Managing users in ArcGIS Enterprise

Objectives

- Manage licensing.
- Manage user privileges.
- Create members.
- Delete members.

Introduction

In this chapter, you'll learn how to manage the members of your ArcGIS Enterprise organization. Setting the appropriate member configurations is important because it affects who will be able to sign in to your ArcGIS Enterprise portal and what they will be able to do after they sign in.

Licensing

Each member is licensed to access certain capabilities of ArcGIS Enterprise. The primary way to assign licenses is to give a member a particular user type. Beyond their user type, members may also have add-on licenses for applications and user type extensions.

A Portal for ArcGIS license file specifies the number and variety of user types and add-on licenses you have available to assign to members. Talk with your Esri representative to make sure you have the right quantity and types of licenses for the work your members need to do.

User type

Every member of your ArcGIS Enterprise portal must be assigned only one user type. A user type defines the capabilities they have within ArcGIS Enterprise and the default set of applications that they can access and use. The specific details of what each user type enables can vary between versions of ArcGIS Enterprise but fall broadly into four categories:

- **Viewing:** Members with any user type have the capability to view content that has been shared with them by other members.
- **Editing:** Some user types provide members with the capability to edit data in content items that have been shared with them by other members.
- **Creating:** Some user types allow members to create content items. The creating capability includes making maps and apps, publishing layers, and performing analysis.
- **App access:** A member's user type will determine which apps they can access. For a given user type, these apps could include ArcGIS Pro as well as web apps, such as ArcGIS Dashboards, ArcGIS Instant Apps, and ArcGIS Experience Builder.

For example, members with the Viewer user type can view items that have been shared with them, but they do not have the capability to own, create, or edit data for those items. The Viewer user type also has the capability to use fundamental web apps, such as Dashboards or ArcGIS StoryMaps℠. Members with the Professional user type, on the other hand, have the capability to view, own, and edit content items and have access to a broader range of apps, such as ArcGIS Notebooks and ArcGIS Pro.

Check the documentation for your version of ArcGIS Enterprise so that you can assign your members the user type that best matches the capabilities and apps they require to do their work.

Add-on licenses

Some members may require access to additional apps beyond the default granted by their user type. For example, a member assigned the Contributor user type does not include access to ArcGIS Pro and would need an add-on license to use it.

When you think about the add-on licenses you require, consider the interaction between the add-on licenses and the member's user types. For example, instead of a Contributor user type and an add-on license for ArcGIS Pro, you may be able to reduce costs and administrative overhead by assigning the member a user type that includes ArcGIS Pro.

User privileges

Distinct from a member's capabilities, each member also has a set of privileges. Although privileges are not the same as capabilities, they are related, and the privileges granted to a user must be compatible with the capabilities defined by their user type. For example, the

Contributor user type enables the capability to view and edit data that has been shared with them. A member with the Contributor user type could be granted the privilege to view data. That member could not, however, be granted the privilege to own content, since that is not one of the capabilities the Contributor user type has.

Privileges are defined in two categories: general and administrative. General privileges allow members to perform common user workflows, such as creating groups, sharing content items, publishing layers, and editing data. Administrative privileges allow members to change the ArcGIS Enterprise deployment or change other members' content. These privileges include federating ArcGIS Server sites, adding members, and reassigning ownership.

When an administrator assigns privileges, an important security best practice is the principle of least privilege: A user should have access to every capability they need to do their job, but they should not have access to any capability they do not need. Members with any administrative privileges have the authority to make impactful changes to your ArcGIS Enterprise deployment. Excessive administrative privileges could cause serious problems for your organization. For that reason, an organization will typically have many more users with general privileges than administrative privileges. Although the privileges in the **General** category have less impact on the functionality of your ArcGIS Enterprise deployment, you should still adhere to the principle of least privilege when granting these privileges.

Default roles

When you first install and configure ArcGIS Enterprise, there are default roles representing bundles of privileges that are broadly appropriate for a few member personas.
- The default **Viewer** role can view content items that have been shared with them but cannot do anything else.
- The default **Data Editor** role can view and make edits to the data of content items that have been shared with them but cannot create, own, or share items.
- The default **User** role has most general privileges but cannot create or edit services.
- The default **Publisher** role has access to nearly all general privileges. Notably, the default **Publisher** role can create and edit services as well as view, create, own, edit, and share portal content items.
- The default **Administrator** role has every privilege.

There are some special considerations for the default Administrator role. At least one member must be assigned this role. It is a good idea to have more than one member assigned a default Administrator role so that administrative tasks can still be done even if one administrator is unavailable.

