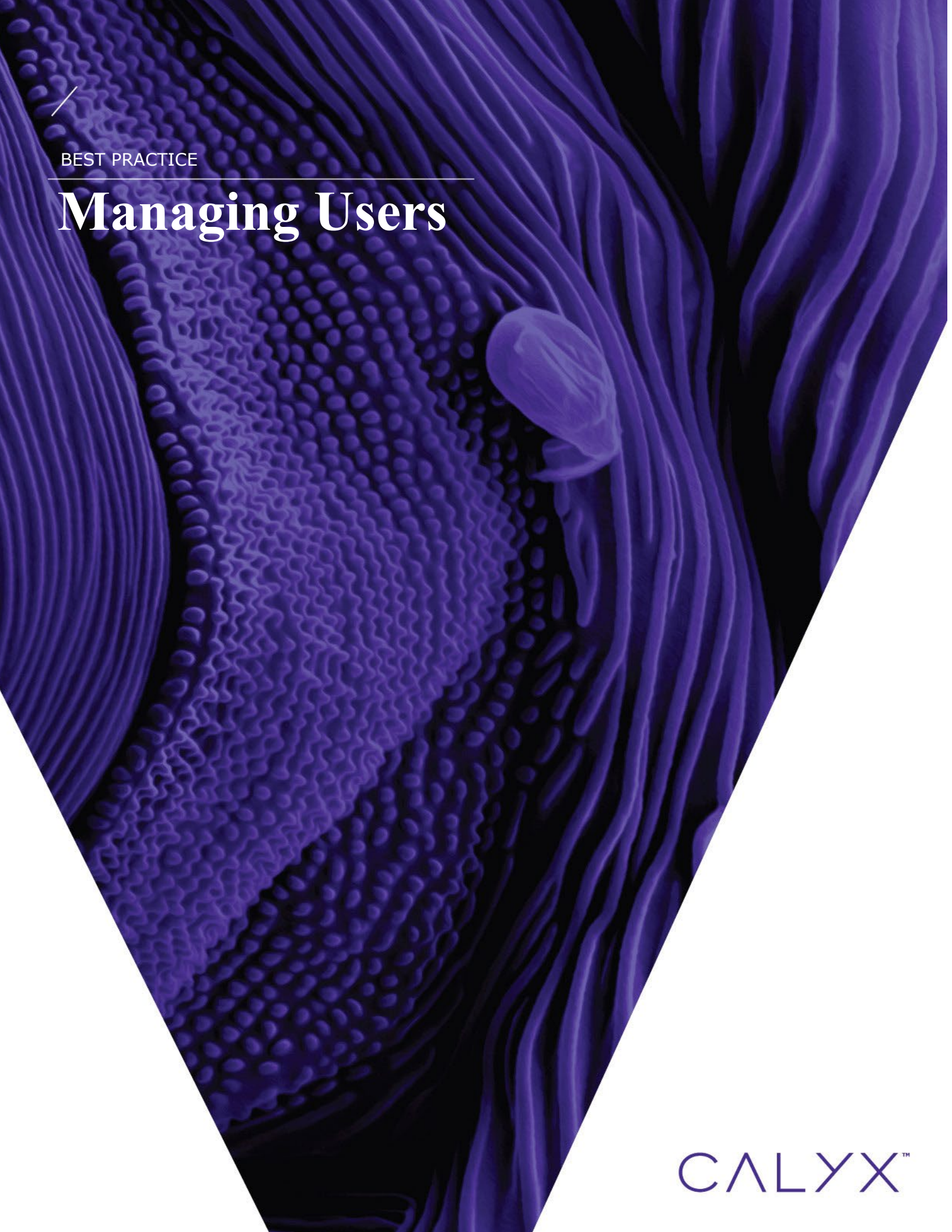


BEST PRACTICE

Managing Users

CALYX™

EN

Copyright and License Notice

EN

1 Contents

1 Contents 2
2 Revision History 3
3 Managing Provisioned Users with System for Cross-Domain Identity Management (SCIM) 3
3.1 Disabling a user via SCIM 3
3.2 Adding a user via SCIM 4
4 Inactivating users via the User Interface 4
4.1 Calyx RIM Registrations and Publishing 4
4.2 4
4.3 Calyx RIM Viewing 5

2 Revision History

When Calyx releases a new major or minor version of Calyx RIM, Release Notes are issued which explain the new features and updates. These Release Notes are reviewed by Calyx RIM Business Consulting to determine any impact to current Best Practices and identify any new Best Practices:

- Impact = Best Practice is impacted by a new version
- No Impact = Best Practice is not impacted by a new version

When a new version impacts Best Practice documentation, Calyx recommends that clients review the entire Release Notes for a full understanding of all changes associated with this Best Practice documentation.

