External identity provider setup (Optional)

Many organisations, particularly those running a multi-account AWS environment, use **AWS IAM Identity Center** with an external identity provider such as **Microsoft Active Directory, Microsoft Entra ID, or Okta**. This allows centralised identity management, where one platform governs access across multiple enterprise systems.

If your organisation uses an external identity platform (for example, Entra), you will need to align its group setup with **Sandbox Studio's IAM Identity Center groups**.

Default Groups in IAM Identity Center

When you install Sandbox Studio, the solution automatically provisions **three groups** in IAM Identity Center. These groups control access based on role type:

1. Administrators

Responsible for configuring and maintaining Sandbox Studio. Administrators are responsible for:

- Setting global policies (e.g. maximum budgets and cleanup rules).
- Provisioning new sandbox accounts and monitoring the sandbox account pool.
- Overseeing security and governance settings.

2. Managers

Oversee day-to-day sandbox usage within a department or team. Managers are responsible for

- Approving or rejecting sandbox requests within their team/department.
- Creating and managing account templates including budgets, pre-provisioned resources and permissions.
- Tracking spending and activity for supervised accounts.

3. Sandbox Users

Login to sandbox accounts and use them for development, testing, training, or experimentation.

Group Naming

The **default names** created by Sandbox Studio are:

- `<namespace>_SsAdminsGroup`
- `<namespace>_SsManagersGroup`
- `<namespace>_SsUsersGroup`

You can change these names during installation.

> **Important:** You must create groups in your external identity platform (e.g. Entra, Okta) with the **exact same names** you configure in Sandbox Studio.

Linking External Identity Provider Groups

1. **Create Groups in Your Identity Platform**
   - Create groups in Entra/Okta/AD that match the IAM Identity Center group names.
   - Example: If your namespace is `Acme`, create `Acme_SsAdminsGroup`, `Acme_SsManagersGroup`, and `Acme_SsUsersGroup`.
2. **Assign Users to Groups in Your Identity Platform**
   - Add users to the relevant group based on their role.
   - Example: Developers should be added to the `SsUsersGroup`, team leads to `SsManagersGroup`, and central admins to `SsAdminsGroup`.
3. **Synchronisation with IAM Identity Center**
   - IAM Identity Center automatically syncs external groups.
   - Once a user is added to the external group, they will inherit the corresponding **Sandbox Studio role and permissions**.

Revision #2
Created 2025-08-28 05:31:18 UTC by Andy
Updated 2025-08-29 07:40:34 UTC by Andy