# **Alteryx Admin Task:** **User Admin Task:** This section contains admin tasks on provisioning and maintaining users, their roles, and their permissions within the Alteryx Analytics Cloud. 1. Manage User 2. Create Role **1. Manage User:** Administrators can manage permitted Alteryx Analytics Cloud (AAC) users.

# All of these functions are available through the Admin console. For more information, go to Admin Console.

# **Sort and Filter Users**

# To easily find users, you can sort based on name or last active time. To sort, select the **Name** or **Last Active** column in the table header.

## You can also filter users by status and roles. To filter users, select the **filter icon** on the right side of the Status or Roles column name in the table header. Select the status or roles you want to filter by, then select **Apply**. Note that for the Roles column, you can also sort for roles that aren't assigned to a user **A. Invite User**

To permit a user to access AAC, an administrator must complete the following steps.

1. Sign in to AAC as an administrator.
2. From the left navigation bar, select **Profile menu > Workspace Admin > Users**.
3. On the Users page, select **Invite**.
4. In the Invite Users dialog, enter a comma-separated list of email addresses to which to send invites.
   1. These addresses become the user identifier for signing in to AAC.
   2. Avoid sending invites to email aliases.
   3. Example:

joe.smith@example.com, mary.jones@example.com

1. To grant product access, you can assign additional roles to the users in the Invite Users dialog. For more information, go to the Roles Page.
2. To invite the list of users and set their roles, select **Invite**.
3. Each valid user receives an email at the email address that you listed. The receiving user must click the link in the email to accept the invitation.

### After the user accepts the invitation, you can find their user account in AAC. You can then modify the user account as needed before the user chooses to sign in. **B. Re-Invite Users**

Admins can re-invite users through the UI or API. For API instructions, go to the API documentation. To re-invite users through the UI, admins have 2 options from the 3-dot menu:

* **Re-invite User**: Send an additional invitation email to an invited user. To re-invite multiple users, either check the box in the table header to select all users or check the boxes for specific users, then select the **Re-invite User(s)** option that becomes available in the table header.
* **Copy Invite URL**: Copy the invitation URL for an invited user.

## **C. Edit User**

### Add or Remove Roles

1. On the Users page, check the box next to each user. If you want to select all users, check the box on the left side of the table header.
2. Select **Add Roles** or **Remove Roles** on the right side of the table header.
3. Add or Remove roles for the selected users, then select **Save**.

### **D. Edit roles**

1. On the Users page, locate the user to review.
2. On the right side of the row for the user, select the 3-dot menu.
3. Select **Edit Roles**.
4. In the dialog, you can add and remove roles for the user account.
5. When finished, select **Save**.

## **E. Disable User**

If needed, you can disable a user's account and prevent their access to AAC.

* The user can no longer sign in to AAC or use any available API endpoints.
* AAC retains the user's assets. Other users who have permission can still access them.

To disable a single user, complete these steps:

1. On the Users page, locate the user to disable.
2. On the right side of the row for the user, select the 3-dot menu.
3. Select **Disable**, then select **Disable** again to confirm.
4. To reactivate a disabled member, select **Enable**.
5. Effective immediately, the user can't sign in to the application.

**To disable multiple users, complete these steps:**

1. On the Users page, check the box next to each user. If you want to select all users, check the box on the left side of the table header.
2. Select **Disable** on the right side of the table header, then select **Disable** again to confirm. To reactivate disabled members, select **Enable**.
3. Effective immediately, the users can’t sign in to the application.

## **F. Remove User**

To remove a user completely, please complete the following steps.

1. On the Users page, locate the user to remove.
2. On the right side of the row for the user, select the 3-dot menu.
3. Select **Remove**.
4. If the user owns assets, you can choose to assign them to another user. If you don't assign them, you will lose the assets.
5. Confirm that you wish to remove the user.

**2. Create Role:**  Administrators can create and assign roles to users to govern access to user-created objects in the Alteryx Analytics Cloud.

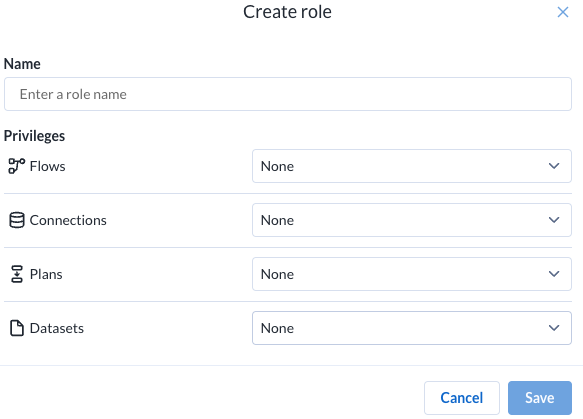
* A role is a set of privileges that can be assigned to users.
* A privilege governs access level to a type of object.
* By default, all users are assigned the default role, which allows users to use the user-created object types.
* For more information, see Privileges and Roles Reference.