The specific available privileges and compatible user types for each default role can change between versions of ArcGIS Enterprise. Refer to the documentation for your version of ArcGIS Enterprise for a list of privileges and compatible user types. If a member's user type

is incompatible with the role you want to assign them, you will need to change their user type to a compatible one first.

Custom roles

The default roles may not be appropriate for all members of your organization. It may be the case that a member needs to perform work that does not match any default role. For example, a member may need to create and edit Notebooks, which is a privilege that is granted by default only to the Administrator role. If that member does not require the full set of administrator privileges to do their job, you should not grant them that role. Instead, you should create a custom role that better aligns with the principle of least privilege.

Most likely, the custom role you need for a member will be similar to an existing role. You can start with that role and add or remove privileges from the full list of privileges, as necessary.

When selecting privileges for a custom role, be aware of the compatible user types for that bundle of privileges. You are not able to assign a role to a member that includes privileges that are incompatible with the capabilities included in their user type. For example, a member with the Viewer user type cannot have a custom role that includes the privilege to create, update, and delete content items, since that is not a capability of the Viewer user type. As with default roles, you may need to assign the member a new compatible user type before assigning them the custom role.

User role versus user type

People occasionally conflate *user type* and *user role*, but it is important to understand that they are different. User types are the first decision you make. It is your way to make sure you have the right user types to provide the capabilities that all your users need to do their job. Then assign each member a role with the privileges they need.

Member categories

Starting at ArcGIS Enterprise 11.1, you can organize the members of your ArcGIS Enterprise portal into hierarchical categories to help manage members by job role, department, or other characteristics. Categories are convenient for filtering and selecting members to manage in bulk. For example, if all the members of a team should be added to a particular ArcGIS Enterprise group, as an administrator, you can use categories to filter and select all those members at once instead of searching for them individually by name.

Members can belong to multiple categories. The hierarchical design of member categories means that when you add a member to a category, they are automatically added to every category above it in the hierarchy. You can set a member's categories when you create the member account, and you can set or change those categories at any time.

Creating members

To allow a user to sign in to ArcGIS Enterprise, you must add them as a member to your ArcGIS Enterprise organization. The process for adding members may depend on the authentication process you have set up to access ArcGIS Enterprise. See chapter 4 for details on authentication options.

If you are using the built-in identity store, you will specify the member's name, email address, username, user type, user role, and password. You must provide a username and password to the member, and you should require them to change that password the first time they sign in.

If you are using an external identity store, such as Security Assertion Markup Language (SAML) or Active Directory for member authentication, you can search for members in that identity store. Because these types of user accounts are separate from ArcGIS Enterprise, the name, email, username, and password are already configured. However, you must still configure a user type and compatible user role.

External identity stores may also have predefined groups of users, which you may be able to use to help add members. For example, if you use Active Directory as the external identity store, you can add members in bulk by their group. Members who are added this way will have the same user type and user role when they are first added.

Regardless of the authentication scheme you have configured for ArcGIS Enterprise, you can add members in bulk by specifying the relevant information in a text file. When you add members this way, the ArcGIS Enterprise portal will provide a CSV template you can download with the required fields for bulk member creation.

You can also configure ArcGIS Enterprise to allow users to add themselves as members if you configure new member defaults in the ArcGIS Enterprise portal organization settings. Each member will create their account the first time they sign in to the organization site. Be careful when using this option because you may rapidly run out of available user type licenses. Generally, it is best to use the Viewer user type and Viewer user role as defaults and update the user type and user role for members who require additional capabilities.

One good use case for having members add themselves is when you are not sure who in your organization will want access to ArcGIS Enterprise. Allowing members to add themselves when needed means that you don't have to consume a license until a user actively starts using the capabilities of ArcGIS Enterprise.

Fictional user story

Every summer, Medio County hires about 15 interns who work across county departments. Everybody who works for the county requires some level of access to capabilities in the county's ArcGIS Enterprise deployment, and interns are no different. Elise Medina, the county GIS manager, is responsible for making sure the interns can access appropriate capabilities, apps, and privileges necessary to do their jobs.

Some interns will work directly for Elise in the GIS department. These interns will perform analysis, manage data, and publish data to ArcGIS Enterprise, mostly using ArcGIS Pro. Elise assigns these interns the Professional user type. She has learned from experience over the years not to grant interns the full privileges of the default Publisher role, so she assigns them a custom Intern Publisher role that disallows unnecessary privileges such as publishing in bulk and sharing content with the public.

For Parks Department interns who will collect and update data using ArcGIS Field Maps, Elise assigns them the Mobile Worker user type and the Data editor role. For the other interns, Elise assigns them the Viewer user type and Viewer role.

