric, Don, Peter, Sean, Ashley, Jason, Tanya, April
  - Direct reports of Sam
    Members: Peter, Sean
  - Direct reports of Don
    Members: Ashley, Jason, Tanya, April
  - Direct reports of Jason
    Members: April

  On the **Query Options** page (Figure 82), you can also specify a criterion to filter the managers for whom you want to create child groups in the Dynasty.

6. Select the **Include manager as member** check box to include the manager as a member of their groups along with their direct reports. With this check box selected, the manager receives a copy of any email sent to the direct reports group.

   By default, this check box is not selected, indicating that the manager of each level of direct reports is not included in their respective group.

7. Select the **Set Manager as owner** check box to set the top manager as the primary owner of the parent Dynasty.

   On the **Owners** page of the wizard, the top manager would be displayed as the primary owner. If you change it, the new recipient would be the owner, even with the **Set manager as owner** check box selected.

   In case the Dynasty is not a flat managerial Dynasty, the manager of each child Dynasty will be set as its respective owner.

8. For a hierarchical managerial Dynasty, by default, the Dynasty structure adds a sub-level manager's Smart Groups in the membership of the top-level manager's Smart Groups. Select the **Exclude nested lists of direct reports** check box to exclude them from the membership.

9. Specify a container for creating child groups. Options are:

- **Create groups in same container as manager**, to create groups in the same container where the top-level manager resides.
- **Create groups in this container**, to specify a container or organizational unit for the child groups to be created in.

10. You can create a managerial Dynasty based on any attribute.

    Click the **Attributes** button to set a custom attribute, such as the XAdditonalManager attribute, to create a managerial lineage in the context of this attribute.

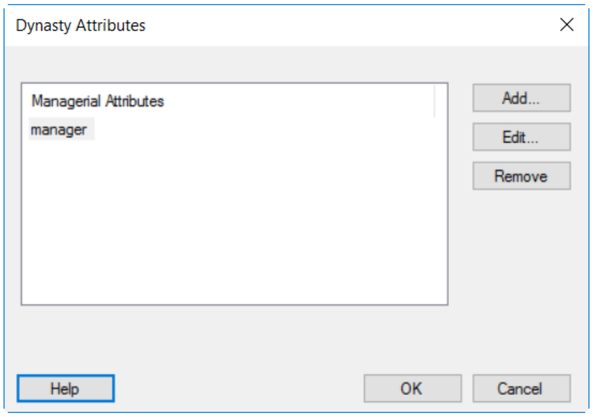


Figure 81: Dynasty Attributes dialog box

By default, the 'Manager' attribute is selected to create a managerial lineage. This attribute involves the collaboration of two attributes: *manager* and *direct reports*, to create the Dynasty's hierarchal structure.

- To add another attribute, click **Add** and select the required attribute.
- To remove an attribute, select it and click **Remove**.
- To replace an attribute, select it and click **Edit**. Select another attribute as a replacement and click **OK**.

Some examples of a managerial Dynasty with a different set of attributes are given below:

Specify the 'XadditionalManager' attribute in addition to the 'Manager' attribute to create a managerial lineage

(Here 'Manager' is the primary attribute to create the managerial lineage.)

You select a top manager to create the Dynasty. The managerial hierarchy for this manager in a provider (such as Active Directory) is as follows:

Top manager: Alan
Alan is the manager of John, Jane, and Josephine
John is the manager of Mark and Martin

Mark is the manager of Sophia and Martin is the manager of Sarah
John is also the additional manager of Sophia and Sarah

When the Dynasty is updated:

- ‘TestManagerial1’ is the parent Dynasty with child Dynasties such as:
    - Direct reports of John
    - Direct reports of Mark
    - Direct reports of Martin
    - Direct reports of Sophia
      (This child Dynasty will be a part of the Direct reports of John and Direct reports of Mark, since John is the additional manager and Mark is the primary manager.)
    - Direct reports of Sarah
      (This child Dynasty will be a part of the Direct reports of Martin.)

If no user is set as additional manager, no child Dynasty will be created with the additional manager attribute.

Specify a single attribute, ‘XadditionalManager’, to create a managerial lineage

Suppose the managerial hierarchy for the top manager in a provider (such as Active Directory) is as follows:

Top manager: Alan
Alan is the additional manager of John, Jane, and Josephine
John is the additional manager of Mark and Martin
Mark is the additional manager of Sophia and Martin is the additional manager of Sarah

When the Dynasty is updated:

- ‘TestManagerial1’ is the parent Dynasty with child Dynasties such as:
    - Direct reports of John
    - Direct reports of Mark
    - Direct reports of Martin

When Alan is not the additional manager of any user, the parent Dynasty would be created without any child Dynasties.

Specify a custom attribute, ‘customattribute1’ to create a managerial lineage

Let’s take employeeID as the custom attribute. Data will be as:

Top manager: Alan with EmployeeId 1
John (EmpID: 2, CA: 1); Jane (EmpID: 3, CA: 1); Josephine (EmpID: 4, CA: 1)
Mark (EmpID: 5, CA: 2); Martin (EmpID: 6, CA: 2)
Sophia (EmpID: 7, CA: 5); Sarah (EmpID: 8, CA: 6)

When the Dynasty is updated:

- ‘TestManagerial1’ is the parent Dynasty with child Dynasties such as:
  - Direct reports of John (having Mark and Martin)
  - Direct reports of Mark (having Sophia)
  - Direct reports of Martin (having Sarah)

Specify multiple attributes – ‘Manager’, ‘XadditionalManager’ and ‘customattribute1’ - to create a managerial lineage

Direct reports for users created with respect to additional manager and custom attribute 1 are added in their respective managers and additional managers according to the custom attribute 1 data.

11. Click **Next**.

12. The **Query Options** page (Figure 78) displays the default query that Automate will use to determine the Dynasty membership. The default query returns all users with Exchange mailboxes, along with users and contacts with external email addresses, which are then grouped as per the managerial Dynasty structure. You can modify this query to limit the number of results, if required.

    For a Dynasty in an Azure based identity store, the default query returns all users and groups.

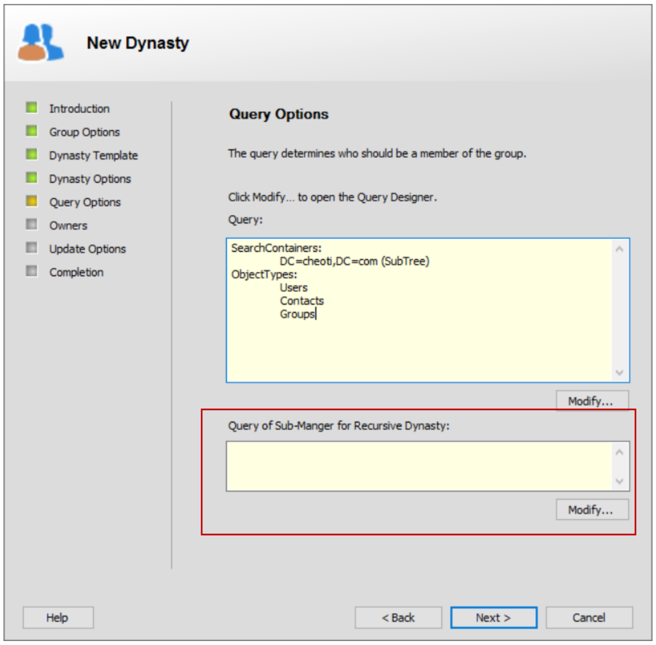
    You can combine an external data source with the manager-related attributes to add an extra filter, so that the query filters objects matching the values of the data source while determining the membership of child groups. For example, if you want to create a managerial Dynasty with all managers whose names are present in an external data source, you can select that data source and map a key field with a directory field. When Dynasty membership is updated, it will filter only those managers from the directory whose names match with the data source, and create a managerial hierarchy.

    Use the **Advanced** tab (Figure 98) of the **Query Designer** dialog box to select the data source and configure the connection settings.

13. To modify the query, click **Modify**; this launches the **Query Designer** dialog box (Figure 88), where you can edit the query.

You can import or export a query from within the **Query Designer** dialog box using the **File > Import Query** or **File > Export Query** command on the main menu.

14. If you have selected the **Recursive flat managerial list** option on the **Dynasty Options** page (Figure 79), the **Query of Sub-Manager for Recursive Dynasty** area is displayed on the **Query Options** page. It is as:



Query Options

The query determines who should be a member of the group.

Click Modify... to open the Query Designer.

Query:

```
SearchContainers:
        DC=cheoti,DC=com (SubTree)
ObjectTypes:
        Users
        Contacts
        Groups
```

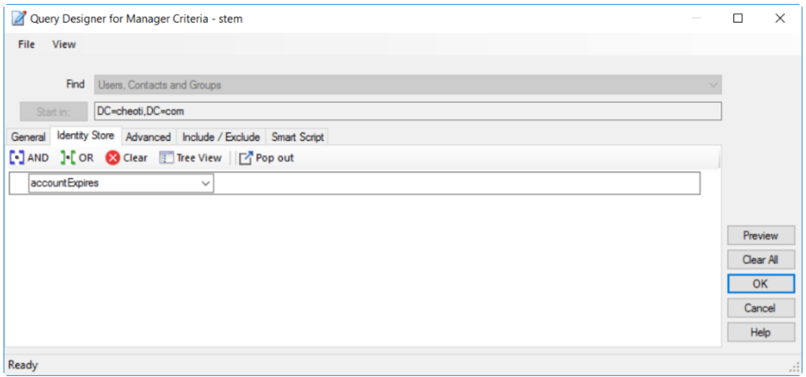
Query of Sub-Manger for Recursive Dynasty:

Figure 82: Query Options page for Recursive Managerial Dynasty

For a recursive flat managerial Dynasty, by default, a child group is created for each manager and sub-manager in the organization.

You can apply a filter to create child groups for specific managers and sub-managers.

a. Click **Modify** in the **Query of Sub-Manager for Recursive Dynasty** area; the **Query Designer for Manager Criteria** dialog box is displayed.



Find: Users, Contacts and Groups

Start in: DC=cheoti,DC=com

accountExpires

Ready

Figure 83: Query Designer for Manager Criteria

This dialog box inherits all settings from the **Query Designer** dialog box. Only the Identity Store tab is different, where you can specify a criterion for manager selection.

b. Select an attribute from the first list. For example, to search for managers who reside in the US, select the countryCode attribute.

c. The Condition list is displayed when you select an attribute. From here, select the condition that you want to apply to the selected attribute. This condition works with the Attribute and Value fields to identify search results. The available conditions are discussed in Table 12.

d. Specify a value for the attribute in the Value box. The query will return results considering the specified criteria (attribute, condition, value).

The Value box is not available for non-comparison operators, such as *Present* or *Not Present*. Non-comparison operators only check whether the value for the selected field exists and return either TRUE or FALSE.

When the value is a date, use the mm/dd/yyyy format.

e. You can add multiple criteria to your query and apply the following operators:

AND

Click this button after selecting two or more records to insert a logical AND to the selected criteria.

To select a record, click the arrow icon next to it and click **Select Row**.

OR

Click this button after selecting two or more records to insert a logical OR to the selected criteria.

f. You can also do the following:

- Clear Click this button to clear the displayed criteria.
- Tree View Displays a hierarchal view of the added criteria.
- Pop out Displays the criteria in a new window.

g. After specifying a query, click **OK**.
The criterion is displayed in the **Query of Sub-Manager for Recursive Dynasty** area on the **Query Options** page (Figure 82).

15. Click **Next**.

16. The **Owners** page is displayed, which is similar to the **Owners** page for a static group (Figure 26). Follow the instructions under the figure to assign

primary and additional owners to the Dynasty and click **Next**.

If you selected the **Set Manager as owner** check box on the Dynasty Options page (Figure 79), the top manager would be displayed as the primary owner instead of the logged-in user.
In case you change the owner, the new recipient would be the Dynasty's primary owner even if the **Set Manager as owner** check box is selected.

For a Dynasty in an Azure based identity store, when the **Set Manager as owner** check box is selected, both the top manager and the logged-in user would be set as primary owners, since Azure supports multiple primary owners for a group.

In either case, when an additional owner is promoted as the primary owner, it is removed from the list of additional owners.

17. The **Update Options** page is displayed, which is similar to the **Update Options** page for a Smart Group (Figure 34). Follow the instructions under the figure to specify when you want to update the membership of the Dynasty and click **Next**.
18. The **Completion** page is displayed, which is similar to the **Completion** page for a Smart Group (Figure 35). Follow the instructions under the figure to create the Dynasty.

Dynasty options

Automate provides advanced options that you can use to enhance the Dynasty structure and its membership. You can modify the group-by attributes for the Dynasty, edit the template used to generate the alias and display names of child groups, and control the attribute inheritance behavior.

Advanced Dynasty options are available for Dynasties of the parent and middle level, but not for the leaf level.

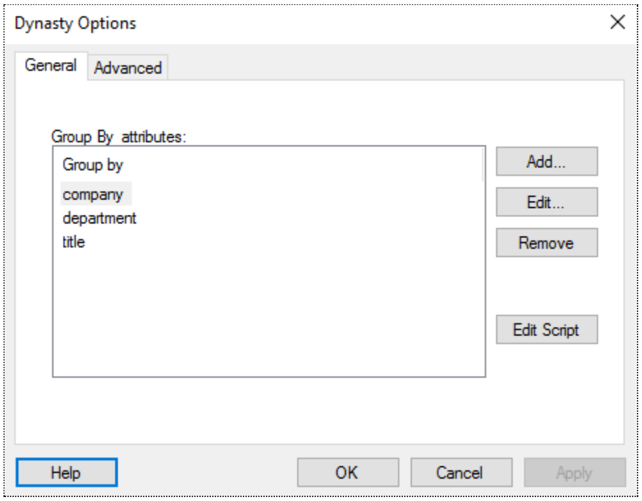
Manage Group-by attributes for an Organizational/Geographical/Custom Dynasty

When you create an organizational, geographical or custom Dynasty, you provide group-by attributes that determine the Dynasty's structure, i.e., they determine how query results are grouped and the order child groups should be created in.

For example, if you group results by the country, state, and city attributes in that order, Automate creates a group for each value of country, then state and finally city that it finds in the query results.

You can view and change these group-by attributes for parent and middle Dynasties. Your changes will be reflected on the next update of the Dynasty.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required organizational/geographical/custom Dynasty and select **Properties**.
3. On the group properties dialog box, click the **GroupID** tab (Figure 44).
4. In the **Advanced** area, click **Options**.
   The **Dynasty Options** dialog box is displayed:

   Group By attributes:

   Group by
   company
   department
   title

   Figure 84: Dynasty Options – General tab

   Options available on the **General** tab are the same as available on the **Dynasty Options** page (Figure 75) of the New Dynasty wizard. Follow the instructions under the figure to modify the group-by attributes.
5. Click the **Edit Script** button to launch the **Script Editor** (Figure 116) to write or modify scripts for customizing the default behavior of the options available on this tab.

   NOTE This scripting feature is only available for parent Dynasties. Child Dynasties inherit the script.
6. After making the required changes, click **OK**.

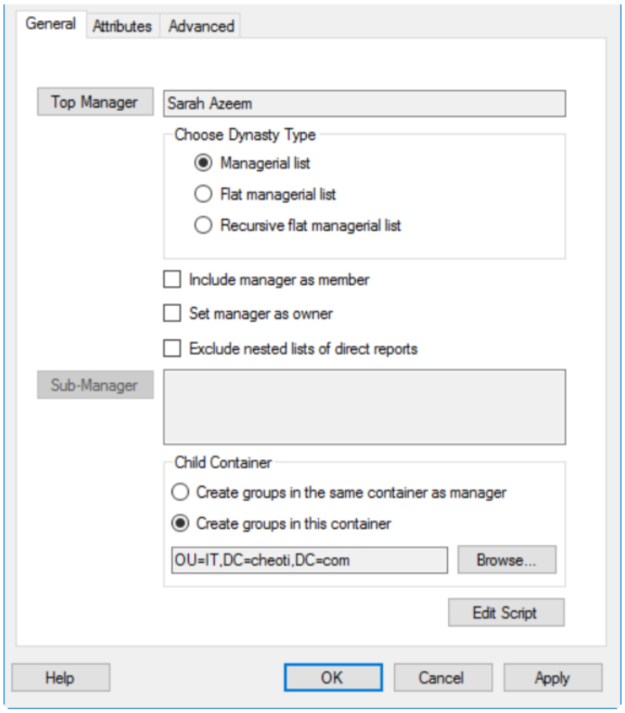
Manage Managerial Dynasty structure

When you create a managerial Dynasty, you specify a Dynasty structure that determines how query results are grouped.

