IDENTITY
AUTOMATION

Roles Module

Agenda

01 Overview

02 Use Cases

03 Settings, Attributes

04 Views (My, Team, Other)

05 Create a Role, Add/View Members

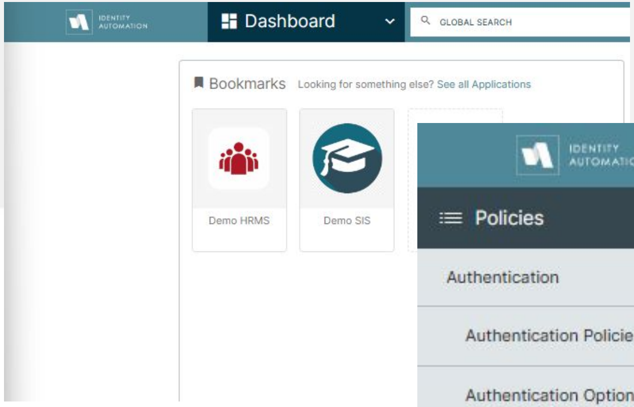
06 Sync Roles

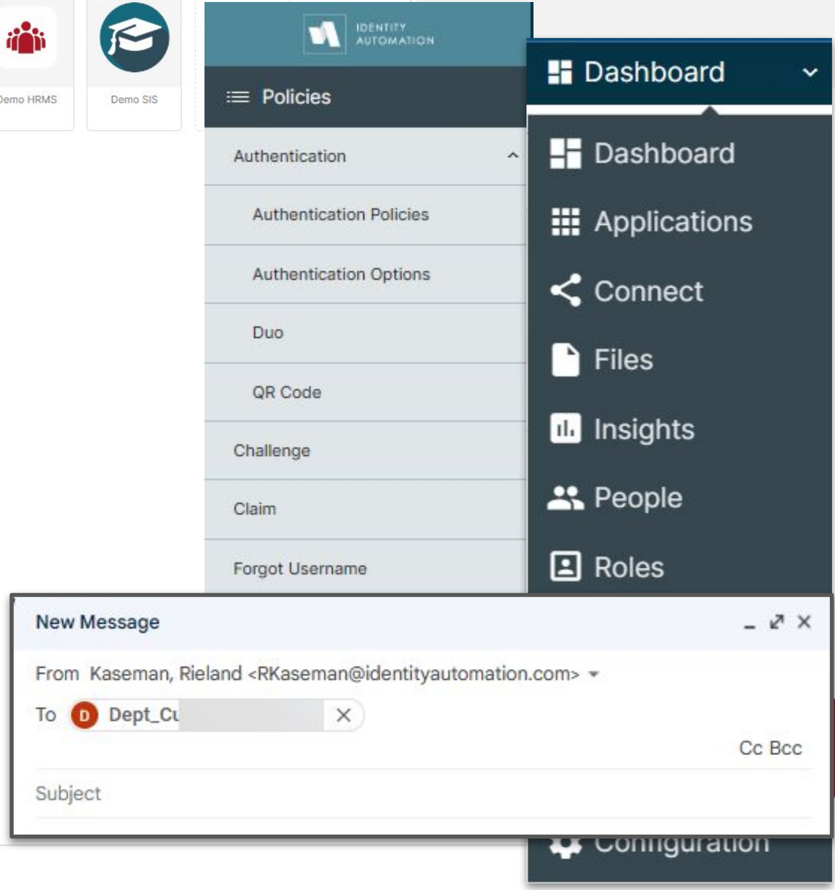
Roles Module - Overview

- Roles are groups of accounts that share something in common, i.e. all staff, or all teachers, students in grade 9, students at a specific school
- Sounds similar to delegations, except delegations are used to perform actions on accounts (password, MFA, unlock, etc), and are restricted to the RI ecosystem, where Roles are used to grant access or for email groups
- Roles can sync to external systems, Active Directory (cloud), Google Workspace, AzureAD, O365

Roles Module - Use Cases

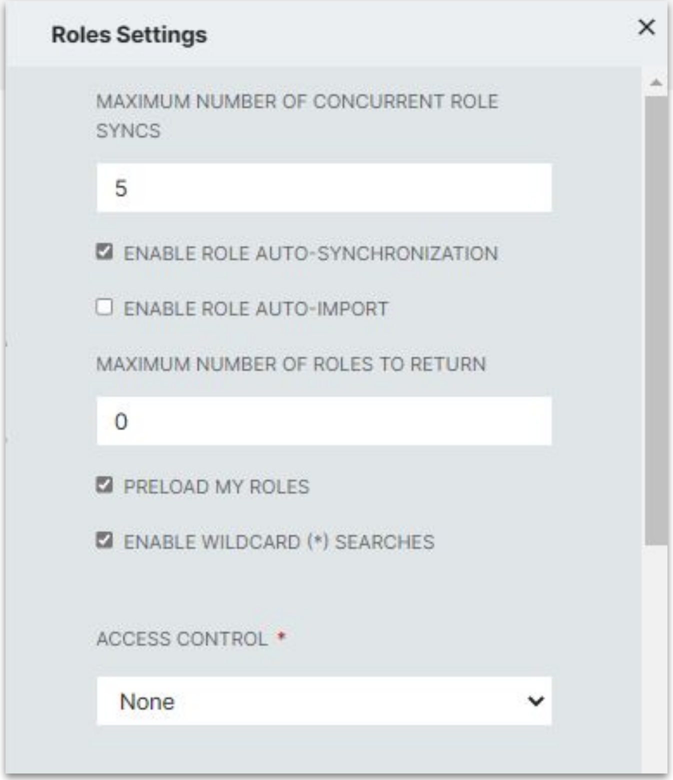
- Security groups in RapidIdentity
  - Grant access to Applications
  - Policies (Authentication, Challenge, Claim, etc.)
  - Module access (Applications, People, Roles, etc.)
- Sync to Active Directory for security groups (Network drives, applications, device or printer access, etc.)
- Sync to Google Workspace for email distribution lists, Shared Drive access, Google Apps access
- Sync to Office 365 for Outlook distribution lists





