Roles

Last Modified on 02/09/2022 9:41 am EST

User Management

SAP Open Connectors, a capability of SAP Integration Suite, offers two roles for accessing the functionality with a stable set of permissions. User roles define what a specific user assigned to the role can do in SAP Open Connectors. The roles are with respect to SAP Open Connectors and do not apply to SAP Business Technology Platform.

- **Default User** (default-user): non-administrator role for users in accounts, allows you to, for example:
  - View profiles
  - Access resources (like Common Resources, Formulas, and Connector API requests)
- **Account Administrator** (admin): self-administering role for users which allows you to, for example,
  - View, add, edit, delete account users
  - View logs accounts
  - Reset account passwords
  - View profiles
  - View, create, edit, delete Connectors,
  - Create Connector instances,
  - View identity users
  - Access resources (like Common Resources, Formulas, and Connector API requests)
  - Edit security settings

The Default User (default-user) is automatically assigned by the system , when you add a new user to the account. You need to assign the Account Administrator (admin) manually. To have the Account Administrator role assigned, reach out to your existing Account Administrator.

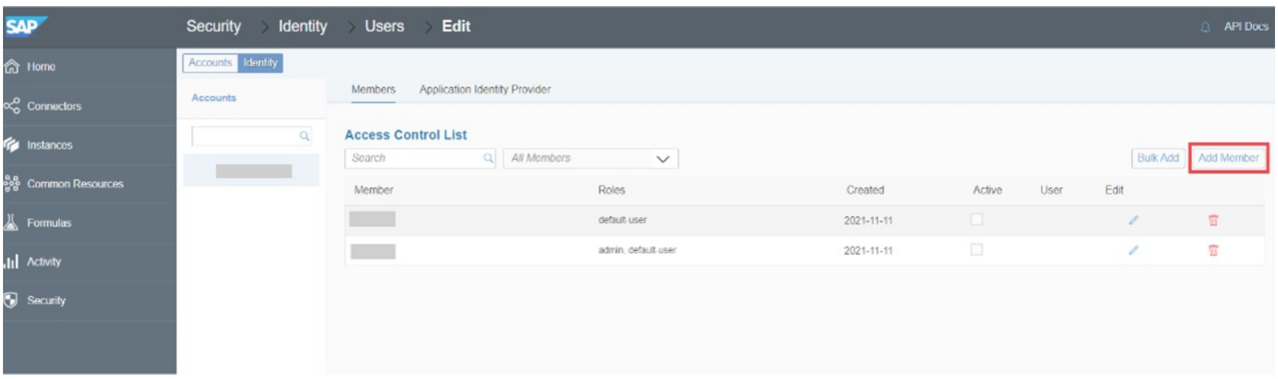
User Management via UI

Assigning Users

The user who creates the account is automatically assigned as the Account Administrator.

To add the Account Administrator role to other members,

1. Go to **Identity tab > Add Member**.
2. Select **Edit** and assign the role accordingly.
3. Click **Save**.



To assign a user as an administrator,

1. Go to **Access Control List**.
2. Select the member and click **Edit**.
3. Then check the checkbox for admin to assign the role and click **Save**.

Deleting or Unassigning Users

To unassign a user as an administrator,

1. Go to **Access Control List.**
2. Select the member and click **Edit**.
3. Then uncheck the checkbox for admin and click **Save.**

To delete a user,

1. Go to **Access Control List**.
2. Select the member and click **Delete**.
3. Then confirm when the **Are You Sure?** dialog appears and the user is deleted.

To deactivate a user,

1. Go to **Access Control List**.
2. Select the member and check the **Active** checkbox.

Note: Consider the following implications when deleting users:
- All user instances are deleted, including VDRs and formulas.
- If there are events or bulks available for the user, they are deleted after seven days.
- Logs will remain until the log retention time (90 days).

User Management via API

Account Administrators can assign the account administrator role to an existing default user by using APIs:

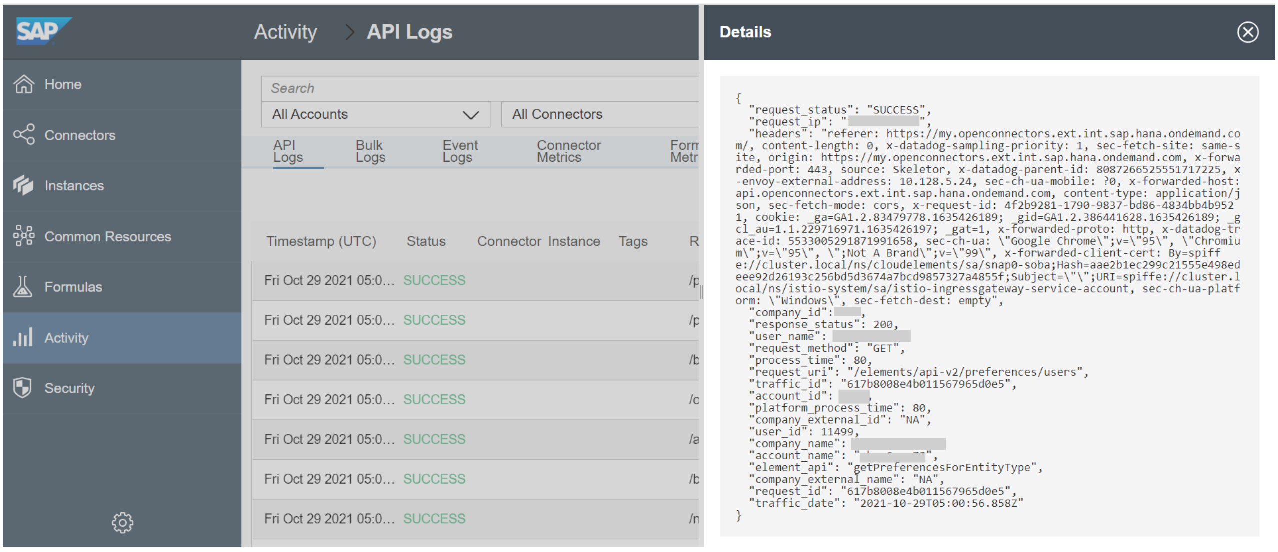
Type	API	Definition	Response fields
Change	PATCH /users/{id}	Update or edit a user associated with a given ID within your account.	• Timestamp • Response Code • Account
Remove	DELETE /users/{userId}/roles/{roleKey}	Revoke user roles associated with a given ID within your account.	• Timestamp • Response Code • Account
Assign	PUT /users/{userId}/roles/{roleKey}	Grant the Account Administrator role associated with a given ID within your account.	• Timestamp • Response Code • Account
Get	GET /users/{id}/roles	Search for all the roles and personal data related to the user ID.	• Timestamp • Response Code • Account

Note: For checking if one of the above APIs has been used,refer to the API logs with respect to Timestamp.

Personal Data Management

Read Personal Data Change Logs

Use **API logs** in the Activity tab to get a list of all the activities for a given time frame, including API calls along with any updates made to user permissions by the Account Administrator. For more details on activities, select the request and check the details pop-up as shown in the following example.



Retrieve Personal Data

Information related to a user including all the related data stored in the background, such as, for example, first name, can be downloaded via APIs. You can download user related data from an API request, which can be performed by account administrators only.