For example, you specify whether you want to create separate Smart Groups for the direct reports of the top manager and sub-level managers, or add all direct reports of the top manager and sub-level managers as members of a single group.

You can view and change these structure options for parent and middle Dynasties. Your changes will be reflected on the next update of the Dynasty.

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required managerial Dynasty and select **Properties**.
3. On the group properties dialog box, click the **GroupID** tab (Figure 44).
4. In the **Advanced** area, click **Options**.
   The **Dynasty Options** dialog box is displayed:



Top Manager: Sarah Azeem

Choose Dynasty Type

● Managerial list
○ Flat managerial list
○ Recursive flat managerial list

□ Include manager as member
□ Set manager as owner
□ Exclude nested lists of direct reports

Child Container

○ Create groups in the same container as manager
● Create groups in this container

OU=IT,DC=cheoti,DC=com

Figure 85: Dynasty Options – General tab for managerial Dynasty

Options available on the **General** tab are the same as available on the **Dynasty Options** page (Figure 79) of the New Dynasty wizard. Follow the instructions under the figure to make the required changes.

When you clear the **Set manager as owner** check box here, the manager set as the primary owner of a parent Dynasty will not be removed. However, when the Dynasty is updated, the primary owner of a child Dynasty may be updated, depending on the Dynasty inheritance options.

For example, if the **Always inherit selected attributes** option is selected (Figure 86) and the *managedBy* attribute is set for inheritance, the primary owner of the parent Dynasty would be set as the primary owner for all child Dynasties, replacing their respective primary owners.

When you clear the **Set manager as owner** check box for a Dynasty in an Azure based identity store, the primary owner of the parent Dynasty and the manager of the child Dynasty are collectively set as primary owners of the child Dynasty.

5. The **Sub-Manager** area is enabled when the Dynasty is a *Recursive flat managerial list*.

   For this Dynasty, a child group is created for each manager and sub-manager in the organization by default.

   You can apply a filter to create child groups for specific managers and sub-managers.

   Click the **Sub-Manager** button; the Q**uery Designer for Manager Criteria** dialog box (Figure 83) is displayed. Follow steps b-f below the figure to specify a criterion for manage selection and click **OK**.

6. Click the **Edit Script** button to launch the **Script Editor** (Figure 116) to write or modify scripts for customizing the default behavior of the options available on this tab.

   This scripting feature is only available for parent Dynasties. Child Dynasties inherit the script.

7. Click the **Attributes** tab.
   This tab is the same as shown in Figure 81. The scenarios discussed under the figure also apply here. For example:

   Specify the 'XadditionalManager' attribute in addition to the 'Manager' attribute for a parent managerial Dynasty

   On update, new child Dynasties are created with respect to the additional manager attribute data and added in their respective managers' direct reports and additional manager's direct reports.

   Remove the 'XadditionalManager' attribute for a parent managerial Dynasty

   On update, the direct reports of users created with respect to the additional manager attribute data are removed from their respective managers' and additional managers' direct reports.

If the Delete Empty and Orphan Dynasty children setting is applied, direct reports of users created due to the additional manager attribute data are not only removed from their respective managers' and additional managers' direct reports; they also get deleted.

8. After making the required changes, click **OK**.

Set attributes inheritance

At the identity store level, the administrator can specify a list of attributes whose values are inherited by Dynasty children from the parent. See Dynasty settings on page 138.

By default, child Dynasties inherit these attributes' values only when these child Dynasties are created. You can change this setting for a parent Dynasty to allow children to inherit attributes' values whenever the parent Dynasty is updated. You can even opt to omit the inheritance of attribute values to child Dynasties.

To update Dynasties, see Update Smart Groups and Dynasties on page 60.

Modifying inherited attribute values

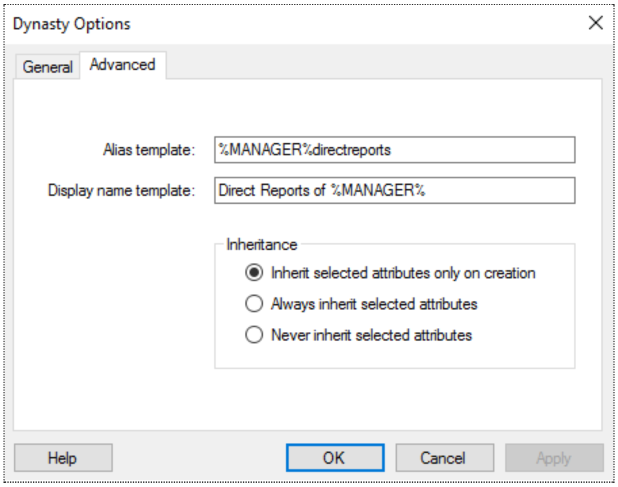
When, for a child Dynasty, you change the value of an inherited attribute, the new value may or may not persist, depending on the inheritance option selected for the parent Dynasty. Here is an example:

Suppose the administrator has set the managedBy attribute for inheritance.

- With the **Always inherit selected attributes** option selected for the parent Dynasty, any modifications made to the value of the managedBy attribute for a child Dynasty will be replaced with the value of the managedBy attribute set for the parent Dynasty, whenever the Dynasty is updated.
- With the **Never inherit selected attributes** option selected, any modifications made to the value of the managedBy attribute for a child Dynasty will persist after update.

To set an inheritance option:

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required Dynasty and select **Properties**.
3. On the **GroupID** tab (Figure 44), click **Options** in the **Advanced** area.
4. On the **Dynasty Options** dialog box, click the **Advanced** tab.



Alias template: %MANAGER%directreports

Display name template: Direct Reports of %MANAGER%

Inheritance

● Inherit selected attributes only on creation

○ Always inherit selected attributes

○ Never inherit selected attributes

Figure 86: Advanced tab

5. In the **Inheritance** area, select the required inheritance option:

   - **Inherit selected attributes only on creation**: Dynasty children will inherit the attributes' values only when the Dynasty is created. Moreover, whenever a new child group is created, it will inherit the attributes' values.
   - **Always inherit selected attributes**: Dynasty children will inherit the attributes' values every time the parent Dynasty is updated.
   - **Never inherit selected attributes**: Dynasty children will never inherit attribute values from the parent.

6. Click **OK**.

Your changes will be reflected on the next update of the Dynasty.

Modify alias and display name structure

You can provide a convention for generating the aliases and display names of Dynasty children. This convention is referred to as 'template'.

The default alias and display name templates for different Dynasties are as follows:

Dynasty Type	Alias Template	Display Name Template
Organizational, Geographical, Custom	DynastyName%GROUPBY%	DynastyName%GROUPBY%
Managerial	%MANAGER%directreports	Direct reports of %MANAGER%

Table 7: Default templates for alias and display name

1. In GroupID Management Console, select **Automate > [required group node]**.
2. In the groups list, right-click the required Dynasty and select **Properties**.
3. On the **GroupID** tab (Figure 44), click **Options** in the **Advanced** area.
4. On the **Dynasty Options** dialog box, click the **Advanced** tab (Figure 86).
5. To update the alias template, type the new template in the **Alias template** box. This setting is used to generate the alias names of the Dynasty's child groups.

    - For an organizational/geographical/custom Dynasty, **%GROUPBY%** is replaced with the actual value of the **Group items by** field (this field is available on the **GroupBy Settings** dialog box - Figure 76).
    - For a managerial Dynasty, **%MANAGER%** is replaced with the alias of the manager. Normally, the mailnickname attribute is used to store the alias. However, if this attribute is not set, then **%MANAGER%** is replaced with the display name of the manager.

      To use an attribute other than mailNickname for generating the alias for child groups, update the **%MANAGER%** statement with the desired attribute name. Note that the value of the attribute must be unique.

      Example using the cn attribute:
      %MANAGER.cn%

      Example using the name attribute:
      %MANAGER.name%

    If Exchange Server is the designated messaging system for the identity store, then the alias length is limited to 64 characters and must be unique to the forest. For other messaging systems, the alias length must not exceed the number of characters supported by the respective messaging system.

    Also, the alias must not contain characters that are invalid for the configured messaging system. Table 2 lists the valid characters for the supported messaging systems.

6. To update the display name template, type the new template in the **Display name template** box. This template is used to generate the display names of the Dynasty's child groups.

    - For an organizational/geographical/custom Dynasty, **%GROUPBY%** is replaced with the actual value of the **Group items by** field (this field is available on the **GroupBy Settings** dialog box - Figure 76).
    - For a managerial Dynasty, **%MANAGER%** is replaced with the display name of the manager. To use an attribute other than displayName to

name the child groups, update the **%MANAGER%** statement with the desired attribute name. Note that the value of the attribute must be unique.

Example using the cn attribute:
%MANAGER.cn%

Example using the name attribute:
%MANAGER.name%

7. Click **OK**.

NOTE For a managerial Dynasty, the **%MANAGER%** variable for the alias and display name templates must be the same. The selected attribute must be a string and cannot include characters that are not supported in pre-Windows 2000 group names.

Your changes will be reflected on the next update of the Dynasty.

Dynasty settings

The administrator can specify the following to control how Automate processes the Dynasties in an identity store:

Update child Dynasties automatically with parent

By default, child Dynasties are updated when the parent Dynasty is updated. However, the administrator can enable a setting that does not update Dynasty children with the parent. In this case, each child group would have to be updated like a single Smart Group.

Delete empty and orphan Dynasty children automatically

An empty child Dynasty is one with no member and an orphan child Dynasty is one whose parent Dynasty has been removed.

By default, empty and orphan Dynasty children are automatically deleted from the identity store. However, if the administrator disables this setting, these children will not be deleted automatically.

Specify the attributes Dynasty-created children inherit from the parent

The administrator can control the attributes that a child Dynasty inherits from its parent. By default, the values of the following attributes are passed on from the parent to child Dynasties:

Attribute	Description
managedBy	Contains information about the group's primary owner.
unauthOrig	Contains the list of DNs of users who do not have permissions to send email to the group.
authOrig	Contains the list of DNs of users who have permissions to send email to the group.
dLMemRejectPerms	Contains the DNs of groups that do not have permissions to send email to the group.
dLMemSubmitPerms	Contains the DNs of groups that have permissions to send emails to the group.
delivContLength	Contains the maximum limit for incoming messages to the group.

Table 8: Default attributes for inheritance

The administrator can add or remove attribute from this list.

At the Dynasty level, however, you can specify whether values of the specified attributes should be inherited by children in the first place, and if yes, then whether it should be a one-time or recurring inheritance. See Set attributes inheritance on page 135.

If, for a managerial Dynasty, the 'Set manager as owner' check box is selected, the **Always inherit selected attributes** option is selected (Figure 86), and the managedBy attribute is set for inheritance, the following applies to child Dynasties:

- The 'Set manager as owner' option takes priority over the managedBy attribute inheritance. Hence, the manager of a child Dynasty would be set as its respective primary owner.
- In an Azure based identity store, where a group can have multiple primary owners, the owner of the parent Dynasty and the manager of the child Dynasty are collectively set as primary owners of the child Dynasty.

Chapter 10 - Query Designer

The Query Designer enables you to create queries for Smart Groups and Dynasties. These queries provide a quick and consistent way to retrieve directory objects on which you want to perform specific tasks. For example, you can construct a query to retrieve all users having mailboxes on an Exchange Server or you can build a query to retrieve all directory objects whose information is present in an external data source, such as Microsoft SQL Server.

The **Query Designer** dialog box provides a visual interface for designing queries, so that you do not have to write the commands. Its preview feature returns the results for the query before you commit them to the directory.

The **Query Designer** dialog box groups similar query options by tabs. Settings that are not grouped in tabs are global; they apply to all tabs.

- General tab: lets you select object categories that you want the query to search in.
- Password Expiry Options tab: this tab is only available for Smart Groups with a password expiry condition, and lets you define password expiry policies.
- Storage tab: lets you filter the mailboxes to return.
- Identity Store tab: lets you add additional filter criteria such as department, company, location, and similar.
- Advanced tab: enables you to combine an external data source with the directory to determine a group's membership.
- Include/Exclude tab: lets you include or exclude objects regardless of whether they are returned by the query or not.
- Smart Script tab: lets you write a script to manipulate query results.

The **Storage**, **Password Expiry Options** and **Smart Script** tabs are not available for groups in a Microsoft Azure based identity store.

Smart Groups and Dynasties use:

- an LDAP query in an Active Directory based identity store.
- a device structured query language in an Azure based identity store.

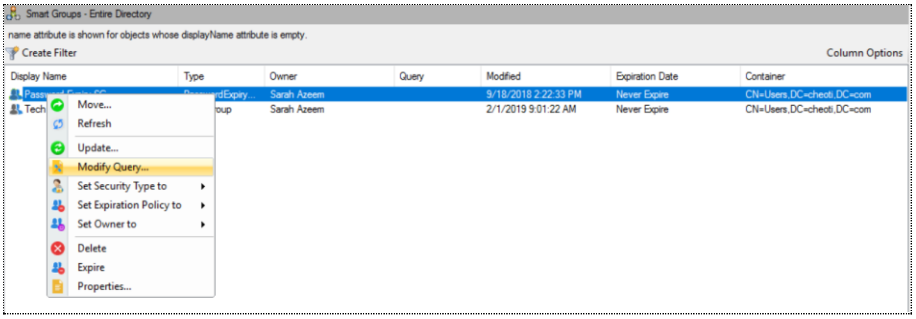
Launching the Query Designer

You can launch the **Query Designer** dialog box for a Smart Group or a Dynasty using any of the following methods:

- While creating a Smart Group or Dynasty
  On the **Query Options** page of the New Smart Group wizard (Figure 33) or New Dynasty wizard, click **Modify**.

- From group properties
  On the **GroupID** tab (Figure 44) in Smart Group/Dynasty properties, click **Modify** in the **Query** area.

- Using the shortcut menu
  Click the Smart Groups or Dynasties node. Then in the groups list, right-click a Smart Group/Dynasty and click **Modify Query** on the shortcut menu.



Smart Groups - Entire Directory

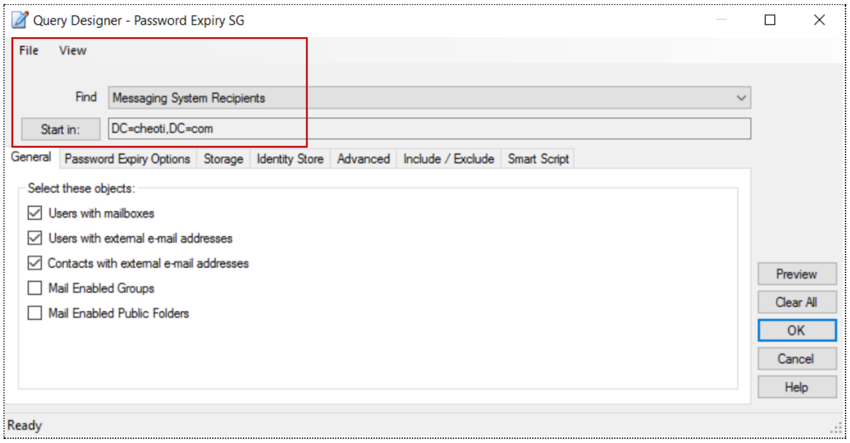
name attribute is shown for objects whose displayName attribute is empty.

Display Name	Type	Owner	Query	Modified	Expiration Date	Container
Passw	rdExpiry...	Sarah Azeem		9/18/2018 2:22:33 PM	Never Expire	CN=Users,DC=cheoti,DC=com
Tech	oup	Sarah Azeem		2/1/2019 9:01:22 AM	Never Expire	CN=Users,DC=cheoti,DC=com

Figure 87: Modify Query command on the shortcut menu

Common functions

Following are the common functions that apply to all tabs on the **Query Designer** dialog box:



Query Designer - Password Expiry SG

Find: Messaging System Recipients

Start in: DC=cheoti,DC=com

Select these objects:

☑ Users with mailboxes
☑ Users with external e-mail addresses
☑ Contacts with external e-mail addresses
□ Mail Enabled Groups
□ Mail Enabled Public Folders

Ready

Figure 88: Common functions on the Query Designer

- Click **Clear All** to clear the settings on the dialog box.
- Click **OK** to save the settings and close the dialog box.
- Click **Cancel** to discard the settings and close the dialog box.