As needed, you can create user roles to define different access levels for different object types.

**Create Role**

To create a new role, please complete the following steps.

**Steps:**

1. In the left nav bar, select **User menu > Admin console > Roles**.
2. In the Roles page, review the list of available roles. For more information, see Roles Page.
3. To create a new role, click **Create Role**.

# In the Create Role dialog, specify the following:

# **Name:**Enter a name for your role. This value must be unique among available roles.

# **Privileges:**

# For each of the available object types, specify the access level for the role.

# For more information on these privileges, see Privileges and Roles Reference.

# To create the role, click **Save**.

# The role is now available and can be assigned to users. See below.

# **Example - Read-only access role**

# Suppose you wish to limit a set of users to read-only access to role-based objects.

# **Steps:**

# In the Roles page, click **Create role**.

# In the Create Role dialog, enter the following:

# Name: read-only

# Privileges: For each available privilege, select viewer.

# Click **Save**.

# The role is now available and can be assigned to users. See below.

# **Example - Empty role**

# In some circumstances, you may wish to assign an empty role to a user. For example, you may wish to limit some administrators to only be able to configure aspects of the platform without providing access to any user-created objects.

# **Steps:**

# In the Roles page, click **Create role**.

# In the Create Role dialog, enter the following:

# Name: empty

# Privileges:

# For every privilege, select none.

# Click **Save**.

# The role is now available and can be assigned to users. See below.

# **Assign Role**

# After a role has been created, you can assign it to users.

# **Steps:**

# In the Roles page, locate the role to assign.

# On the right side of the screen, click the context menu for the role. Select **Assign role...**.

# In the Assign role dialog, enter a list of email addresses for users to whom you wish to assign the role.

# Click **Assign**.

# The role and its associated privileges are applied immediately to the user account(s).

# **Modify Role**

# After a role has been created, you can modify it as needed.

# **Steps:**

# In the Roles page, locate the role to modify.

# In the context menu on the right side of the page, select **Edit**.

# Review the privileges assigned to the role, and make any changes as necessary.

# Click **Save**.

# All users who currently have the role in their account immediately receive the changed privileges.

# **Unassign Role**

# Use the following steps to remove a role from a user account.

# **Steps:**

# In the Roles page, locate the role that you wish to remove from one or more user accounts.

# Select the role.

# In the Role Details page, click the Users tab.

# Locate the user to un-assign the role. In the context menu for the user, select **Unassign from role**.

# The user no longer has the role in the account.

# **Delete Role**

# **Steps:**

# In the Roles page, locate the role to delete. In the context menu, select **Delete**.

# Confirm the deletion.

# The role is deleted. All users who had the role can no longer access the privileges assigned in the role.

**Alteryx Patch Update Guide**

Alteryx now lets you update your Designer or Server software with patches, so you don't have to completely uninstall and reinstall the program. This makes the update process quicker and reduces downtime.

**Key Points:**

1. **Patch Updates vs. Major Releases**:
   * Patches fix bugs but don't add new features.
   * Major releases (e.g., 21.2, 21.3, 21.4) still happen as usual.
2. **Benefits of Patch Updates**:
   * Fix bugs between major releases.
   * Easier and faster to install than the old stable/minor releases.
3. **Installing Patches**:

**Scenario 1: Patch Your Existing Major Version**:

* + If you already have a major version installed (e.g., 21.4.2), you can just install the patch over it.
  + The build number stays the same, but you can see the patch number in Designer under Help > About or in the InstallInfo.ini file.
    - **Non-Admin Version**: C:\Users<username>\AppData\Local\Alteryx\Settings
    - **Admin Version**: C:\Program Files\Alteryx\Settings
  + The file will show something like PatchNumber=x.

**Scenario 2: Upgrade to a New Major Version with Patches**:

* + If you have an older major version (e.g., 21.3.x), you can upgrade directly to a new major version with patches (e.g., 21.4.2 with Patch 1).
  + This involves a full uninstall and reinstall.
  + The new version number indicates it's patched.

1. **Before Installing a Patch**:
   * **For Designer**: Close the program before installing the patch.
   * **For Server**: Stop Alteryx-related processes in Windows Task Manager before installing the patch. They will restart automatically after the installation.
2. **Downloading and Installing a Patch**:
   * Go to the Alteryx Licensing & Downloads portal.
   * Select either Alteryx Designer or Server.
   * Choose the product version.
   * Download the Admin or Non-Admin version patch.
   * Run the installer and follow the instructions.

# 