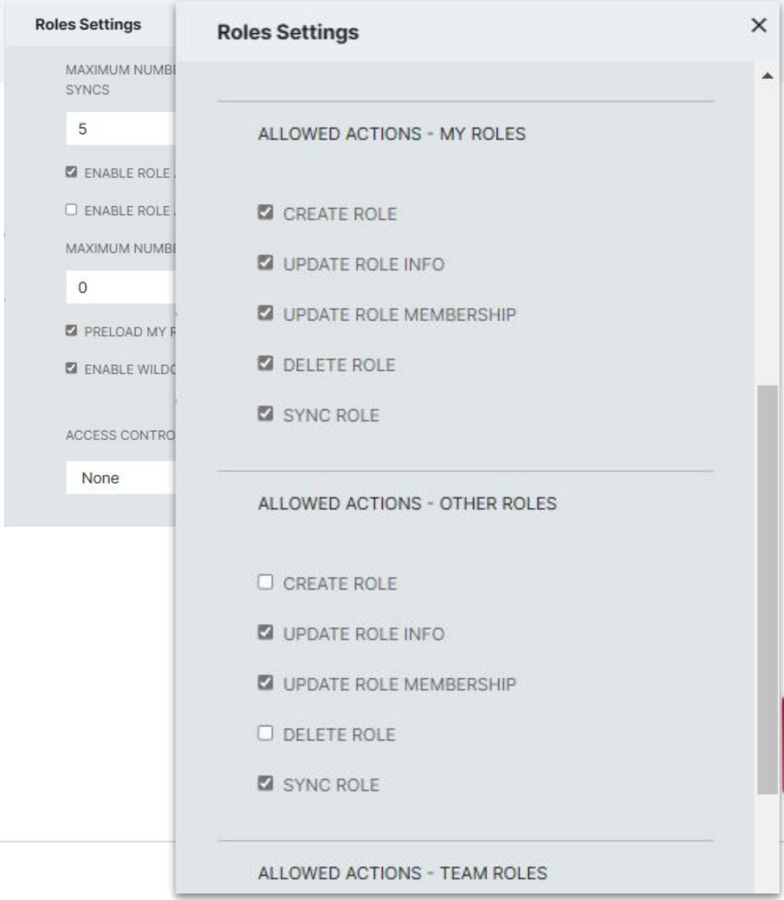
Roles - Settings

- At the bottom left, choose Settings > General
- Maximum Number of Concurrent Role Syncs
    - Leave this at 5, or fewer
- Enable Role Auto-Synchronization
- Enable Role Auto-Import
- Maximum Number of Roles to Return
- Preload “My Roles”, also applies to Team Roles
- Enable Wildcard (*) Searches
- Access Control: Role-Based or Attribute-Based



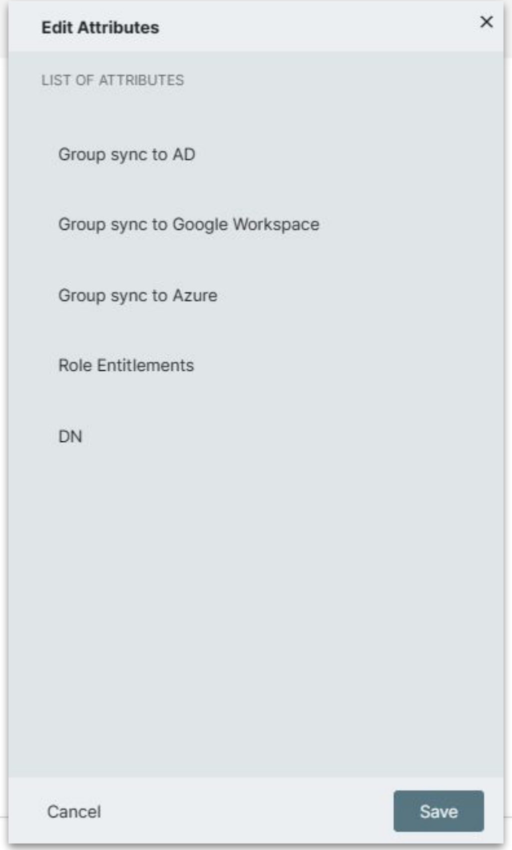
Roles - Settings

- Allowed Actions on “My Roles”
- Allowed Actions on “Team Roles”
- Allowed Actions on “Other Roles”