Import or export a query

You can export and import queries using an XML file.

- To import a query from an XML file, click **File > Import Query** on the Query Designer dialog box.

  Om import, the Query Designer dialog box is populated with the settings for the imported query.
- To export a query to an XML file, click **File > Export Query** on the Query Designer dialog box.

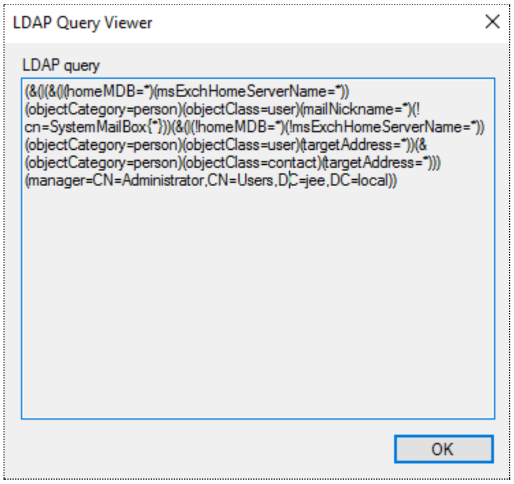
  The exported query is one that is obtained with the current settings on all tabs of the **Query Designer** dialog box.

You can view a query before you export it or after you import it.

View a query

You can view the query obtained with the current settings on all tabs of the **Query Designer** dialog box.

Click **View > Query**; the **Query Viewer** dialog box displays the query.



```
(&(|(&(|(homeMDB=*)(msExchHomeServerName=*))
(objectCategory=person)(objectClass=user)(mailNickname=*)(!
cn=SystemMailBox{*}))(&(|(!homeMDB=*)(!msExchHomeServerName=*))
(objectCategory=person)(objectClass=user)(targetAddress=*))(&
(objectCategory=person)(objectClass=contact)(targetAddress=*)))
(manager=CN=Administrator,CN=Users,DC=jee,DC=local))
```

Figure 89: Query Viewer

Specify object type for query

Select an option from the **Find** list to specify the type of object the query should fetch to include in the membership of the group.

- **Messaging System Recipients** - Mail-enabled objects
- **Computers** - Returns computers only
- **Custom** - Returns all objects regardless of objectClass. Be sure to add an objectClass predicate on the **Advanced** tab (Figure 98) to avoid unpredictable results.
- **Users, Contacts, and Groups** - Any user, contact, or group, regardless of whether they are mail-enabled.

The *Computers* and *Contact* object types are not supported in a Microsoft Azure-based identity store.

Specify a 'Start in' container

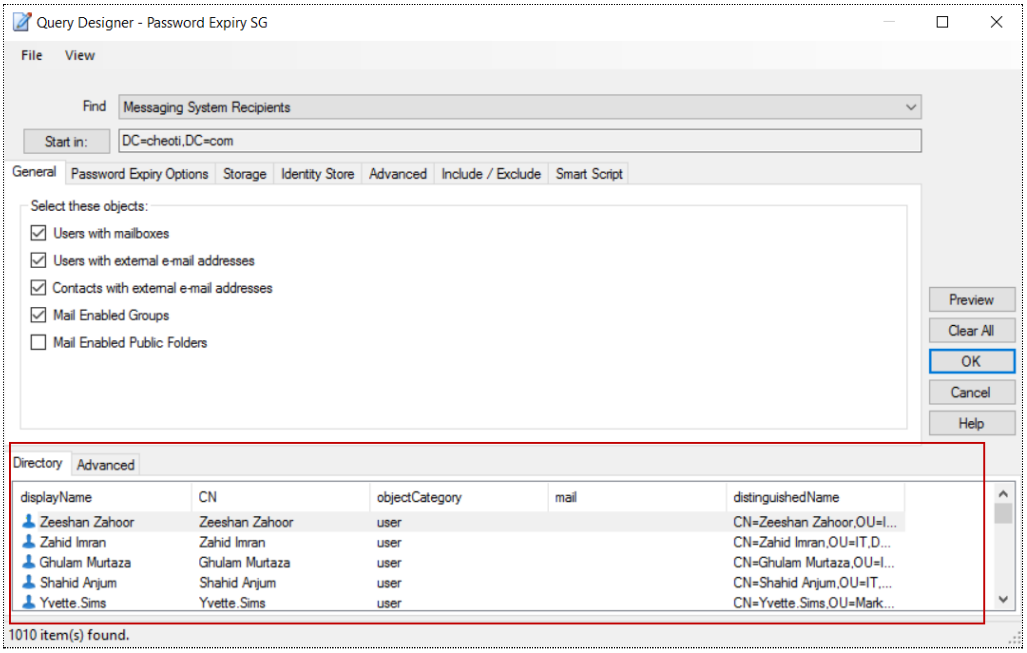
You must specify the containers that the query should search for retrieving the results.

Click the **Start in** button and select a container on the **Select Container** dialog box (Figure 108). The query would search for objects only in this container and its sub-containers to determine a group's membership.

Preview query results

Use the **Preview** button to preview query results obtained with the current settings on all tabs of the **Query Designer** dialog box. This is a check to ensure the accuracy of data before changes are committed to the directory.

On clicking it, results are displayed in the Preview pane, that appear at the bottom of the dialog box: This pane consists of two tabs; **Directory** and **Advanced**,



Find: Messaging System Recipients

Start in: DC=cheoti,DC=com

Select these objects:

- ☑ Users with mailboxes
- ☑ Users with external e-mail addresses
- ☑ Contacts with external e-mail addresses
- ☑ Mail Enabled Groups
- ☐ Mail Enabled Public Folders

displayName	CN	objectCategory	mail	distinguishedName
Zeeshan Zahoor	Zeeshan Zahoor	user		CN=Zeeshan Zahoor,OU=I...
Zahid Imran	Zahid Imran	user		CN=Zahid Imran,OU=IT,D...
Ghulam Murtaza	Ghulam Murtaza	user		CN=Ghulam Murtaza,OU=I...
Shahid Anjum	Shahid Anjum	user		CN=Shahid Anjum,OU=IT,...
Yvette.Sims	Yvette.Sims	user		CN=Yvette.Sims,OU=Mark...

1010 item(s) found.

Figure 90: Preview pane

Directory tab

This tab displays the results for the current query, as built with all the options set on all the tabs of the **Query Designer** dialog box.

You can choose the schema attributes to use as column headers on the **Directory** tab. See Specify attributes for preview on page 144 for details.

Of these selected attributes, you can further choose whether you want to use all or some attributes as column headers. See Table 9: Directory tab - Display preferences on page 146 for reference.

Advanced tab

This tab displays the results from the selected external data source when you click the **Execute** button on the **Advanced** tab (Figure 98) of the **Query Designer** dialog box.

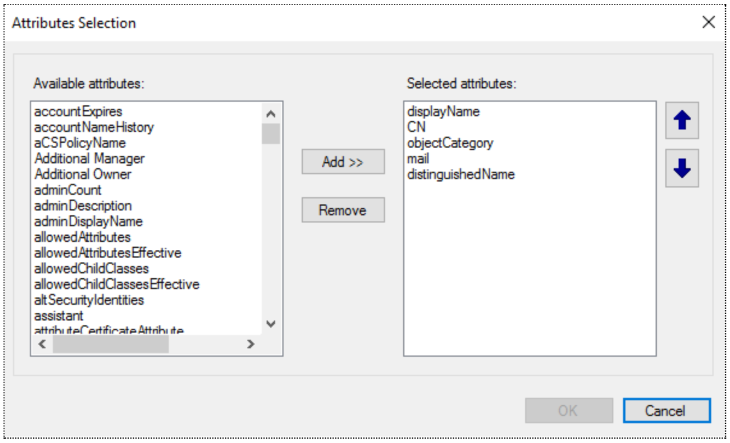
Each attribute in the query is used as a column header on this tab.

Specify attributes for preview

The Preview pane (Figure 90) of the Query Designer dialog box enables you to preview query results obtained with the current settings on all tabs of the dialog box.

On the **Directory** tab, results are displayed in a list, where each column header represents a schema attribute. For each record, the column displays the value of the respective header attribute. You can add and remove columns on the tab.

1. On the **Query Designer** dialog box, click **View > Add/Remove Preview Columns**; the **Attributes Selection** dialog box is displayed.



Available attributes:

accountExpires
accountNameHistory
aCSPolicyName
Additional Manager
Additional Owner
adminCount
adminDescription
adminDisplayName
allowedAttributes
allowedAttributesEffective
allowedChildClasses
allowedChildClassesEffective
altSecurityIdentities
assistant
attributeCertificateAttribute

Selected attributes:

displayName
CN
objectCategory
mail
distinguishedName

Figure 91: Attributes Selection dialog box

2. The **Selected attributes** column displays the schema attributes that are being employed as column headers on the **Directory** tab in the preview.

   - To add a new column, select an attribute in the **Available attributes** list and click **Add**. The attribute is moved to the **Selected attributes** list and will appear as a column header on the **Directory** tab.

   - To remove a column, select the required schema attribute in the **Selected attributes** list and click **Remove**. The attribute is moved to the **Available attributes** list and will not appear as a column header on the **Directory** tab.

   - Use the Up and Down arrows next to the **Selected attributes** list to sort the order of column headers.

3. Click **OK**.

Display preferences

On the **Attributes Selection** dialog box (Figure 91), you can specify the attributes to be used as column headers for the **Directory** tab of the preview pane (Figure 90). Of these selected attributes, you can further choose to set all or some attributes as column headers.

Right-click the column header on the **Directory** tab and use the context menu to set the attributes of the objects displayed on the tab. Options are:

Column header's context menu option	Description
Size All Columns to Fit	Set the column size of each column to fit its content.
<Attribute Name>	The names of the attributes selected on the **Attributes Selection** dialog box (Figure 91). For attributes currently displayed on the tab, the check box next to the attribute name is selected. Clear the check box for an attribute to remove it from the **Directory** tab.
More	Launches the **Attributes Selection** dialog box (Figure 91), where you can select additional attributes to display on the tab. After adding or removing attributes, re-launch the **Directory** tab to refresh the list of the attributes displayed.

Table 9: Directory tab - Display preferences

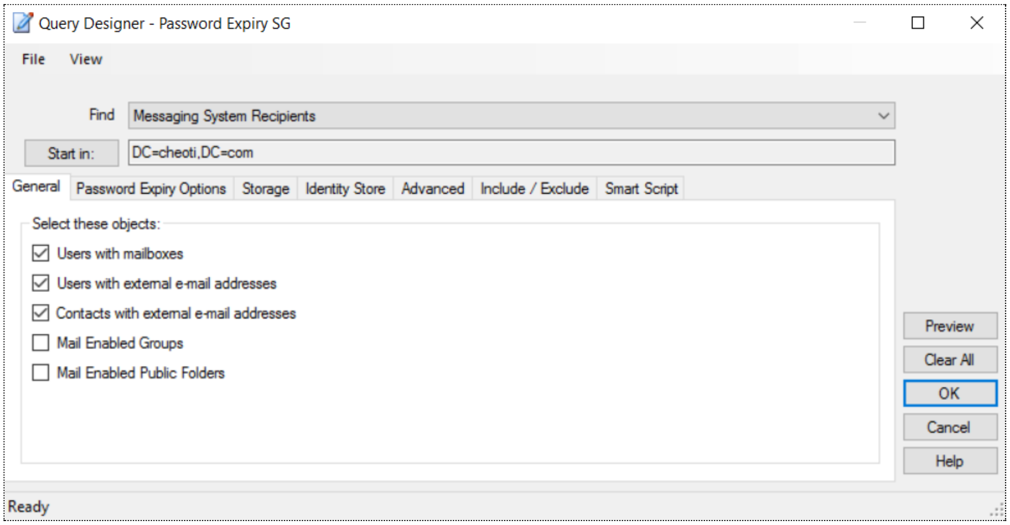
The **Directory** tab also provides object display options that are available when you right-click an object. These are:

Object's context menu options	Description
Add to Exclude	Add the object to the Exclude list so that it cannot be added to the group's membership.
Export	Export the selected object's information to a comma-separated value (csv) or XML file. The export action exports only the attributes displayed on the tab.
Export All	Export the information of all objects on the **Directory** tab to a comma-separated value (csv) or XML file. The export action exports only the attributes displayed on the tab.

Table 10: Advanced tab - Display preferences (2)

General query options

Use the **General** tab of the **Query Designer** dialog box to specify the type of objects to include in your search. The available options vary according to the object type selected in the **Find** list. See Specify object type for query on page 143.



Find: Messaging System Recipients

Start in: DC=cheoti,DC=com

Select these objects:

☑ Users with mailboxes
☑ Users with external e-mail addresses
☑ Contacts with external e-mail addresses
☐ Mail Enabled Groups
☐ Mail Enabled Public Folders

Figure 92: General tab

In the **Select these objects** area, select the categories of the object type to include in your search.

The following table lists the options available in the **Select these objects** area for each object type in the **Find** list.

Option in Find list	Categories on the General tab
Messaging System Recipients	• Users with mailboxes Include users with messaging system mailboxes. • Users with external email addresses Include users with email addresses that are external to your organization. • Contacts with external email addresses Include contacts with email addresses that are external to your organization. • Mail-enabled groups Include mail-enabled groups. • Mail-enabled public folders Include mail-enabled public folders.
Computers	• Workstations and Servers Include workstations and servers. • Domain Controllers Include domain controllers.
Custom	By default, it includes all object options for Messaging System Recipients, Computers, and Users, Contact, and

	Groups. For this reason, the **General** tab does not display any option for this object type.
Users, Contacts, and Groups	• Users Include users. • Contacts Include contacts. • Groups Include groups.

Table 11: Object types and their categories

The *Computer* and *Contact* object types are not supported in a Microsoft Azure-based identity store.

Password expiry options

The **Password Expiry Options** tab is only available for password expiry groups. You can create a password expiry group by selecting the **Run to create Password Expiry group** option on the **Welcome** page (Figure 32) of the **New Smart Group** wizard.

Purpose of a password expiry group:

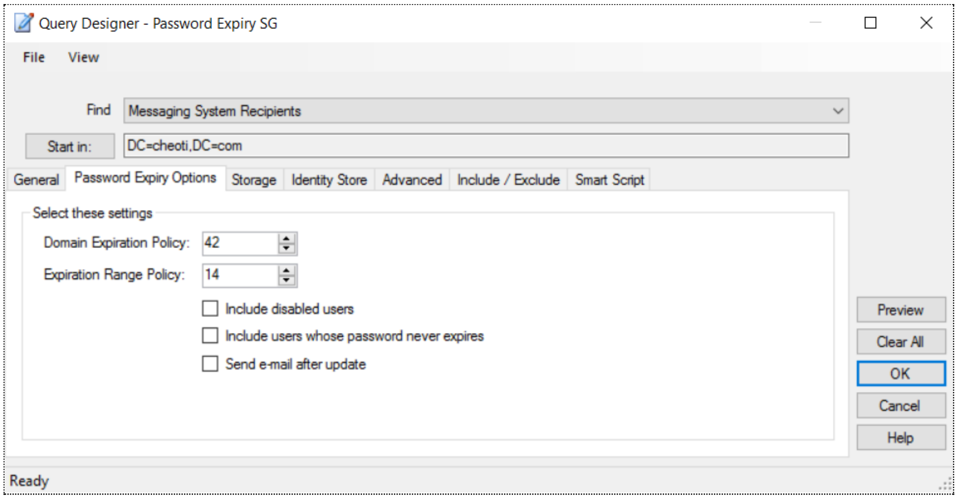
A password expiry group contains users as members whose identity store account passwords are approaching their expiry dates. Members are notified by email to change their passwords. On doing so, they are automatically removed from group membership.

How does a password expiry group work?

On the **Password Expiry Options** tab of the Query Designer, you can define settings for group membership. Based on these settings and the **PWDLASTSET** attribute, Automate creates this group with users whose passwords will soon expire.

When the group is updated, Automate adds/removes users from the group and sends email notifications to all members. To update the group, see Update Smart Groups and Dynasties on page 60.

You can also include disabled users and users whose password never expire to the password expiry group.