As part of the member creation process, Elise assigns all the interns to the Intern member category.

Deleting members

You may occasionally need to delete members. This might happen if a user leaves your organization or if their job role changes in a way that means they should no longer have access to content or ArcGIS Enterprise organization resources. When you delete a member, their licenses are revoked and made available for you to reassign. You can delete members individually or in bulk.

Members who own content items or groups cannot be deleted while they still own those items or groups. For this reason, members who were added automatically from an external identity store such as Active Directory are not automatically removed if they are deleted from that identity store.

It may take some time to determine what should happen to the groups and content owned by members you are deleting. While you make that determination, you can quickly disable a member's account to prevent them from signing in or using an organization's resources. Disabling accounts is also a good option for members who should have their access to capabilities temporarily removed, such as people who are on leave.

Fictional user story

At the end of the summer, Elise needs to delete the interns' member accounts from the ArcGIS Enterprise portal.

Three of the interns from ArcGIS Enterprise have been hired into full-time positions with the county. From the Members tab of the Organization page, Elise selects these three members and recategorizes them to remove the Intern category.

Each departing intern was supposed to delete any unneeded content or groups and transfer the remainder to a new owner, but Elise knows from experience that sometimes that doesn't happen. Before deleting any members, she runs a Python script that transfers any groups owned by any user in the Intern member category to herself.

After running the script, Elise selects the remaining members of the Intern category and deletes them in bulk, choosing the option to transfer their content to herself. After the interns' accounts are deleted, she will go through the leftover content and groups she now owns and reassign any that should have a different owner.

7

Tutorial 7: Create a new member with appropriate privileges

In this tutorial, you will practice the workflows for managing members. You will create a member, investigate available licenses and roles, create and assign a custom role, create and assign a member category, and delete the member.

This tutorial involves making changes in your ArcGIS Enterprise portal. The changes in this tutorial are low risk because they do not involve your current members, content, or ArcGIS Enterprise configuration. It is still recommended, however, that you perform the steps of this tutorial in a test or development environment to avoid any risk of inadvertently making undesired changes to your production environment.

Create a new member

1. Sign in to ArcGIS Enterprise with an account assigned the default **Administrator** role or a custom role with appropriate privileges.

2. Navigate to the **Organization** tab.

95

3. Click the **Members** tab and then click **Add Members**.

4. Choose the option to **Add built-in portal members** and then click **Next**.

5. Click **New member**.

6. Complete the **New member** information with the following values:
   - **First name**: Test
   - **Last name**: Viewer
   - **Email address**: test.viewer@invalid.internal
   - **Username**: test.viewer
   - **User type**: Viewer
   - **Role**: Viewer
   - **Password**: test.viewer1

Note: You must have at least one available Viewer user type, and the assigned username cannot belong to any existing member.

| Member	User type	Role	Included licenses	
Test Viewer TV test.viewer · test.viewer@invalid.internal	Viewer	Viewer		

7. Click **Next** and then continue to accept the default values for other member properties.

8. Click **Add members**.

View options for changing member licensing and user role

1. From the **Members** tab, click the three horizontal dots (menu button) for the Test Viewer member you just created and then click **Manage user type**.
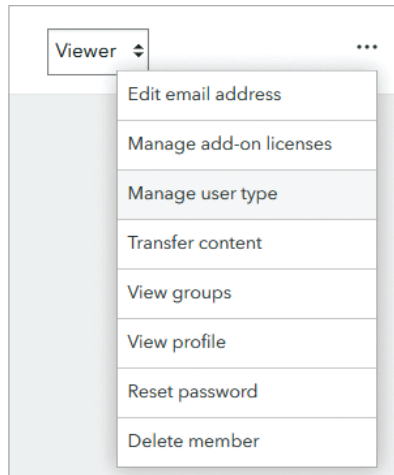
2. Under **Role**, click the **Viewer** role to see that there are limited compatible roles available with the **Viewer** user type you assigned this member.

3. Under **User type**, click the **Viewer** user type to open the drop-down menu. From the list, select **Creator**.

4. Open the **Role** drop-down menu again to see the expanded list of available roles that are compatible with the **Creator** user type.

5. Click **Cancel** to close the window without saving any changes.

6. Click the menu button for the **Test Viewer** member and click **Manage add-on licenses**.

7. Review the list of available add-on licenses, if any.

   Tip: Because this user has the lowest level of user type, most add-on licenses will be unavailable to assign.

8. Click **Cancel** to close the window without saving any changes.