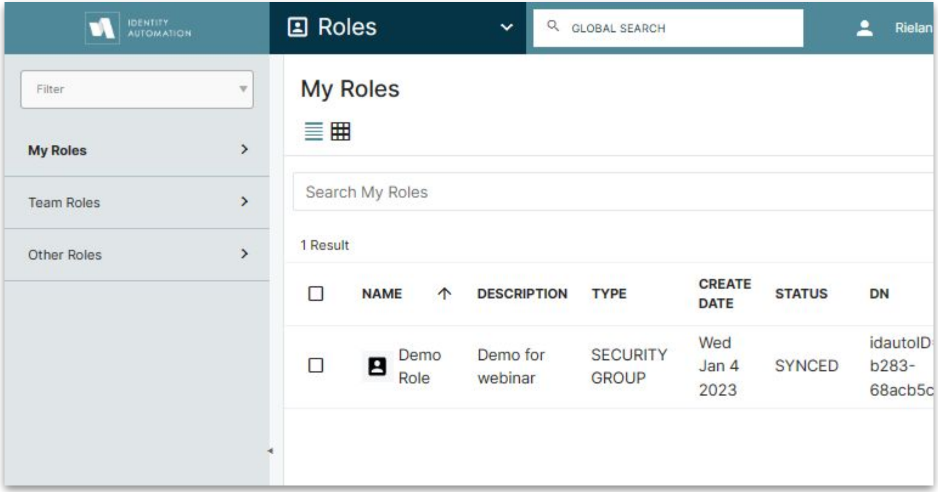
Roles - Settings - Attributes

- At the bottom left, select Settings > Attributes
- Any group attribute can be added here, but may not function as expected if the attribute is not added to the group sync action set
- Hover between the attributes or at the bottom to Add a New Attribute (just like attributes on a People delegation)
- Hover an existing attribute to edit, drag/drop to reorder, or delete



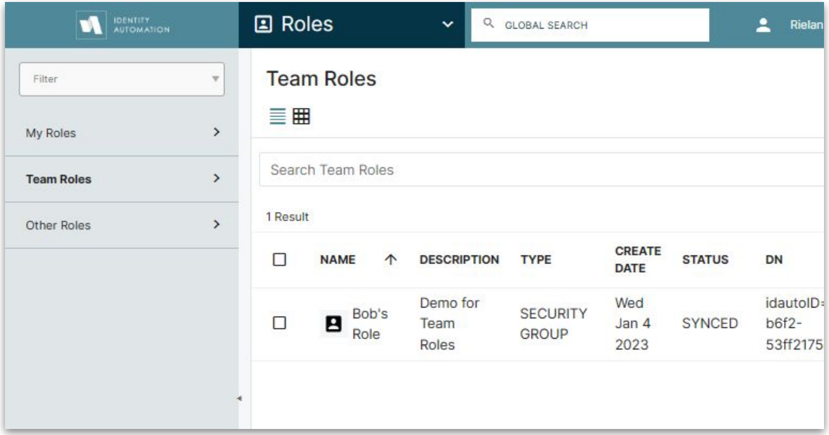
Roles - My Roles

- These are the roles where you are the assigned Owner or Membership Manager, created by you or created by a role admin and assigned to you
- Preload the list is controlled under General Settings



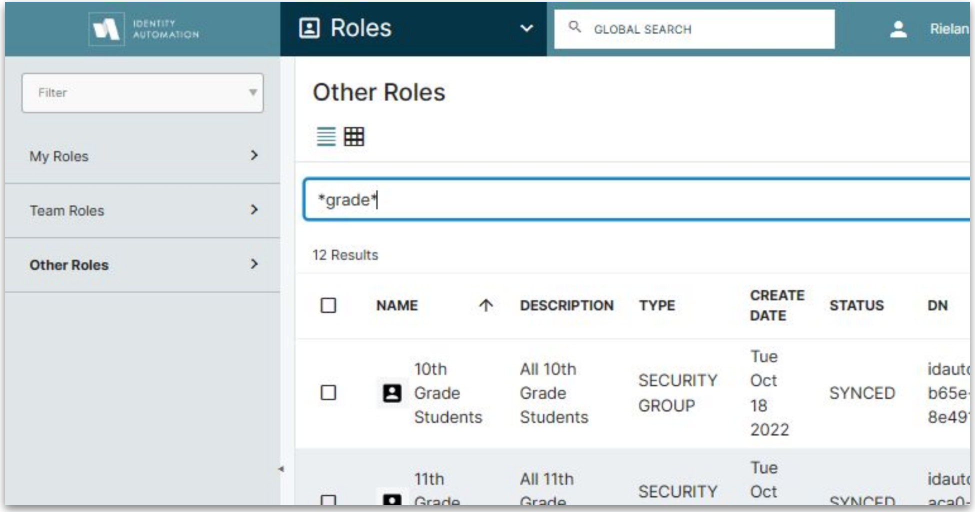
Roles - Team Roles

- You are a manager and must have at least one direct report, using the Manager attribute (e.g. Bob Jones has Rieland Kaseman in the Manager attribute on his account)
- The direct report (Bob) must be a member of the “Portal Roles Manager” role
- The direct report must be the owner of at least one role
- You will see Team Roles on the left menu, but they will not; the roles they own are viewed under their My Roles menu option