Find: Messaging System Recipients

Start in: DC=cheoti,DC=com

Select these settings

Domain Expiration Policy: 42

Expiration Range Policy: 14

□ Include disabled users

□ Include users whose password never expires

□ Send e-mail after update

Figure 93: Password Expiry Options tab

1. In the **Domain Expiration Policy** box, specify the maximum password age. The default age is 42 days.

   This setting does not affect your domain security settings on the directory server. However, it is recommended that the password age you specify here should be the same as that set in your domain policy.

2. In the **Expiration Range Policy** box, type or select the expiration range. The expiration range determines when to include a user in the password expiry group.

   For example, take a domain expiration policy with a maximum password age of 30 days. Setting the expiration range policy to 10 days includes users who have passwords aged 20 days or older in the password expiry group.

3. Select the **Include disabled users** check box to include disabled user accounts in the password expiry group.

4. Select the **Include users whose password never expires** check box to include users with the ‘password never expires’ setting enabled, as group members.

5. Select the **Send email after update** check box to send a password expiry warning email to group members each time group membership is updated either manually or through a scheduled job.

   This email contains a URL that redirects users to a Password Center portal for changing their identity store account passwords. (The administrator specifies this URL while configuring an SMTP server for the identity store.)

   The **Send email after update** options is enabled after the group is created.

   Warning emails are not sent to group members (users) whose passwords are set to 'never expire'. Such users are included in group membership when you select the **Include users whose password never expires** check box or add them to the **Include** list on the **Include / Exclude** tab (Figure 102).

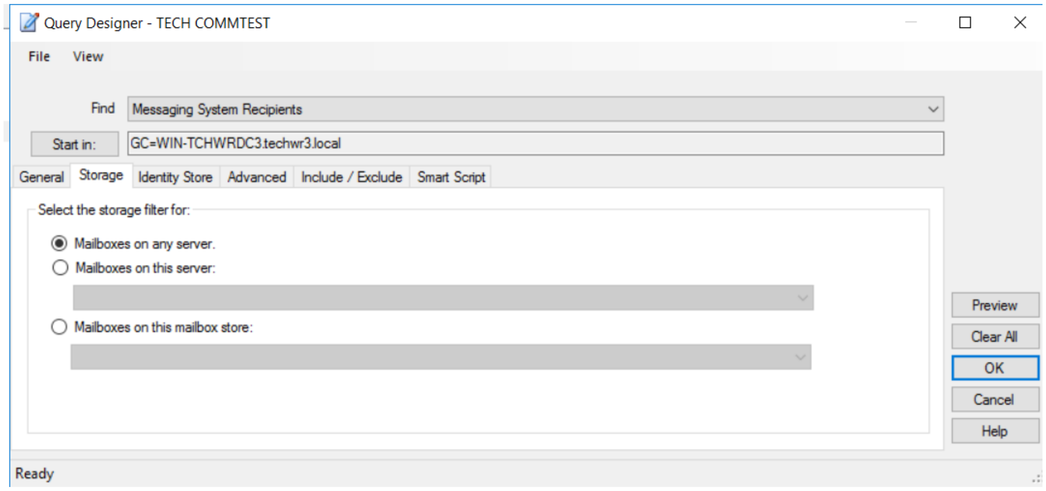
NOTE For warning emails to be sent, you must have an SMTP server configured for the identity store.

Storage options

Settings on the **Storage** tab are available when the 'Messaging System Recipients' option is selected in the Find list.

For the 'Messaging System Recipients' option, the default settings on the Storage tab retrieve all mailboxes, irrespective of any server or mailbox store. You can apply a filter to mailboxes you want the query to return.

If filters are specified, the query will return only mailboxes on the specified server or mailbox store. This filter does not affect custom recipients, public folders, and distribution lists.



Query Designer - TECH COMMTEST

Find: Messaging System Recipients

Start in: GC=WIN-TCHWRDC3.techwr3.local

Select the storage filter for:

● Mailboxes on any server.

○ Mailboxes on this server:

○ Mailboxes on this mailbox store:

Ready

Figure 94: Storage tab

The **Select the storage filter for** area displays the available options for the storage filter.

- **Mailboxes on any server**
  Returns all mailboxes. No filter applies with this selection.
- **Mailboxes on this server**
  Returns mailboxes from the server you select from the drop-down list.
- **Mailboxes on this mailbox store**
  Returns mailboxes from the mailbox store you select from the drop-down list.

This list displays all mailbox stores on the Exchange server(s) in your organization.

Identity Store tab

You can add custom criteria to your query that do not fit any of the categories represented on other tabs of the Query Designer dialog box. For example, you can add criteria to retrieve all directory users who live in Houston and have a fax number. You can also apply logical operators (AND, OR) to your custom query to achieve the most accurate results.

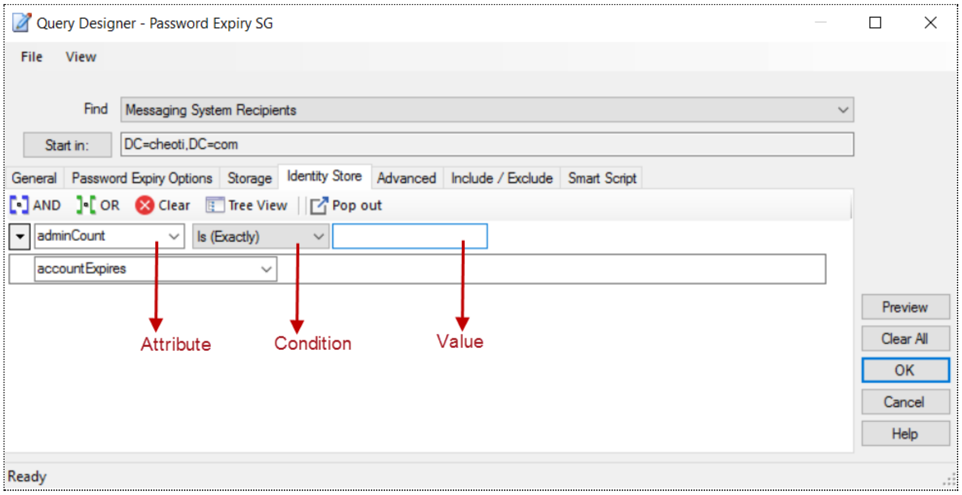


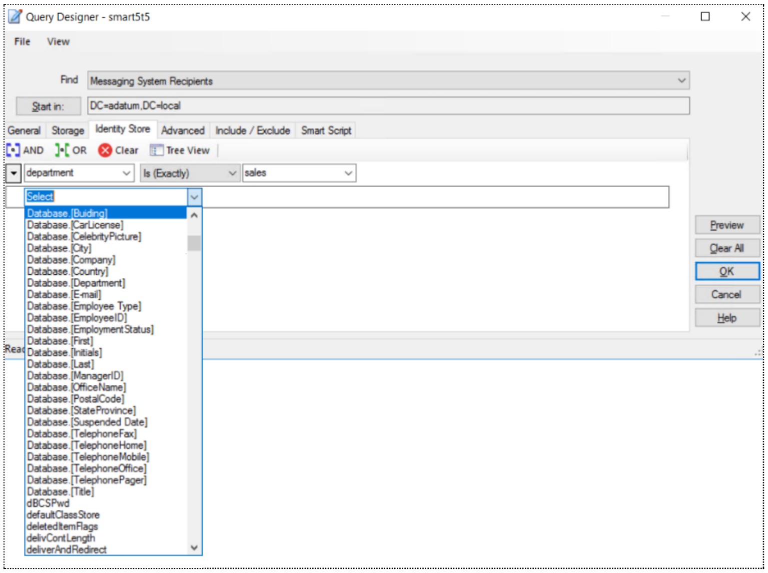
Figure 95: Identity Store tab

1. In the Attribute list, select a schema attribute, database attribute, or messaging system attribute to be searched. For example, to search for users who live in the city of Houston, select the City attribute from this list.

   Database attributes will only be listed if you have specified an external data source on the **Advanced** tab (Figure 100).

   For messaging system attributes, only Exchange attributes are supported.

   Figure 96 displays the Attribute list with database attributes.



Find: Messaging System Recipients

Start in: DC=adatum,DC=local

department | Is (Exactly) | sales

Figure 96: Attribute list displaying database attributes

2. The Condition list is displayed when you select an attribute. From here, select the condition that you want to apply to the selected attribute. This condition works with the Attribute and Value fields to identify search results. The following table lists the available conditions:

Condition	Description
Starts with	Returns everything that starts with the value.
Does not start with	Returns everything that does not start with the value.
Ends with	Returns everything that ends with the value. Searching against this condition is resource-intensive for the directory server.
Does not end with	Returns everything that does not end with the value Searching against this condition is resource-intensive for the directory server.
Is (exactly)	Returns everything that matches the value.
Is not	Returns everything that does not match the value.
Contains	Returns everything that contains the value. Searching against this condition is resource-intensive for the directory server.
Not contain	Returns everything that does not contain the value. Searching against this condition is resource-intensive for the directory server.

Present	Returns everything that has a value.
Not present	Returns everything that does not have a value specified.
Greater than (>=)	Returns everything with a value greater than or equal to the given value.
Less than (<=)	Returns everything with a value less than or equal to the given value.
All flags on	Performs a bit-wise comparison to find objects that have all of the flags set for the attribute according to the specified value. The value must be a decimal number; it cannot be a hexadecimal number or a constant name. For example, to search for all users who do not need a password (decimal value of PASSWD_NOTREQD flag = 32) and for those whose passwords never expire (decimal value of DONT_EXPIRE_PASSWORD flag = 65536), set the value of UserAccessControl's attribute against this condition to 65568 (65536 + 32). For more information, refer to the article http://support.microsoft.com/kb/305144.
Any flag off	Performs a bit-wise comparison to find objects that have any of the flags not set for the attribute according to the specified value. The value must be a decimal number; it cannot be a hexadecimal number or a constant name. For example, to search for all users that are either disabled (decimal value of ACCOUNTDISABLE flag =2) or locked out (decimal value of LOCKOUT flag = 16), set the value of UserAccessControl's attribute against this condition to 18 (2 + 16). For more information, refer to the article http://support.microsoft.com/kb/305144.
Any flag on	Performs a bit-wise comparison to find objects that have any of the flags set for the attribute according to the given value. The value must be a decimal number; it cannot be a hexadecimal number or a constant name. For example, to search for all users who do not need a password (decimal value of PASSWD_NOTREQD flag = 32) or whose passwords never expire (decimal value of

	DONT_EXPIRE_PASSWORD flag = 65536), set the value of UserAccessControl's attribute against this condition to 65568 (65536 + 32). For more information, refer to the article http://support.microsoft.com/kb/305144.
All flags off	Performs a bit-wise comparison to find objects that have all the flags not set for the attribute according to the specified value. The value must be a decimal number; it cannot be a hexadecimal number or a constant name. For example, to search for users that are neither disabled (decimal value of ACCOUNTDISABLE flag =2) nor locked out (decimal value of LOCKOUT flag = 16), set the value of UserAccessControl's attribute against this condition to 18 (2 + 16). For more information, refer to the article http://support.microsoft.com/kb/305144.
Chain match	Limited to the attributes of DN (distinguished name) type only. This is a special extended filter that walks the chain of ancestry in objects all the way to the root until it finds a match. For example, you can use this filter with the ManagedBy attribute to find all the groups for which the selected user is a direct or indirect owner.

Table 12: Conditions list

3. Specify a value for the attribute in the Value box. The query will return results considering the specified criteria (attribute, condition, value).

   The Value box is not available for non-comparison operators, such as *Present* or *Not Present*. Non-comparison operators only check whether the value for the selected field exists and return either TRUE or FALSE.

   When the value is a date, use the mm/dd/yyyy format.

Following the procedure above, you can add multiple criteria to your query.

Toolbar options

Click this button after selecting two or more records to insert a logical AND to the selected criteria.

To select a record, click the arrow icon next to it and click **Select Row**.

OR

Click this button after selecting two or more records to insert a logical OR to the selected criteria.

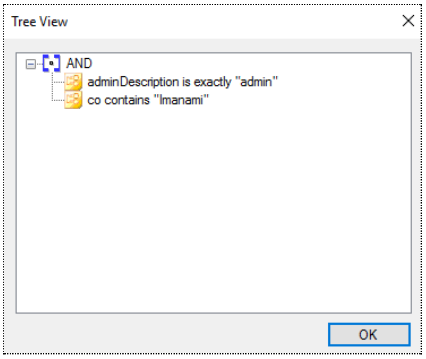
To select a record, click the arrow icon next to it and click **Select Row**.

Clear

Click this button to clear the displayed criteria.

Tree View

Displays a hierarchal view of the added criteria.



AND
adminDescription is exactly "admin"
co contains "Imanami"

Figure 97: Tree view of criteria

External data source options

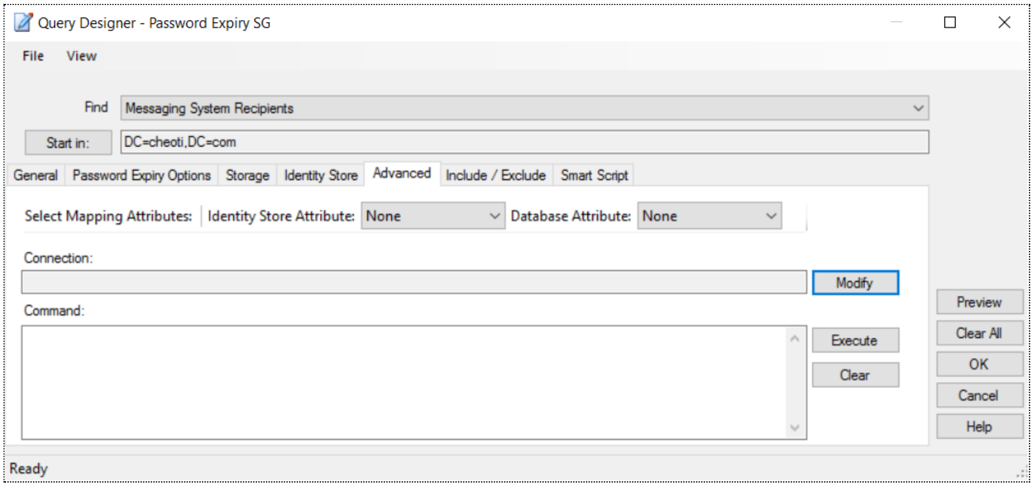
You can combine an external data source with the directory to determine a group's membership. The external data source can be Microsoft SQL Server, ODBC data source, Oracle, text files, and so on.

It works as follows:

- Configure a connection with an external data source.
- Specify a command to fetch objects from the data source.
- Map one column returned by the command with a directory attribute to join the external data source to the identity store.
- GroupID compares the values of the mapped attributes for objects that are returned by the command. Objects that have the same value in the directory and the data source are added to group membership.

Here is an example. You have an HR database with employee salaries, benefits, retirement plans, etc. You want to create a group of employees with annual salaries equal or less than USD 70,000. Since this information is not stored in your Active Directory, you must combine the directory with your HR database in order to create the group.

On the **Advanced** tab, you provide settings to connect to the HR database and specify a command that fetches the required employees (group members) from the database. Then you must map an Active Directory attribute to an attribute from the data source (such as employeeID in Active Directory and Reference No. in the HR database). GroupID fetches records from the database using the command and checks whether mapped attributes have the same value in Active Directory and the HR database for an object. If yes, the object is added to group membership.



Query Designer - Password Expiry SG

Find: Messaging System Recipients

Start in: DC=cheoti,DC=com

Select Mapping Attributes: Identity Store Attribute: None Database Attribute: None

Connection:

Command:

Ready

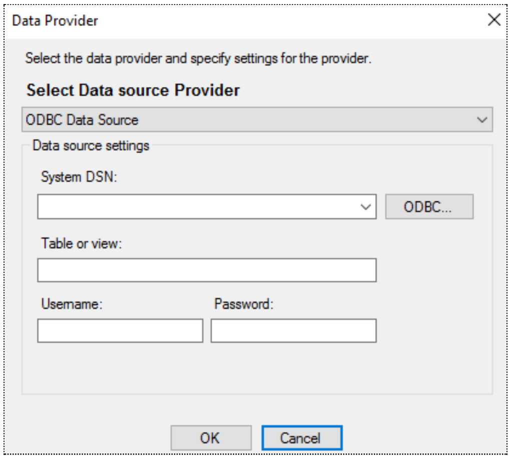
Figure 98: Advanced tab

When you specify an external data source (as shown in Figure 100), data source attributes will be available in the Attribute list on the **Identity Store** tab (Figure 96).