Software Version	Release/Revision Date	Summary of Change(s) (Refer to Release Notes for Full Description)
v7.2 and v6.0 (Viewer)	10 January 2024	First release

3 Managing Provisioned Users with System for Cross-Domain Identity Management (SCIM)

The System for Cross-Domain Identity Management (SCIM) user management API enables automatic provisioning of users and groups between Azure AD to Calyx Applications. As SCIM provisioning is configured in a client's Azure AD environment, the designated environment Administrator must manage the users and groups that are provisioned into the Calyx Applications.

Best Practice Recommendations for Managing SCIM Users:

- Only add groups containing users that are required to access the Calyx application.
- Any user that is no longer required to be enabled in a Calyx application should be removed from the Azure AD group that is being used for SCIM Provisioning. This will trigger disabling of the user in the Calyx Application during the next SCIM Provisioning cycle.

3.1 Disabling a user via SCIM

Please note that:

- Disabling users from Security Admin in the Calyx RIM Application not remove the user from the application.
- Removing users from Azure AD Enterprise Application SCIM Provisioning does not remove the user or group from the application. It will disable the user or group in the application.

To disable a user in the Calyx Application through SCIM provisioning:

- Navigate to Microsoft Azure > Microsoft Entra ID > Enterprise Applications > {your application name}.
- On the Enterprise Application page for your Application, select “Users and groups”.
- Remove any listed groups or users that are not required to be provisioned through SCIM. If you do not see a user directly listed, open the corresponding group, and remove the user directly from that group in Azure AD to disable the user in the associated Calyx Application.

Please allow up to one hour for the provisioning cycle to complete and disable users or groups in the application database.

3.2 Adding a user via SCIM

To add a user to the Calyx Application through SCIM provisioning:

- Navigate to Microsoft Azure > Microsoft Entra ID > Enterprise Applications > {your application name}.
- On the Enterprise Application page for your Application, select “Users and groups”, then select “Add user/group” button.
- On the “Add Assignments” page, select “Users and groups”.
- Search and select any necessary Users or groups that should be provisioned to the Calyx application.
- Click “Select” and then “Assign”.

Please allow up to one hour for provisioning cycle to add users or groups into the application database.

4 Inactivating users via the User Interface

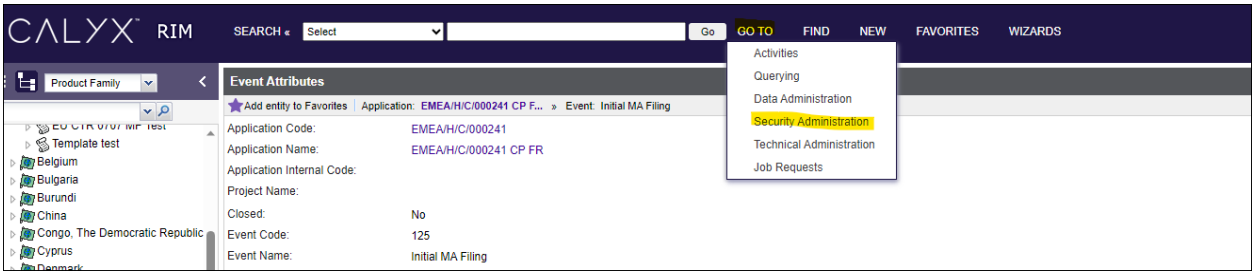
4.1 Calyx RIM Registrations and Publishing

For user accounts, the best practice is to disable users via SCIM. In the event this is not possible or to expedite the process the RIM system allows for the modification of users, by users with appropriate administrator access, using the RIM Security Administration as outlined below:

4.2

To modify a user or group:

1. Choose Go To > Security Administration. The Security Administration page opens listing all the users and groups.



2. Click the link for the user or group you want to modify. The Privilege Detail page for the user or group opens.
3. Do any of the following:
   - To disable the user/group, choose Disable as of and enter the date when the user/group should no longer be able to log into Calyx RIM. If you do not specify a date, the user/group will remain enabled.
   - To remove a user from a group, click Disassociate User from the Group, then change the privileges for the user. The User Type for an overridden user on the Privilege Detail page is STANDALONE.

Note: If the user does not belong to an IdP (Identity Provider) group and you click Disassociate User from the Group, the field-level/page-level security assigned to the role with which the user is associated is retained unless you specifically move the user to a different role.

- Click Re-associate User with the Group to replace the user's privileges with those defined for the IdP group.

Note: Before you re-associate a user with a group, remove the user from any roles with which he or she has been associated.

- Change the security privileges for the user/group.

4. Click Save when you are finished.

4.3 Calyx RIM Viewing

Accounts of users not required to use Viewing can be made inactive by a Calyx RIM administrator.

To deactivate users:

1. Click Edit User.
2. Select the user name and click Edit.
3. Select Inactive and click Save.

You can delete any user account in the system using the Delete option on the Edit User window.

1. Click Edit User to open the Edit User window.
2. Select the user from the User Name list.
3. Delete.
   - Click Yes to confirm deletion.
   - Click No to retain the user.