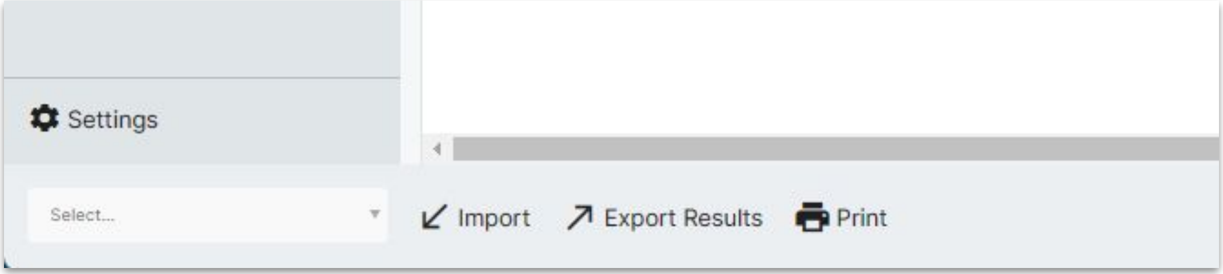
Roles - Other Roles

- If you are a tenant or system admin, you can view all roles, regardless of owner or membership manager
- Must search for roles by default - there’s no setting to preload results



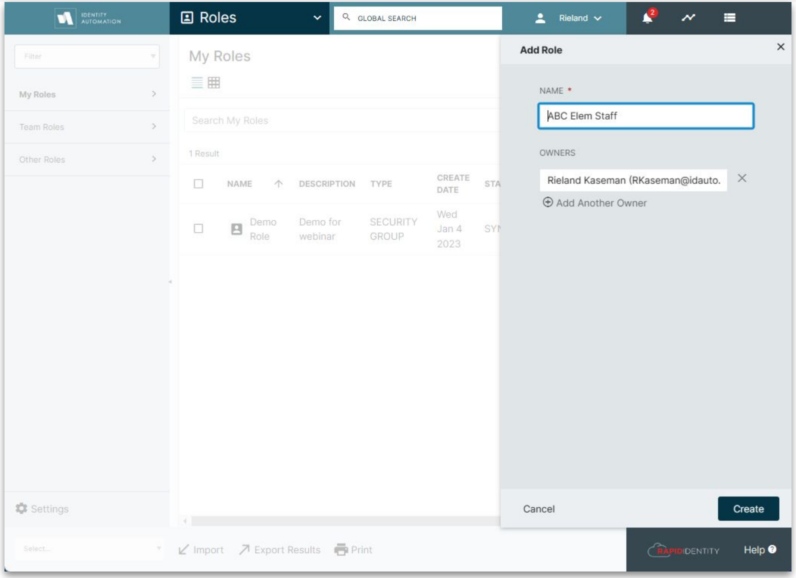
Roles - Other Roles

- At the bottom of each page, there is an option to Import roles created in Active Directory
  - Must have an owner (user dn) in the idautoGroupOwner attribute
  - Max limit of 500 static members
  - Search for the topic “import roles” on help.rapididentity.com for detailed instructions
- Export and Print is for the list of group names (does not include the members)



Roles - Create a Role

- Select **Add Role** at the top right (the Add Role button is made available or restricted under General Settings)
- Give the role a succinct name, keeping in mind some systems (like Google) may have length limitations
- Search for your name to be the owner
- Roles can have multiple owners, so select Add Another Owner to assign more than one
  - Role Owners must be a member of the “Portal Role Manager” security group
  - Roles can be owned by a service account to avoid having to reassign ownership upon employee turnover.



Roles - Create a Role

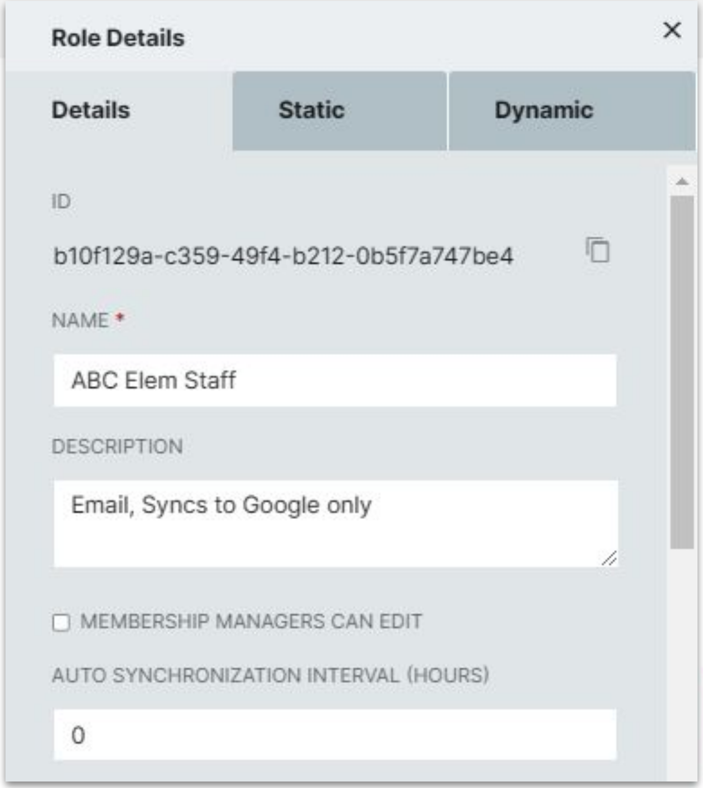
- ID is the group's GUID that can be used in queries, action sets, searching log files
- Description - 256 characters to describe the group
- Membership Manager Can Edit
  - Owners can create, edit and delete groups and members
  - Membership Managers can add or remove members
  - If this box is checked, they can also edit details on this pane and Dynamic LDAP filters
- Auto Synchronization Interval (Hours)
  - Frequency of auto-sync to AD, Google, Azure, used when dynamic filters manage membership