Connect to an external data source for retrieving members

1. Click **Modify** next to the **Connection** box to set or change the external data source and its connection settings.

   The **Data Provider** dialog box is displayed, where you can select the data provider and configure connection settings.



Data Provider

Select the data provider and specify settings for the provider.

Select Data source Provider

ODBC Data Source

Figure 99: Data Provider dialog box

2. Select a provider from the **Select Date Source Provider** list and enter connectivity details. Supported providers are:

    - Microsoft Text Driver
    - ODBC Data Source
    - Sun ONE iPlanet Driver
    - Lotus Notes
    - Microsoft SQL Driver
    - Oracle

    These providers are discussed in detail with reference to the 'import group membership' feature. See step 9 under Figure 64.

    Also see Appendix E - External database connectivity for ODBC and SQL driver on page 189.

3. Click **OK** to close the **Data Provider** dialog box.

    The **Connection** box displays the connection string settings for the data source.

4. Use the **Command** box to specify the command the Query Designer executes to retrieve records from the data source. This can be a query statement and can include multiple columns separated by commas (,). Field names are enclosed in brackets ([ ]) to prevent any ambiguity the query engine might encounter due to spaces between column names.

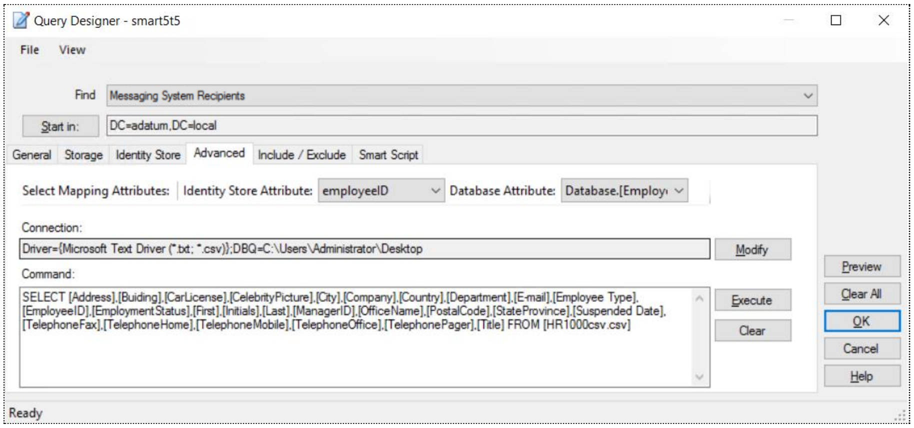
    The column names included in the command statement are available on the Advanced tab in preview.

For improved performance, select only the columns required to create your group. For example:

```
SELECT [Column1],[Column2] FROM [Filename.csv]
```

5. In the **Select Mapping Attributes** area, map an external data source attribute to an identity store attribute. The external data source attribute you select for mapping must be one returned by the command.

   - In the **Identity Store Attribute** list, select an identity store attribute to map a data source attribute to it.
   - In the **Database Attribute** list, select a data source attribute to map it to the selected identity store attribute.



Find: Messaging System Recipients

Start in: DC=adatum,DC=local

Select Mapping Attributes: Identity Store Attribute: employeeID Database Attribute: Database.[Employ

Connection:

```
Driver={Microsoft Text Driver (*.txt; *.csv)};DBQ=C:\Users\Administrator\Desktop
```

Command:

```
SELECT [Address],[Buiding],[CarLicense],[CelebrityPicture],[City],[Company],[Country],[Department],[E-mail],[Employee Type],
[EmployeeID],[EmploymentStatus],[First],[Initials],[Last],[ManagerID],[OfficeName],[PostalCode],[StateProvince],[Suspended Date],
[TelephoneFax],[TelephoneHome],[TelephoneMobile],[TelephoneOffice],[TelephonePager],[Title] FROM [HR1000csv.csv]
```

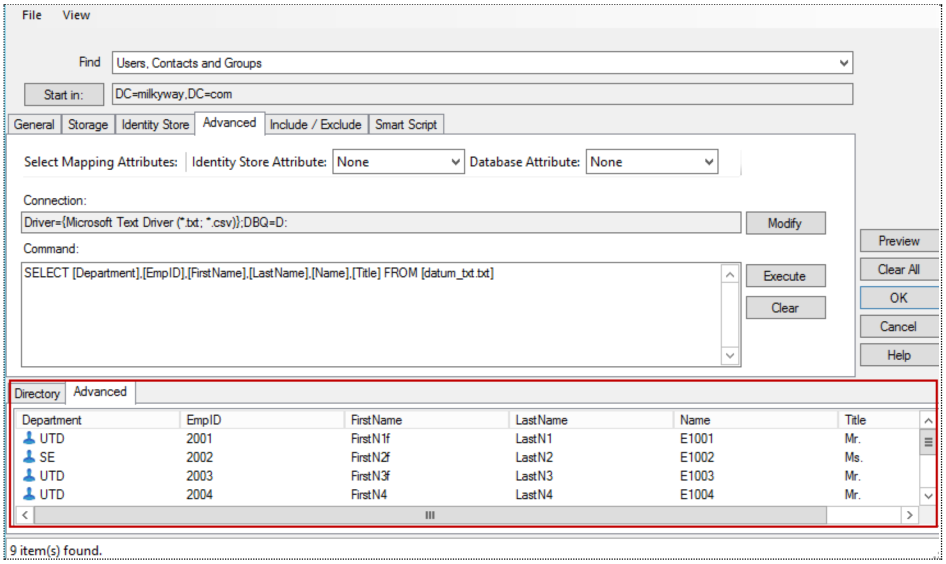
Figure 100: Advanced tab showing attribute mapping

When you specify an external data source (as shown in Figure 100), data source attributes will be available in the Attribute list on the **Identity Store** tab (Figure 96).

NOTE If you have upgraded to GroupID 10 from a legacy product or a previous GroupID version, you must re-map these attributes.

6. Click **Execute** to execute the command and preview the results. This process may take time, depending on the size of your data source.

   Results are displayed on the **Advanced** tab of the preview pane.



Find: Users, Contacts and Groups

Start in: DC=milkyway,DC=com

Select Mapping Attributes: Identity Store Attribute: None Database Attribute: None

Connection:

```
Driver={Microsoft Text Driver (*.txt; *.csv)};DBQ=D:
```

Command:

```
SELECT [Department],[EmpID],[FirstName],[LastName],[Name],[Title] FROM [datum_txt.txt]
```

Department	EmpID	FirstName	LastName	Name	Title
UTD	2001	FirstN1f	LastN1	E1001	Mr.
SE	2002	FirstN2f	LastN2	E1002	Ms.
UTD	2003	FirstN3f	LastN3	E1003	Mr.
UTD	2004	FirstN4	LastN4	E1004	Mr.

9 item(s) found.

Figure 101: Advanced tab of the preview pane

Include/Exclude objects in query results

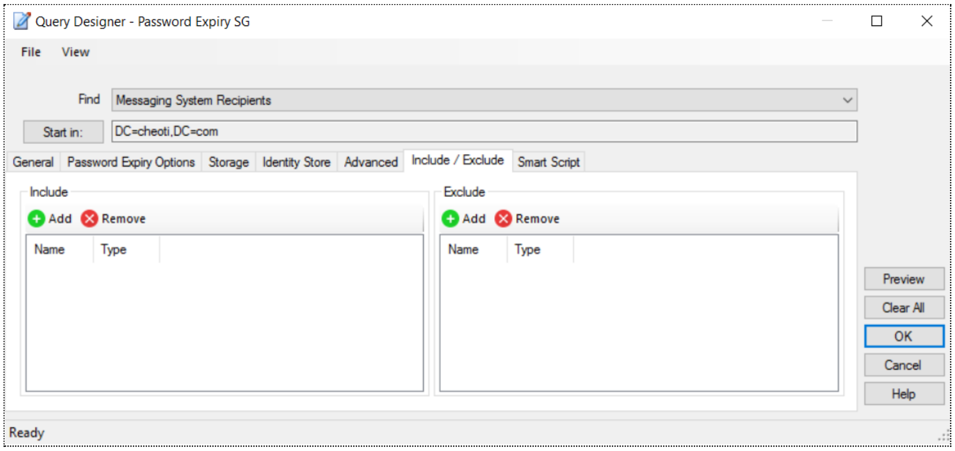
You can include or exclude an object from group membership regardless of whether it is returned by the query. The Include and Exclude lists on the **Include/Exclude** tab affect group membership at two points in the update process:

- **Immediately** - When you close the Query Designer dialog box, Automate adds the objects in the Include list to the group membership and removes the objects in the Exclude list from the group membership.
  If you have removed objects from the Include list, the group's membership is updated immediately. However, if you have removed objects from the Exclude list, the group's membership is updated only by manual update or by a scheduled job.
- **At group membership update** - When you update group membership, Automate obtains the query results, adds the objects to include, and then removes the objects to exclude.

  To update group membership, see Update Smart Groups and Dynasties on page 60.

NOTE

For best performance, use criteria to include or exclude objects as opposed to statically selecting the objects on the **Include/Exclude** tab.



Find: Messaging System Recipients

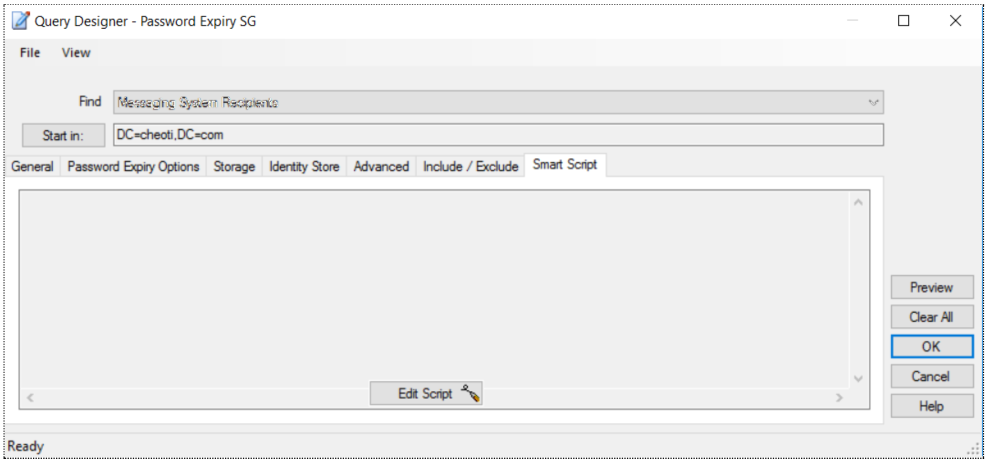
Start in: DC=cheoti,DC=com

Figure 102: Include/Exclude tab

- The **Include** area displays the list of objects to include in query results, and hence in group membership. The list also displays the objects that are imported to the membership of this group using the Self-Service portal's bulk import feature or using Automate's import membership feature. Use the **Add** and **Remove** buttons to modify this list.
- The **Exclude** area displays the list of objects to exclude from query results, and hence from group membership. Use the **Add** and **Remove** buttons to modify this list.

Smart Script tab

Use the scripting feature of the Query Designer to write a script for your custom logic. Automate scripting enables you to manipulate group memberships and Query Designer attributes (except for Include/Exclude attributes).



Find: Messaging System Recipients

Start in: DC=cheoti,DC=com

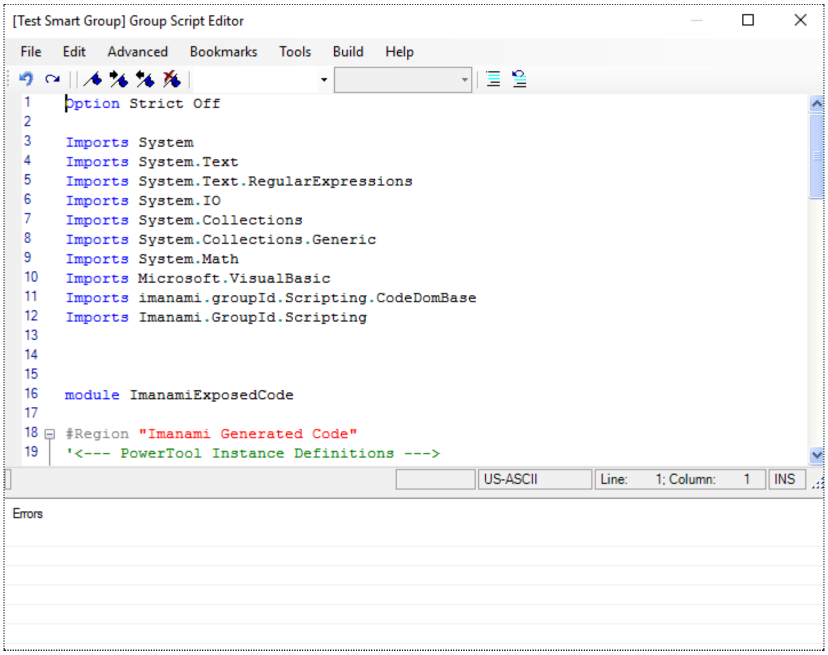
Figure 103: Smart Script tab

If no script has been added for the group, this tab is blank.

Click the **Edit Script** button to launch the Group Script Editor for writing a script.

Group Script Editor

The Group Script Editor is a full-function scripting environment for writing, testing and debugging code. Its supported language is Visual Basic .NET. In addition to the default .NET libraries, you get custom, specialized libraries called PowerTools.



```
Option Strict Off

Imports System
Imports System.Text
Imports System.Text.RegularExpressions
Imports System.IO
Imports System.Collections
Imports System.Collections.Generic
Imports System.Math
Imports Microsoft.VisualBasic
Imports imanami.groupId.Scripting.CodeDomBase
Imports Imanami.GroupId.Scripting



module ImanamiExposedCode

#Region "Imanami Generated Code"
'<--- PowerTool Instance Definitions --->
```

Figure 104: Group Script Editor

The code that you see when you open the editor for the first time is a template. It includes:

- Import statements for all default namespaces that must be included in your code.
- The region where the initializing code for Imanami PowerTools will be added. The initializing code is automatically generated whenever a new PowerTool reference is added to the environment.
- The events exposed by the scripting framework.

Automate saves scripts written in Group Script Editor in the GroupID database, so no physical file is created. Each time you open the editor for viewing or editing, it retrieves your script from the database. Should you need to use a script for another Smart Group or Dynasty, you must copy it from the source editor and then paste it in the editor of your target group.

Adding References

Use the **Tools > Add Reference** command to display the **Add Reference** dialog box that lists the various components and DLL libraries included in your script. The Add References dialog box functions in a manner similar to that of Visual Studio. This dialog box edits the script references for the current script. A script references file contains information about the run-time requirements of a library or component, such as which files are needed, how they are to be registered, and where on the host machine they should be installed.

There is an issue that arises when incorporating components that require full-trust permissions to run. During development, components run at full-trust, which may not be the case in the environment the project is deployed to. At run time, if the environment is running at a partial-trust security level, you can get code-access security violations. Thus, it is necessary to test applications in a variety of diverse 'trust' scenarios.

Chapter 11 - Customizing Views in Automate

For an identity store, you can customize the different group listings available in Automate. For example, you can:

- Set the page size for Automate listings
- Specify the number of workflow requests in listings
- Specify whether to show groups from all containers in the identity store or from a specific container
- Specify column headers for group listings
- Filter groups in a listing

Set Pagination for Automate listings

You can specify the page size for Automate listings. This means that you can set the maximum number of items to display on a page. Users will have to use the page navigation options at the bottom of the listing to move back and forth between pages.

Automate listings include:

- All Groups and its sub-listings
- My Groups
- My Memberships
- Recycle Bin

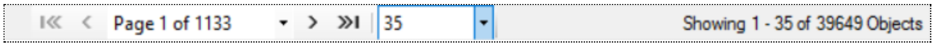
By default, 35 items are displayed on a page; you can set it to any number between 10 and 2147483647. If you specify a value beyond this range, it is automatically reset to the default value, that is, 35.

For optimal performance, leave this setting to default.