    0=Never (used for static members)

    1= Every hour

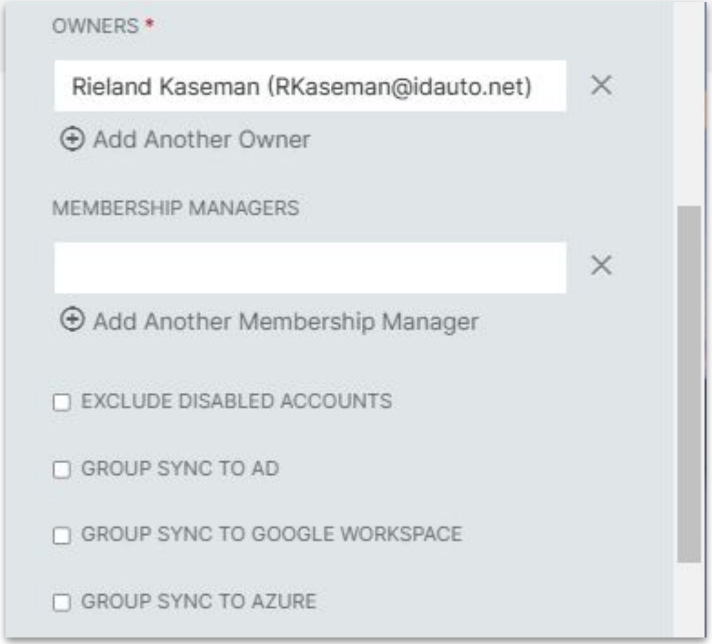
    4=Every 6 hours/4 times per day

    24=Once per day



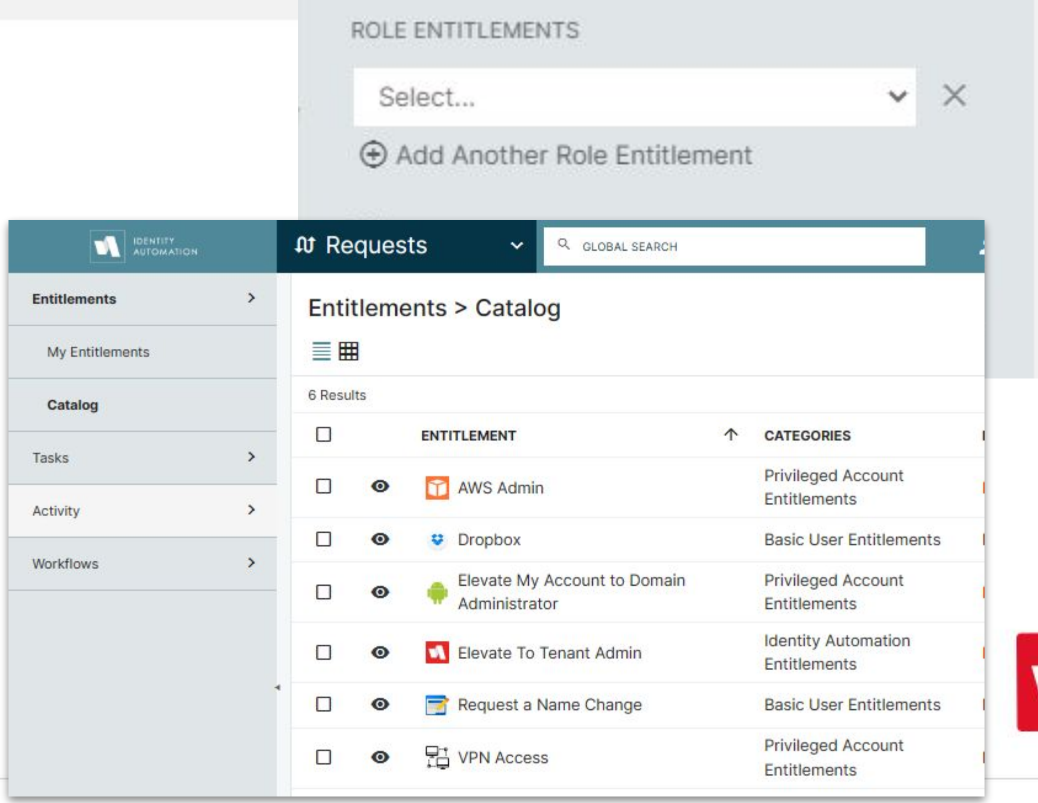
Roles - Create a Role

- Owners
  - Add multiple users to own this group
  - Click the X on the right to remove an owner
  - Can’t save the group without at least one owner
- Membership Managers
  - Add one or more names to delegate member updates
- Exclude Disabled Accounts (Cloud only)
  - Should always be checked
  - Removes inactive accounts for email distribution lists
  - Removes members for licensing groups
  - *On-prem customers can use this in LDAP include filter: (!(userAccountControl:1.2.840.113556.1.4.803:=2))*
- Group Sync to AD/Google Workspace/Azure
  - Granular controls over syncing groups to these systems
  - Must have corresponding logic in the group sync action set