To set the page size:

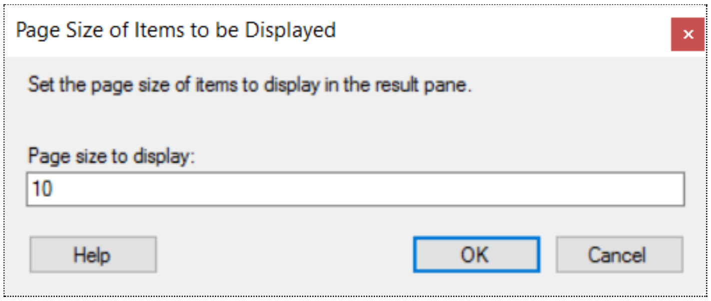
1. In GroupID Management Console, expand the **Automate** node and select the required sub-node.

   The bar at the bottom of the page displays the settings that control the page size.

2. Use the drop-down list to specify the number of items to display in the listing on this page. Options are: *35*, *100*, *500*, *1000*, and *Other*.

   Select *Other* to specify a different number.

   Page Size of Items to be Displayed

   Set the page size of items to display in the result pane.

   Page size to display: 10

   Figure 105: Page Size of Items to be Displayed dialog box

3. In the **Page Size to display** box, type the number of items you want to display on the page and click **OK**.

Set the number of Workflow requests in listings

You can set the number of workflow requests to be displayed on the **My Requests**, **Requests Inbox**, and **All Requests** pages. (These pages are displayed when you expand the **Requests** node in GroupID Management Console.)

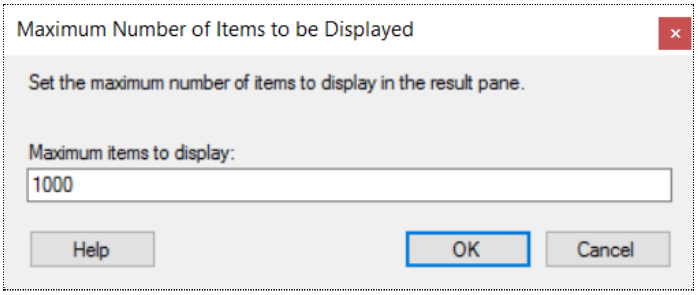
This settings also applies to the number of records fetched as search results on the **Find** dialog box (Figure 46).

Users can launch the **Find** dialog box from multiple pages in Automate to search for objects to designate as owners, managers, additional owners, members, and more.

By default, the **Find** dialog box and workflow request listings display 1000 items. You can modify this setting to limit the records.

To set the number of items for display:

1. In GroupID Management Console, expand the **Automate** node, right-click **All Groups**, and then click **Modify Maximum Items to display**.



Maximum Number of Items to be Displayed

Set the maximum number of items to display in the result pane.

Maximum items to display:

1000

Figure 106: Maximum Numbers of Items to be Displayed dialog box

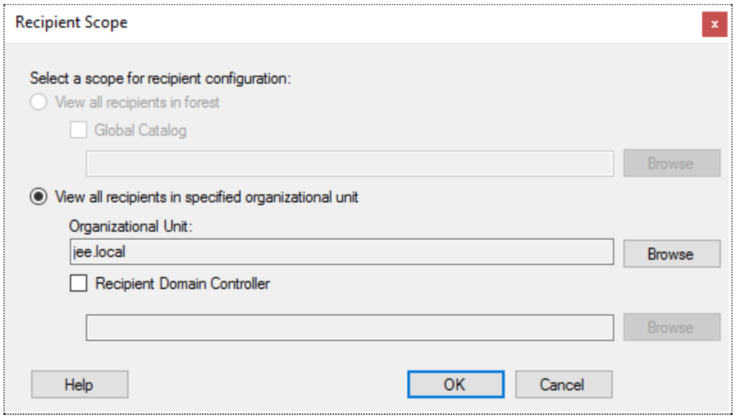
2. In the **Maximum items to display** box, type the number of items you want to display as search results on the **Find** dialog box. This setting also applies to the number of workflow requests displayed on the **My Requests**, **Requests Inbox**, and **All Requests** pages.

3. Click **OK**.

Managing resources through data scope

By default, Automate displays groups from the entire identity store. You can save network bandwidth and resources by limiting the display scope to an organizational unit.

1. Expand the **Automate** node, right-click **All Groups** and select **Modify Group Scope**.



Recipient Scope

Select a scope for recipient configuration:

○ View all recipients in forest

□ Global Catalog

● View all recipients in specified organizational unit

Organizational Unit:

jee.local

□ Recipient Domain Controller

Figure 107: Recipient Scope dialog box

The **Select a scope for recipients configuration** and **Recipient Domain Controller** options do not apply.

2. You can specify an organizational unit for Automate to display groups only from that organizational unit.

a. Make sure that **View all recipients in specified organizational unit** is selected.

b. Click the **Browse** button next to the **Organizational Unit** box.
The **Select Container** dialog box is displayed:

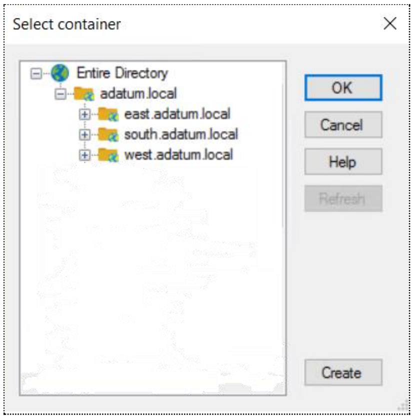


Figure 108: Select Container dialog box

c. Select an organizational unit and click **OK**. Groups residing in the selected organizational unit will be displayed in Automate group lists.

Group lists are discussed in Table 1.

3. Click **OK**.

NOTE The groups displayed in listings also depend on the search policy defined for a security role in an identity store.

For example, when the search policy restricts the search scope for Automate to a container (C1), the user can only select a sub-container under C1 on the **Modify Group Scope** dialog box. As a result, Automate listings display groups from that sub-container only.

The *modify group scope* setting only applies to the logged-in user.

Sorting a group list

To display groups in lists, GroupID employs columns, where each column header represents a schema attribute. The column displays this attribute’s value for each group listed. (Group lists in Automate are discussed in Table 1.)

You can add and remove columns. To add a column, simply select an attribute to use it as column header. Columns added or removed apply to all group listings.

GroupID also employs column sorting to make it easier to locate specific groups in lists. By default, group lists are sorted alphabetically by group name. You can change the default sorting criterion to other column headers. This setting is specific to each group list.

Specify column headers for group lists

1. In GroupID Management Console, select **Automate** > [any group node].
2. Click **Column Options** in the top right corner.

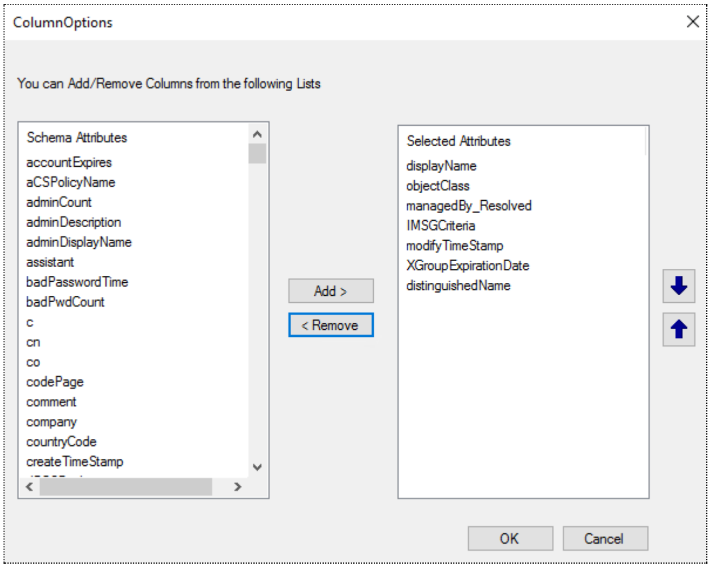


Figure 109: Column Options dialog box

3. The **Selected Attributes** column displays the schema attributes that are being employed as column headers in group listings.
   - To add a new column, select an attribute in the **Schema Attributes** list and click **Add**. The attribute is moved to the **Selected Attributes** list and will be displayed as a column header in group lists.
   - To remove a column, select the required schema attribute in the **Selected Attributes** list and click **Remove**. The attribute is moved to the **Schema Attributes** list and will not be displayed as a column header in group lists.
4. Click **OK**.

This column header setting applies to all group listings in Automate, such as those discussed in Table 1.

Sort the groups in a list

1. In GroupID Management Console, select Automate > [required group node].
2. In the groups list, click a column header to sort the groups by it. For example, click the **Owner** column header to sort the groups by owner.

   Clicking once on a column header arranges the group list in ascending order and clicking again sorts it in descending order.

Apply filters to a group listing

You can apply filter expressions to reduce the number of results returned in a group list in Automate. (Group lists in Automate are discussed in Table 1.)

A groups list, by default, shows all relevant groups in the connected identity store, based on the maximum limit set for displaying groups (see Set Pagination for Automate listings on page 163) and the specified data scope (Figure 107).

Filters help you narrow down groups list based on the criterion you specify. Select an attribute and specify a value, along with an operator that sets the condition that the value must satisfy for groups to be displayed in the list. For example, if you select Expiration Date as the attribute, specify a date as value and apply the ‘is exactly’ operator, all groups that will expire on the specified date will be displayed in the groups list.

Note that the Recycle Bin in Automate does not support DN based filters.

To apply a filter expression:

1. In GroupID Management Console, select **Automate** > [required group node].
2. Click **Create Filter** at the top of the list.
   This displays a row of fields for specifying the filter expression.

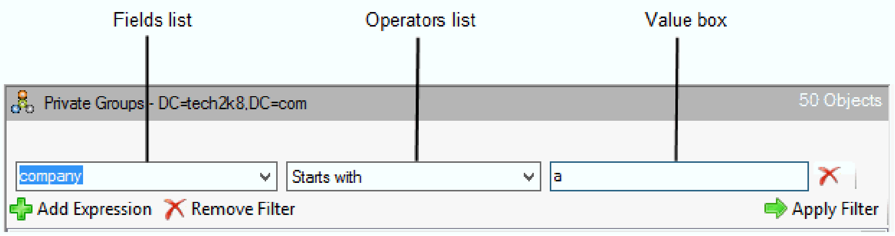


Figure 110: Group list filter

3. Specify a filter expression to filter the group list.

   a. From the first box (Fields list), select an attribute to apply the filter on.

      This list contains all schema attributes and two database attributes, ‘Expiration Date’ and ‘Expiration Policy’.

      In case of Active Directory, if Exchange schema was added to Active Directory schema by the network administrator, then this list also contains Exchange attributes.

   b. From the second box (Operators list), select the operator or rule to apply to the selected attribute and its value.

      See Table 12 to learn about the available operators.

   c. In the third box, specify a value for the attribute. The operator determines whether the groups that have the specified value for the selected attribute should be displayed in the groups list or not.

      For some operators, this field is not available, such as **is present** or **is not present**, which are not comparison operators. Both conditions use a wildcard to return all groups that fit the criteria.

   The filter will return results considering the specified criteria (attribute, condition, value).

4. For each additional expression, click **Add Expression** and repeat step 3. You can create up to 10 expressions.

   Each additional filter applied will be combined with the others to return results that satisfy all the given filters.

   - You can remove a filter by clicking ✗ next to the required filter expression.
   - Click **Remove Filter** to remove all filter expressions for a group view.

5. Click **Apply Filter**.

Appendix A

Group Management Concepts

Group classification

GroupID classifies groups into two broad categories: Unmanaged (static) groups and Managed (Smart Groups). These categories are discussed in Chapter 4 - Creating Groups on page 27.

Group security

Security type indicates the access level for a group. GroupID provides three security types:

Private groups

A private group is one whose membership is determined solely by the group owner. The owner determines who can join and leave the group. Additional owners can also manage group membership. However, users cannot even request to join or leave a private group.

Semi-private groups

Semi-private groups, like private groups, have an owner who determines membership, except that members can request to join and leave the group.

Public groups

A public group is open to all users. Users can join and leave a public group without requiring owner permission. The administrator can configure email notifications to be sent to the group owner when a member joins or leaves the group.

NOTE The group security option is available with a GroupID Self-Service license.

Group type

Groups fall into two functional categories: distribution groups and security groups.

Distribution groups

Distribution groups, also called distribution lists, are designed to combine users together so that you can send emails (via a mail server) collectively to a group rather than individually to each user in the group.

Distribution groups can be used only with email applications (such as Microsoft Exchange). These groups are not security-enabled, which means that they cannot be listed in discretionary access control lists (DACLs). If you need a group for controlling access to shared resources, create a security group.

Security groups

Security groups provide an efficient way to assign access to resources on your network. Using security groups, you can:

- Assign user rights

  User rights are assigned to security groups to determine what members of that group can do within the scope of a domain (or forest).

  For example, a user who is added to the Backup Operators group can back-up and restore files and directories located on each domain controller in the domain. So, by being a member of this group, you inherit the user rights assigned to the group.

- Assign permissions to resources

  This is different from user rights because user rights apply across an entire domain versus permissions that are directed to a specific entity. Permissions determine who can access the resource and the level of access, such as Full Control or Read-only.

Security groups can also be used as a distribution group in Exchange. These are known as security-enabled distribution groups.

Group scope

Groups are characterized by a scope that identifies the extent to which the group is applied in a domain or forest. The boundary, or reach, of a group scope is also determined by the domain functional level of the domain in which it resides.

A group’s scope determines:

- the domains from which members can be added to the group
- the domains where the group can be used to grant permissions
- the domains where the group can be nested in other groups

A group can be of universal, global, or domain local scope.

Universal

Use groups with universal scope to consolidate groups that span domains. To do this, add the accounts to groups with global scope, and then nest these groups within groups that have universal scope. When you use this strategy, any membership changes in the groups that have global scope do not affect the groups with universal scope.

Do not change the membership of a group with universal scope frequently, because membership changes cause the entire membership of the group to be replicated to every global catalog in the forest.

Global

Use groups with global scope to manage directory objects that require daily maintenance, such as user and computer accounts. Because groups with global scope are not replicated outside their own domain, you can change accounts in a group having global scope frequently without generating replication traffic to the global catalog.

As a matter of best practice, you should use global groups or universal groups rather than domain local groups when you specify permissions on domain directory objects that are replicated to the global catalog.

A global group can contain users, computers, and groups from the same domain but not universal groups.

Domain Local

Groups with domain local scope help you define and manage access to resources within a single domain. For example, to give five users access to a printer, you can add all five user accounts in the printer permissions list. If, however, you later want to give the five users access to a new printer, you must again specify all five accounts in the permissions list for the new printer.

A domain local group can contain users, computers, global groups, and universal groups from any domain in the forest and any trusted domain, as well as domain local groups from the same domain. Such a group can be a member of any domain local group in the same domain.

Appendix B

Azure AD vs. Active Directory based identity stores

This appendix discusses the GroupID features that work differently in Active Directory and MS Azure-based identity stores.

Group expiration policy

The Azure portal offers limited options to define a default expiry policy for groups whereas GroupID provides a comprehensive Group Life Cycle policy.

Since these policies are not integrated; you can either use Azure AD's or GroupID's expiration policy settings for groups in an Azure-based identity store.

Group naming policy

The group naming policy defined in Azure AD is not integrated with GroupID's Group Name Prefixes policy. As a result:

- Azure's group naming policy has no impact on groups created using GroupID.
- Prefixes or suffixes that are applied to groups created in Azure, cannot be modified using GroupID.

To use the same prefixes for group names as are defined in Azure AD, it is recommended that you define the same prefixes in GroupID.

Dynamic Groups in Azure AD

A dynamic group created in the Azure portal would not be automatically upgraded to a Smart Group in GroupID. It will be displayed as a static (unmanaged) group. However, its membership would be managed dynamically in Azure.

You should apply a query to a group either in the Azure portal or in GroupID. Do not manipulate the same object simultaneously from GroupID and the Azure portal.

Multifactor authentication policy

In GroupID, a multifactor authentication policy can be defined for an identity store. This policy applies to GroupID Password Center User portals and the GroupID mobile app.

The multifactor authentication policy defined for the Azure portal cannot be integrated with the GroupID multifactor authentication policy. Azure’s policy would apply to the Azure portal only while the GroupID policy would apply to the GroupID Password Center user portal and the GroupID mobile app only.

User roles in Azure AD and GroupID

When a user, with a simple user role in the Azure portal, is assigned a security role in GroupID, then he/she can manipulate directory objects using GroupID that he/she cannot otherwise manipulate directly on the Azure portal due to limited role permissions.

The actions that a user can perform using GroupID depend on the permissions assigned to his or her role in GroupID. These permissions may conflict with the permissions that the user has on the Azure portal.

For example, a user who cannot create groups in the Azure portal can create groups in Azure AD using GroupID if his or her GroupID role has permissions to create new groups.

To avoid conflicts, GroupID administrators should grant permissions to security roles with discretion.

Groups in Azure

- You can create security groups, Office 365 groups, and distribution lists using GroupID, if Office 365 is set as the messaging provider for the identity store. However, security groups cannot be mail-enabled.
- Azure AD does not allow a group to be added to the membership of an Office 365 group. For this reason:
  - An Office 365 group can only have user objects as its members.
  - Even if the query for an Office 365 group returns different object types, only user objects are added to group membership.
  - The nesting option in the ‘out of bounds’ settings for an identity store would empty the membership of a Smart Group of the Office 365 type, since nested groups cannot be added as group members.

  - A Dynasty cannot be created as an Office 365 group.

- You cannot create Office 365 connected Yammer groups, Teams groups, and Planner groups using GroupID.

  These groups can be created from their respective portals.

  However, Yammer, Teams, and Planner groups will be displayed in Automate and the Self-Service portal when their respective subscriptions are added to Office 365. When you update these groups using GroupID, your changes will be reflected on the Yammer, Teams, and Planner portals respectively.

- Azure AD supports multiple primary owners for a group. However, you cannot create a group unless you specify at least one primary owner for it.

- Only user objects can be set as primary owners.

- When you expire an Office 365 group using GroupID, its member list is backed up in the database and then cleared from Office 365. The Microsoft Graph API does not allow for the modification and removal of the *mail* attribute; therefore, it is not possible to remove the group’s email and make it mail-disabled.

User and Contact objects in Azure

- You can create users (non mail-enabled) and mailboxes in an Azure based identity store. The *contact* object type is not supported.

- The *Photo* attribute is only available for an Office 365 user (mailbox).

- GroupID Password Center portal does not display the password expiry date of a user account in an Azure based identity store.

- The ‘block sign in’ option in the Azure portal is enabled when a user's account is disabled or locked out in GroupID.

  For example, if a user is locked out due to the domain policy or disabled by the User Life Cycle job, the Azure *block sign in* will be enabled. The disabled/locked user will not be able to log into his or her workstation either.

Other

- For an Azure based identity store, you must configure Office 365 as the messaging provider and SMTP server.

- The Reports module in GroupID does not generate reports for an Azure based identity store.
- The Recycle Bin does not display any data for an Azure based identity store.
- GroupID Management Shell cannot communicate directly or remotely with Microsoft Azure and Office 365.
- Microsoft Azure is not supported as a source or destination provider in a Synchronize job. However, you can use Office 365 as a destination provider to provision or deprovision objects n Azure.
- Smart Groups and Dynasties in an Azure based identity store use a device structured query language (and not an LDAP query) to update group membership.
- Only the Azure AD attributes listed in the Microsoft Graph API v 1.6.2 schema file are available in GroupID.
- The *company* attribute in Azure AD stores the name of the company registered on the Azure portal and cannot be manipulated using GroupID. An Azure based identity stores uses the OfficeLocation attribute as an alternative for the company attribute.

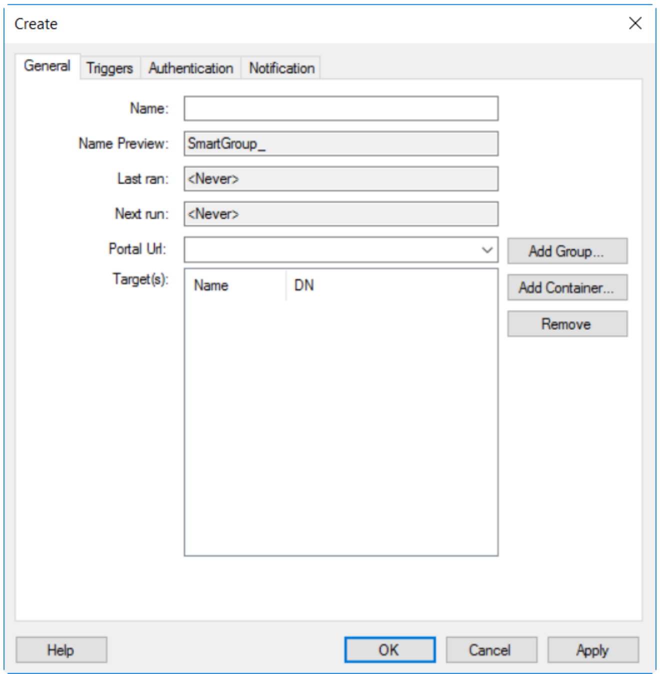
Appendix C

Define a Smart Group Update job

You can define a Smart Group Update job for an identity store and apply it to Smart Groups and Dynasties. The Task Scheduler keeps checking scheduled jobs and initiating scheduled job runs.

Multiple Smart Group Update jobs can be defined; however, you can also apply one job to multiple groups.

The **Create Job** dialog box is as follows:



Name:

Name Preview: SmartGroup_

Last ran: <Never>

Next run: <Never>

Portal Url:

Target(s):

Name	DN

Figure 111: Create Job dialog box – General tab

General tab

1. In the **Name** box, type a name for the job.
2. The **Name Preview** box displays the job name prefixed with **SmartGroup_**. The job is displayed with this name in the scheduled jobs list and email notifications.

3. The **Last ran** box displays the date and time the job last ran.
4. The **Next run** box displays the next date and time the job will run. Use the **Triggers** tab (Figure 112) to specify a triggering criterion for the job, that, when met, starts the execution of the job.
5. From the **Portal Url** list, select a Self-Service portal URL to include it in job-specific notification emails. This URL redirects recipients to the portal.

   You must be licensed to use GroupID Self-Service for portal URLs to appear here.
6. The **Target(s)** box is for specifying the containers, Smart Groups, and Dynasties the job will process.
   - To specify a Smart Group or Dynasty, click **Add Group**. Then use the **Find** dialog box (Figure 46) to search and select the required group(s).
   - To specify a container, click **Add Container**. Then use the **Select Container** dialog box (Figure 108) to select one or more containers. The job will process all Smart Groups and Dynasties in the selected container and its sub-containers.

   To remove a group or container from the **Target(s)** box, select it and click **Remove**.

Triggers tab

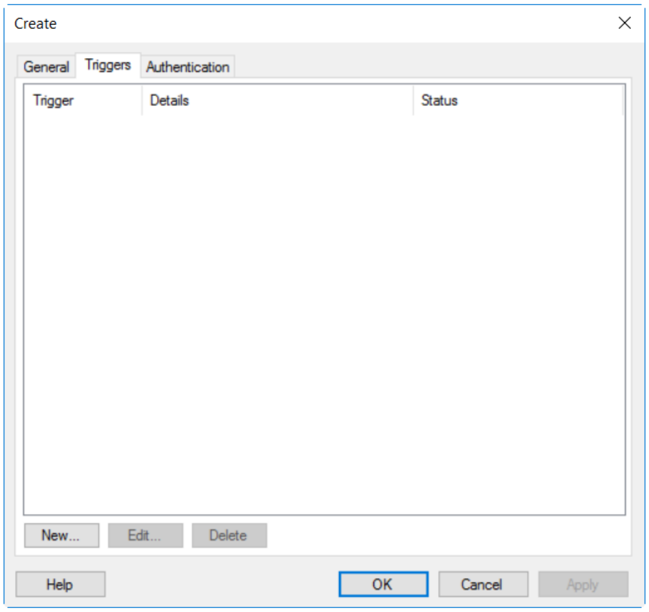
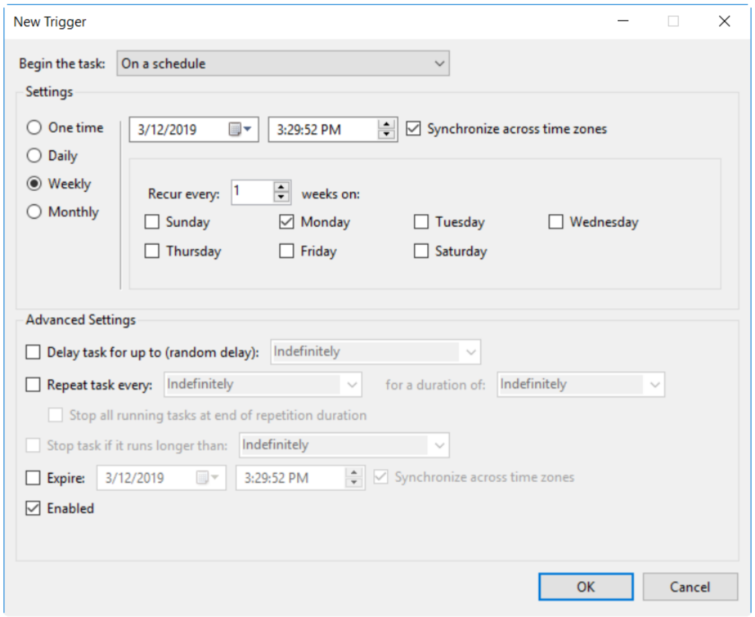


Figure 112: Triggers tab

1. Click **New** to specify a triggering criterion for the job, that, when met, starts

the execution of the job.



New Trigger

Begin the task: On a schedule

Settings

○ One time
○ Daily
● Weekly
○ Monthly

3/12/2019 3:29:52 PM ☑ Synchronize across time zones

Recur every: 1 weeks on:

☐ Sunday ☑ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday ☐ Saturday

Advanced Settings

☐ Delay task for up to (random delay): Indefinitely
☐ Repeat task every: Indefinitely for a duration of: Indefinitely
☐ Stop all running tasks at end of repetition duration
☐ Stop task if it runs longer than: Indefinitely
☐ Expire: 3/12/2019 3:29:52 PM ☑ Synchronize across time zones
☑ Enabled

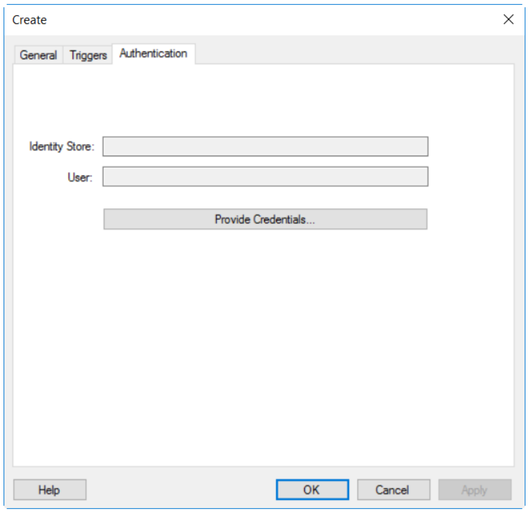
Figure 113: New Trigger dialog box

The **Triggers** dialog box is the same as available in **Windows Task Scheduler**. Visit this page for help.

2. After specifying the settings, click **OK**.
   The trigger is displayed on the **Triggers** tab (Figure 112).

   A job can have one or more triggers, allowing it to start in many ways. With multiple triggers, the job will start when any of the triggers occur.

Authentication tab



Create

Identity Store:

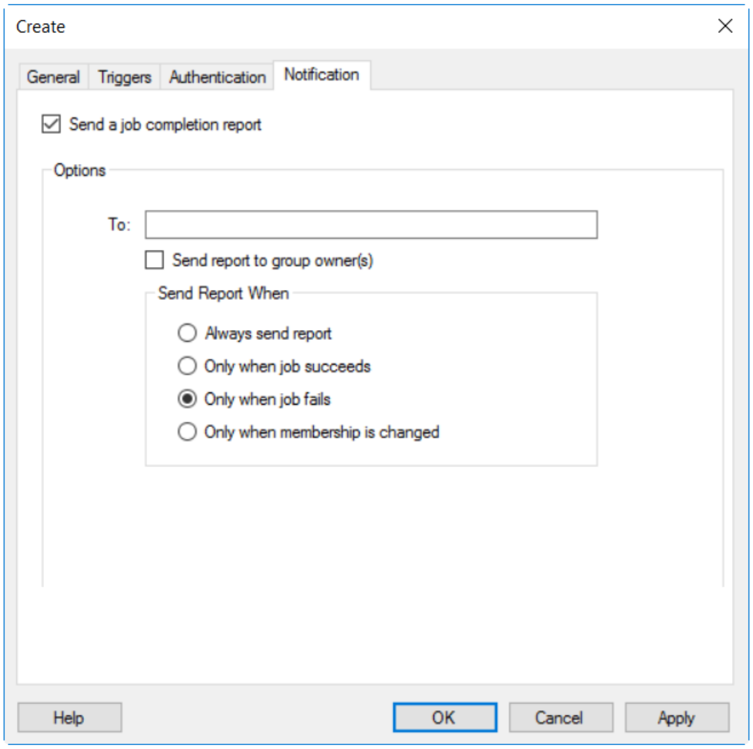
User:

Figure 114: Authentication tab

A Smart Group Update job is specific to an identity store. On the **Authentication** tab, select an identity store and provide the credentials of a service account to run the scheduled job in the identity store.

1. Click **Provide Credentials**; the **Login** window (Figure 2) is displayed. Select the identity store that GroupID Management Console is connected to, and provide the credentials of a service account to run the scheduled job in the identity store. This account must have administrative privileges in GroupID.
2. Click **Log in**.
   The identity store and the service account are displayed in the **Identity Store** and **User** boxes.

Notification tab


Create

☑ Send a job completion report

Options

To:

□ Send report to group owner(s)

Send Report When

○ Always send report
○ Only when job succeeds
● Only when job fails
○ Only when membership is changed

Figure 115: Notification tab

Use the **Notification** tab to set Automate to send a summary report to the group owner(s) as well as to any other recipient when the group is updated.

This summary report is sent as an email notification and contains a URL that redirects users to the Self-Service portal, where they can take the actions indicated in the notification. This URL is selected on the **General** tab (Figure 111) of the **Create Job** dialog box.

1. Select the **Send a job completion report** check box to enable email

notifications.

When a job run is completed, a summary report will be sent to the specified recipients.

2. In the **To** box, enter the email addresses of one or more notification recipients, separating multiple addresses with a semicolon (;).

   All the recipients mentioned here will get a report of all the groups updated by the job.

3. Select the **Send Report to group owner(s)** check box to send a report to each unique group owner of the groups processed by the job. Moreover, each Dynasty owner receives a notification about its group and direct child Dynasties.

   Group owners include the primary owner, additional owner(s), and Exchange additional owner(s).

4. In the **Send Report When** area, select one of the following options:

   - **Always send report** - Always send the notification, whether the job succeeds or fails to update the group(s).
   - **Only when job succeeds** - Send the notification only when the job successfully updates the group(s).

     With this option selected, a notification will be sent only when all groups added to the job are successfully updated when the job runs. Even if one group fails to be updated, the notification will not be sent.
   - **Only when job fails** - Send the notification only when the job fails to update the group.

     With this option selected, a notification will be sent even when all except one group fails to be updated when the job runs.
   - **Only when membership is changed** – Send the notification only when any changes are made to group membership as a result of the job run.

5. Click **OK**.

NOTE For email notifications to be sent, an SMTP server must be configured for the identity store.

NOTE When a Smart Group Update job runs on a group, the notification behavior is as follows:

- If the email address of a group's additional owner is specified in the **To** box but the **Do not Notify** check box is selected for it on the **Managed By** tab in group properties (Figure 39), the additional owner will receive the notifications.
- If the **Send Report to group owner(s)** check box is selected but the **Do not Notify** check box is selected for an additional owner on the **Managed By** tab in group properties (Figure 39), the additional owner will not receive the notifications.

NOTE When a Smart Group Update job is bound to only one OU that contains all expired Smart Groups/Dynasties, a notification will not be sent, even if the **Always send report** option is selected. Expired Smart Groups and Dynasties are not evaluated for the update process. However, even if one Smart Group/Dynasty in the OU is not expired, a notification will be sent for all objects with *failed* status for expired objects.