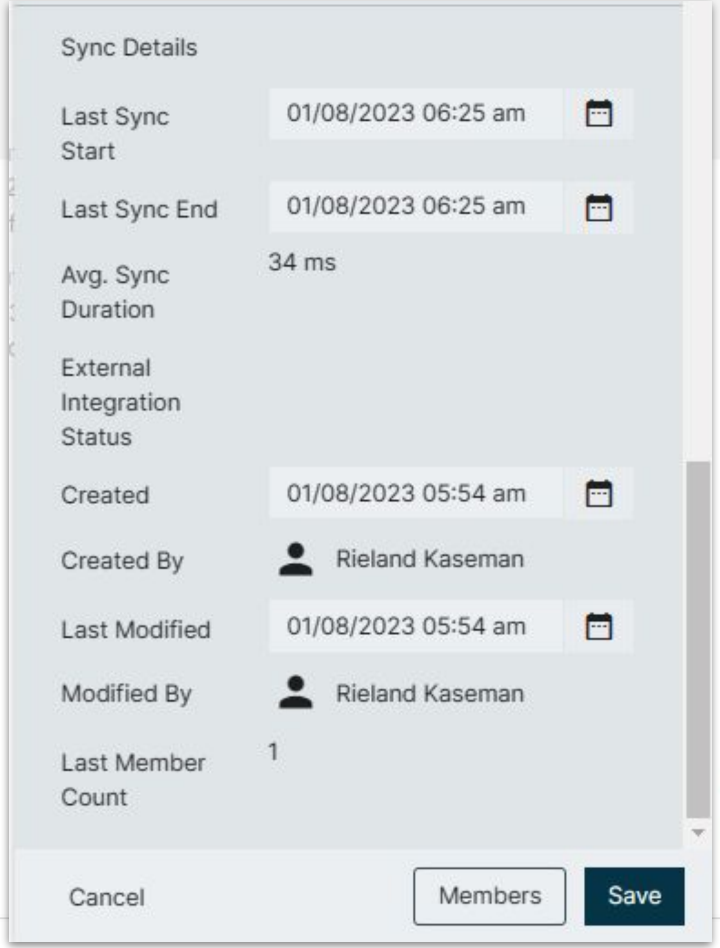
Roles - Create a Role

- Role Entitlements
  - The members of this role are automatically granted the corresponding entitlement in the Requests (Governance) module
  - Search “Governance use cases” on help.rapididentity.com for ideas how to automate repeatable processes
  - To discuss Governance licensing, please contact your Customer Success Manager



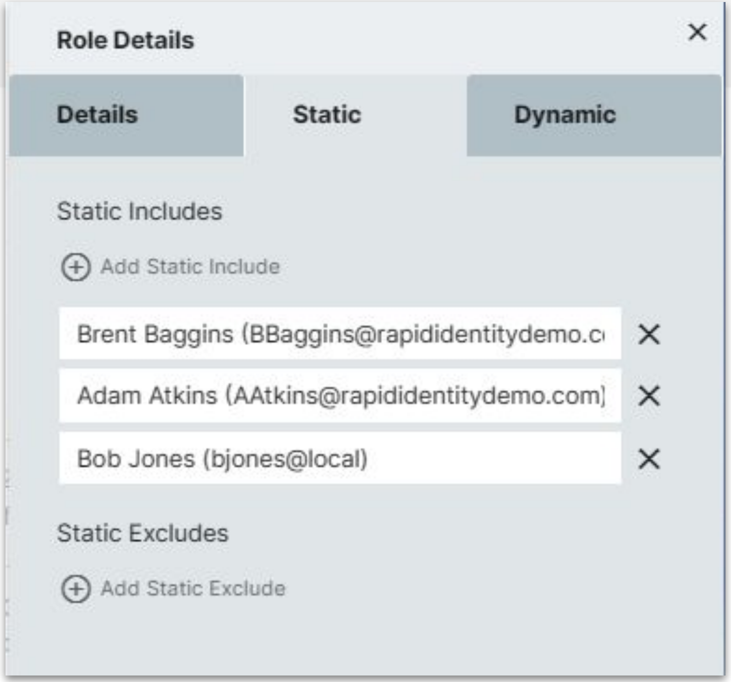
Roles - Create a Role

- Sync Details (can't edit these, for information only)
  - Last Sync Start/End - Verify this role is syncing as scheduled, this is the start date/time for auto-sync
  - Average Sync Duration - Should be measured in milliseconds or seconds
  - External Integration Status - for roles syncing to AD/Google/Azure
  - Created - Date and person
  - Last Modified - Date and person, this records who changed the group details and dynamic filter, and when the changes were made
  - Last Member Count - Number of confirmed members as of the last sync (does not include Add or Remove Pending)



Roles - Members

- Static tab
  - Accounts are manually added and removed by name
  - Useful when members have no attributes in common (location, department, job titles, employee type, etc.)
- Static Include
  - Adds the member to the group
  - Click Add Static Include, then search the People directory (includes students and sponsored accounts)
  - Click the X on the right to remove the member
- Static Exclude
  - Useful when the majority of the group membership is Dynamic, but one or more accounts needs to be excluded
- When using static memberships and syncing to AD, keep in mind the limit of max 500 members