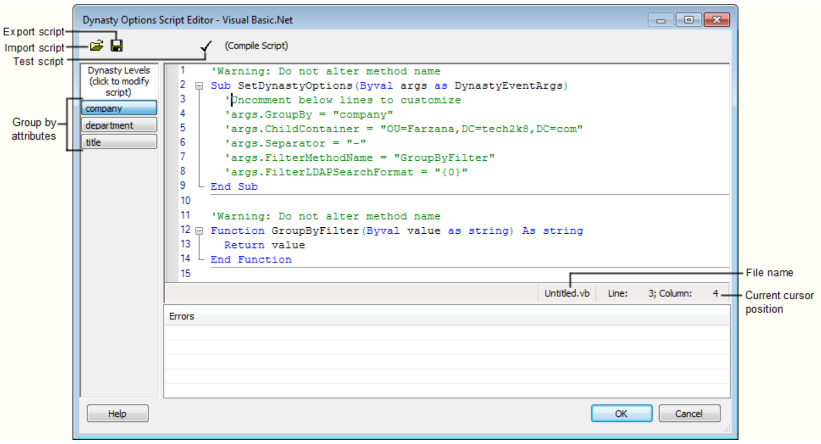
Appendix D

Script Editor in Automate

The Dynasty Options Script Editor provides an environment for writing custom scripts using Visual Basic .NET to customize settings for parent Dynasties.

To launch the editor:

1. On the **GroupID** tab (Figure 44) in group properties, click the **Options** button.
2. Click the **Edit Script** button on the **General** tab of the **Dynasty Options** dialog box.



```
'Warning: Do not alter method name
Sub SetDynastyOptions(Byval args as DynastyEventArgs)
  'Uncomment below lines to customize
  'args.GroupBy = "company"
  'args.ChildContainer = "OU=Farzana,DC=tech2k8,DC=com"
  'args.Separator = "-"
  'args.FilterMethodName = "GroupByFilter"
  'args.FilterLDAPSearchFormat = "{0}"
End Sub

'Warning: Do not alter method name
Function GroupByFilter(Byval value as string) As string
  Return value
End Function
```

Figure 116: Script Editor for an organizational/geographical/custom Dynasty

The Dynasty Options Script Editor is a lightweight editor that not only fulfills the basic requirements of opening and saving files, but provides some advanced functions, such as color-coding for keywords, auto-complete, and a utility for testing your script.

Group-by attributes buttons

The editor creates a button for each group-by attribute and displays them in its left pane. Click a button to view code in commented form for the general settings defined for the corresponding group-by attribute. You can un-comment the code for the desired setting and customize it according to your requirement.

Group-by buttons are available for use with all Dynasties except managerial Dynasties.

Sample script for an Organizational Dynasty

The following lines of code customize the group-by filter to strip out the value of the group-by attribute after the slash (/), including the slash. This sample code also defines the LDAP search format in the FilterLDAPSearchFormat command.

NOTE Do not change the value of FilterMethodName. It should always be GroupByFilter.

```
'Warning: Do not alter method name
Sub SetDynastyOptions(Byval args as DynastyEventArgs)
'Uncomment below lines to customize
'args.GroupBy = "company"
'args.ChildContainer = "OU=Farzana,DC=tech2k8,DC=com"
'args.Separator = "-"
args.FilterMethodName = "GroupByFilter"
args.FilterLDAPSearchFormat = "{0}/*"
End Sub

'Warning: Do not alter method name
Function GroupByFilter(Byval value as string) As string
Return value.split("/")(0)
End Function
```

Sample Script for a Managerial Dynasty

The following lines of code customize the top manager logic by passing two top managers and have the dynasty structure built upon the top manager found in the directory.

```
'Warning: Do not alter method name
Sub SetDynastyOptions(Byval args as DynastyEventArgs)
'Uncomment below lines to customize
args.TopManager = ChooseTopManager ("CN=Farzana
Qureshi,CN=Users,DC=tech2k8,DC=com","CN=Faiqa
Usman,CN=Users,DC=tech2k8,DC=com"
'args.ExcludeNestedReports = False
'args.Container = "CN=Users,DC=tech2k8,DC=com"
'args.CreateFlatManagerialList = True
'args.IncludeManagerAsMember = False
End Sub

Function ChooseTopManager(ByVal mgr1 as String,ByVal mgr2
as String) as String
Dim entry as DirectoryEntry
```

```
entry =
ActiveDirectoryTool.BindToDirectoryEntry("CN=Users,DC=tech2
k8,DC=com","admin","abcd123R")
Dim result as
System.DirectoryServices.SearchResultCollection
Dim resultArray as System.Collections.ArrayList
result =
ActiveDirectoryTool.FindAll(entry,"(distinguishedName=" &
mgr1 & ")",1)
resultArray=ActiveDirectoryTool.SearchResultToDistinguished
NameList(result)

if resultArray.Count=1 then
return mgr1
else
return mgr2
end if
End Function
```

Writing Scripts

Scripts written in the script editor may include:

- The ATM Object
- PowerTools, provided their reference is added in Group Script Editor
- VB .NET keywords and operators
- VB .NET decision structures and loops
- Local variables
- VB .NET global string functions and other global functions
- VB .NET framework class library namespaces, objects, and methods
- COM objects with late binding

Some restrictions apply:

- No classes, modules, namespaces are allowed. If required, their references should be added in Group Script Editor.
- No module-level statements – such as Import or Option statements – are permitted.

The ATM object

Automate Transformation Manager (ATM) is a shared (static) object that is accessible from the Group Script Editor. ATM exposes the events for the membership update process. It also exposes methods and properties that enable you to access in-memory data structures and Query Designer attributes. The script in Group Script Editor is executed within the scope of ATM.

The following tables list the events that ATM exposes.

Public Members

Member	Description
Context (property)	Provides access to the in-memory context object.
AddToContext (method)	Adds a new data item to the context object.
CancelUpdate (method)	Cancels the membership update process.
RemoveFromContext (method)	Removes the specified item from the context object.

Public Events

Event	Description
Startup	The Startup event is raised when the membership update session starts. If PowerTools are used, they are initialized along with other objects.
BuildQuery	During BuildQuery, the settings from the Query Designer are used to construct the LDAP statement that will be executed to update the membership of the target group. The Query Designer settings are accessible within the scope of this event and can be accessed and changed using the QueryEventArgs object. NOTE Any changes to the attribute values are not permanent and are limited to the scope of the script. Therefore, if you open the Query Designer dialog box (Figure 88) after executing the script, the Query Designer settings will be the same as they were before executing the script.
MembershipUpdating	This event is raised before memberships are updated in memory. At this stage, memberships can be manipulated as required. The Query Designer smart attributes at this stage are also accessible, but any changes to their values will be ignored.

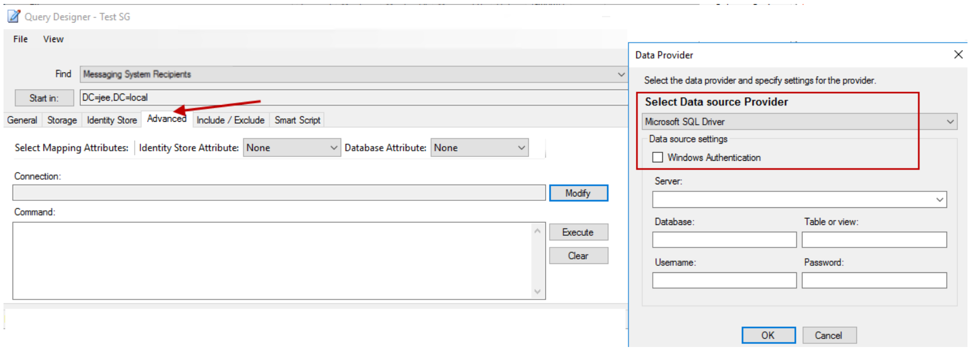
Event	Description
MembershipUpdated	Memberships have been updated in memory according to the query statement created in the BuildQuery event. NOTE Any changes to memberships at this stage are not validated and are considered a forced change. For example, if a new object is programmatically added to the membership, its existence on the source will not be validated.
MembershipCommitting	This event is raised before memberships are saved at the destination data source. Even at this stage, any changes to the memberships are considered to be forced and are not validated.
MembershipCommitted	Memberships are saved at the destination data source.
UpdateFailed	Any error that causes the job to fail raises this event. This event is useful for handling exceptions, such as logging the error, sending an email to the administrator, or adopting an alternate course of action for your code to continue ignoring the error.
Shutdown	The membership update session is about to finish. This event is useful for de-allocating resources, sending notifications, and other similar activities.

While you can manipulate the memberships of Smart Groups and Dynasties using different events in the membership update process, then group membership setting defined at the identity store level, such as Out of Bounds and Nesting Membership, still apply to them.

Appendix E

External database connectivity for ODBC and SQL driver

When you use an external data source for a Smart Group query, GroupID uses SQL authentication to connect to this data source. However, for Microsoft SQL Driver and ODBC connectors (only System DSN supported), you can choose to connect via Windows authentication.



Query Designer - Test SG

Find: Messaging System Recipients

Start in: DC=jee,DC=local

Select Mapping Attributes: Identity Store Attribute: None Database Attribute: None

Data Provider

Select the data provider and specify settings for the provider.

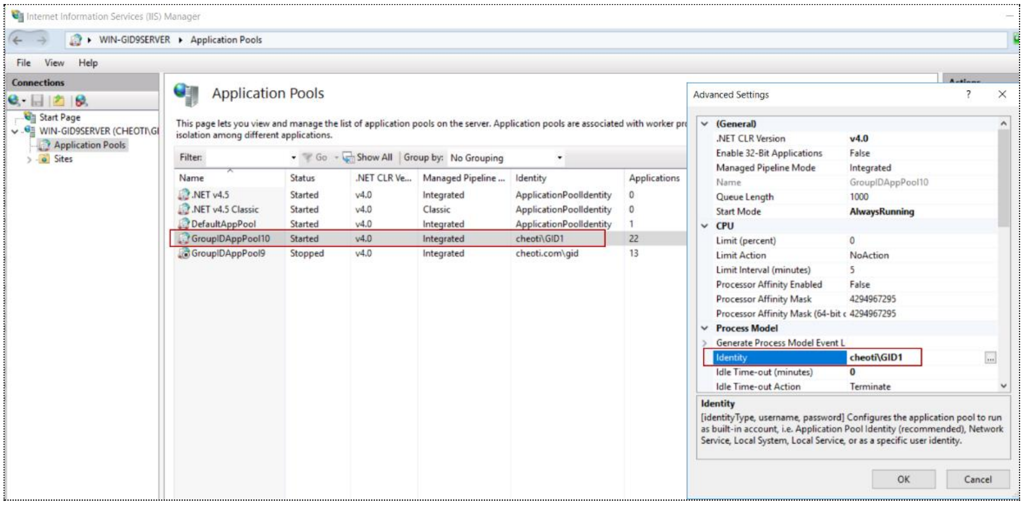
Select Data source Provider: Microsoft SQL Driver

Data source settings

☐ Windows Authentication

Figure 117: Authentication modes for data providers

When Windows authentication is selected for a data source provider (SQL Driver or ODBC) on the **Data Provider** dialog box, GroupID 10 uses the account configured in GroupIDAppPool10 to connect to the external data source.


Internet Information Services (IIS) Manager
WIN-GID9SERVER ▸ Application Pools
File View Help
Connections
Start Page
WIN-GID9SERVER (CHEOTI\GI
Application Pools
Sites
Application Pools
Filter: Go Show All Group by: No Grouping
Advanced Settings
OK
Cancel

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker pr
isolation among different applications.

Name	Status	.NET CLR Ve...	Managed Pipeline ...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	1
GroupIDAppPool10	Started	v4.0	Integrated	cheoti\GID1	22
GroupIDAppPool9	Stopped	v4.0	Integrated	cheoti.com\gid	13

(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Name	GroupIDAppPool10
Queue Length	1000
Start Mode	**AlwaysRunning**
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**cheoti\GID1**
Idle Time-out (minutes)	**0**
Idle Time-out Action	Terminate

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

Figure 118: GroupIDAppPool10 configured with domain account, cheoti\GID1

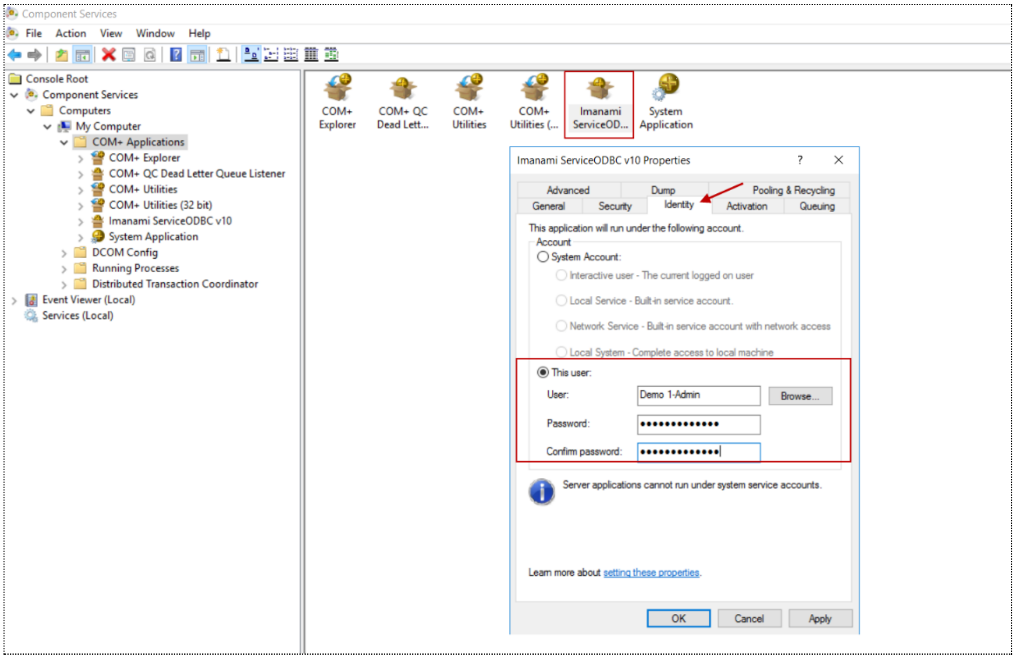
For the authentication mode (SQL authentication or Windows authentication), the following scenarios apply to the SQL Driver and ODBC data sources:

Scenario # 1: When GroupID 10 Data Service is connected to SQL Server via SQL authentication and SQL Server is on the same machine as GroupID.

In this case, GroupIDAppPool10 will be configured with a domain account or gMSA, as specified in the GroupID Configuration tool.

- For SQL Driver, if this domain account/gMSA is present in SQL Server with ‘db-owner’ rights on the respective database, the system will allow Query Designer to connect with SQL. Server (external data source).
- For ODBC, System DSN will work if the third-party database has a Windows login of the account configured in GroupIDAppPool10 in case of 64-bit System DSN.

  In case of 32-bit System DSN, the system will not look for the account configured in GroupIDAppPool10 in IIS, but will use the credentials configured in Imanami ServiceODBC v10 (provided that the user credentials exist in third party database with Windows login).



Imanami ServiceODBC v10 Properties

This application will run under the following account.

Account

○ System Account:

○ Interactive user - The current logged on user

○ Local Service - Built-in service account.

○ Network Service - Built-in service account with network access

○ Local System - Complete access to local machine

● This user:

User: Demo 1-Admin

Password: •••••••••••••

Confirm password: •••••••••••••

Server applications cannot run under system service accounts.

Learn more about setting these properties.

Figure 119: Credentials configured in Imanami ServiceODBC v10

Scenario # 2: When GroupID 10 Data Service is connected to SQL Server via Windows authentication and SQL Server is on the same machine as GroupID.

In this case, the account configured in GroupIDAppPool10 should have Windows login and ‘db owner’ rights on the respective database source.

For ODBC, the behavior is the same as discussed in Scenario # 1.

Scenario # 3: When GroupID 10 Data Service is connected to SQL Server via SQL authentication and SQL Server is on a machine other than the GroupID machine.

In this case, GroupIDAppPool10 will be configured with a domain account or gMSA.

- For SQL Driver, GroupIDSSUser will not be able to connect with SQL Server since it is a local account.
- For ODBC, the behavior is the same as discussed in Scenario # 1.

Scenario # 4: When GroupID 10 Data Service is connected to SQL Server via Windows authentication and SQL Server is on a machine other than the GroupID machine.

In this case, a domain account will be configured in GroupIDAppPool10 and it should have Windows login in the respective database source.

For ODBC, the behavior is the same as discussed in Scenario # 1.

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