Roles - Members

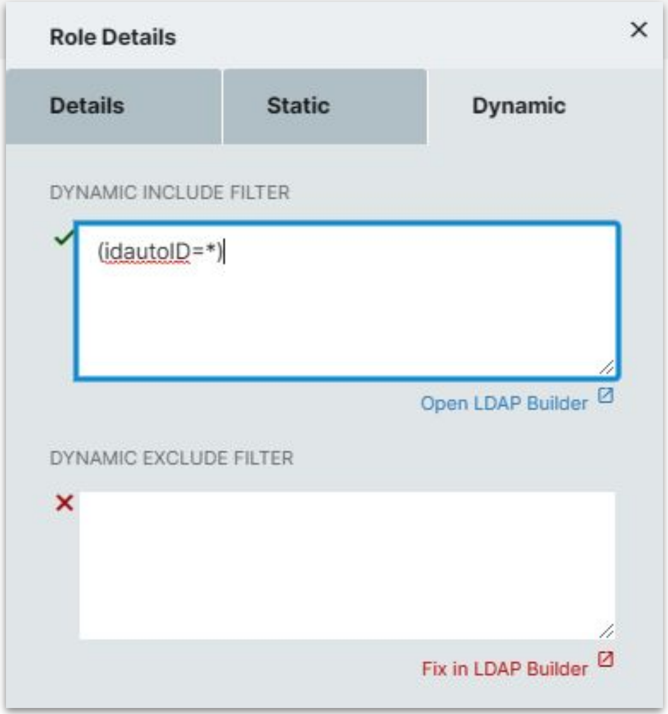
- Dynamic tab
    - Uses LDAP filters to populate group members with accounts in RapidIdentity that have matching attributes

<u>Everyone:</u>
idautoID=*

<u>ABC Elementary staff:</u>
(&(idautoPersonLocName=ABC Elementary)(employeeType=Staff))

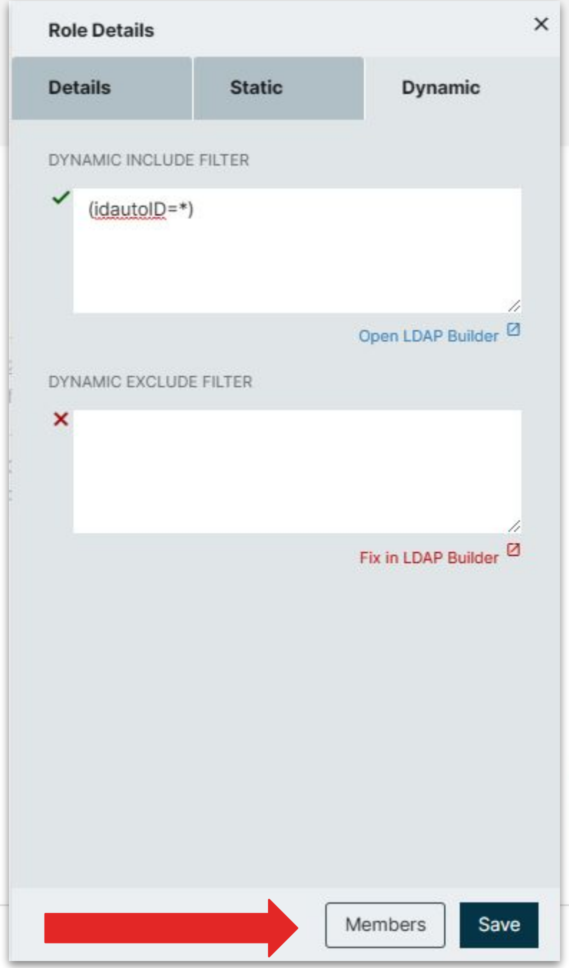
<u>ABC Elementary students:</u>
(&(idautoPersonLocName=ABC Elementary)(employeeType=Student))

<u>ABC Elementary Teachers:</u>
(&(idautoPersonLocName=ABC Elementary)(employeeType=Staff)(idautoPersonJobTitle=Teacher))



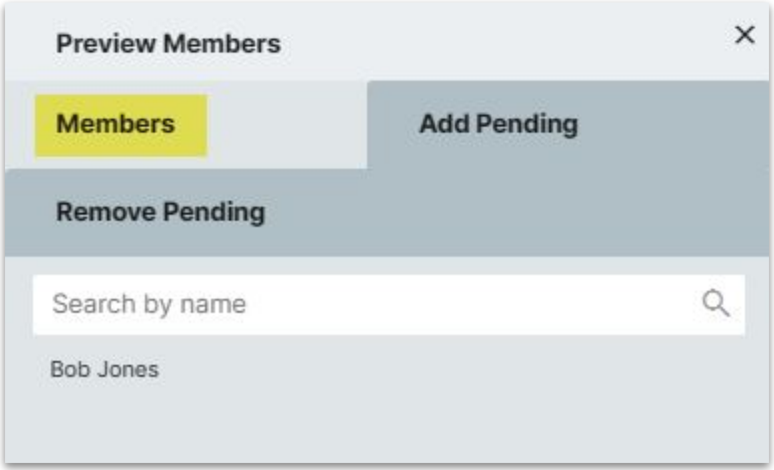
Roles - Members

- Select the Members button at the bottom of any of the tabs



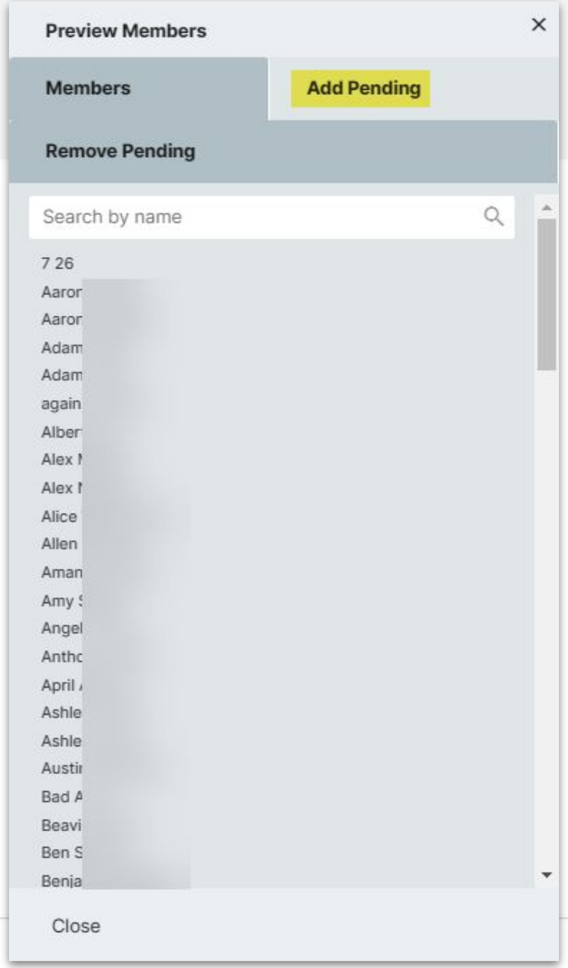
Roles - View Members

- The light background is the active tab
- Members - Shows who is actually a member of the group as of the last sync
- Use the Search By Name field to quickly find a member on a long list



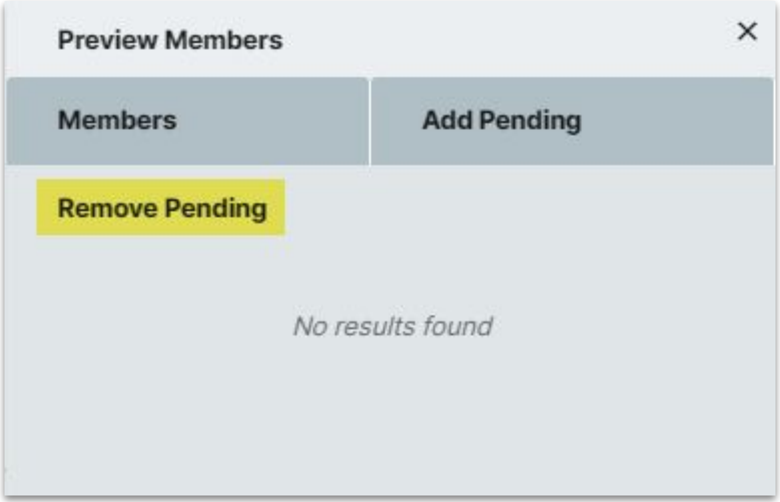
Roles - View Members

- Add Pending - Shows the accounts that will be added the next time the group syncs (auto or on-demand)
- These are not official members, and have not synced to external systems yet, or do not have policies applied in RI
- This is useful when creating or modifying LDAP filters to confirm the membership is what you expect



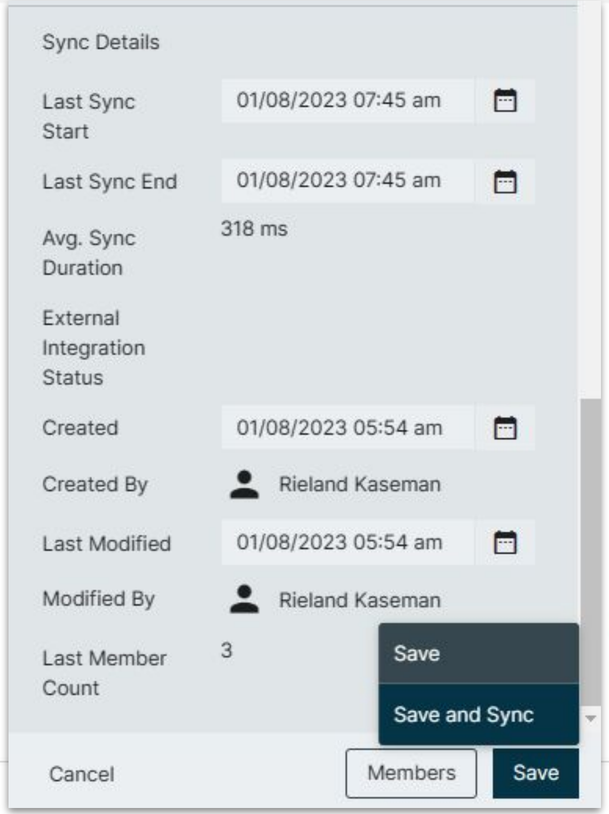
Roles - View Members

- Remove Pending - Shows the accounts that will be removed the next time the group syncs (auto or on-demand)
- These accounts are still members and have not any security or access revoked yet



Roles - Sync

- When the members are correct, close the Members view
- Save and Sync - Forces an immediate sync
  - Always force a sync when the group is created so the action set can schedule it based on Last Sync Start + auto-sync interval
  - Always force a sync when there are only static members, not dynamic
- Save - Let the action set sync the group the next time it's scheduled to run
- The Sync Details at the bottom of the Details tab will be updated with the next sync



Thank you for joining us today!

Link to this webinar will be posted on help.rapididentity.com
where you can also view upcoming events

We invite you back on Thursday at 2:00 CST for
tips and tricks to write LDAP filters!