Configure Users and Groups

On this page:

This topic describes how to create local users in the AppDynamics Controller UI. The credentials for this type of user are stored by the Controller. Alternatively, you can configure the Controller to authenticate and authorize users based on externally stored credentials in LDAP or SAML.

Create Local Users

1. As an administrator in the Controller UI, click **Settings** > **Administration**.
2. Click the **Users** tab.
3. Click the **Create New User** button.
4. Enter the information for the fields, including the Username, Name, Email, and so on.
   Because of browser incompatibilities, AppDynamics recommends using only ASCII characters for user names and passwords.
5. Choose at least one role for the new user.
   If you do not choose a role before saving, a warning message appears in the UI. You can assign the user to a role later, but the user will not be able to use any features in the UI until assigned a role.
6. Optionally, choose a group for the user.
7. Click **Save**.

Manage Local Users

After creating a user, you can manage and modify the user account in several ways, including:

- Modify a user's settings by selecting the user and clicking the **Edit** icon.
- Delete a user to disable access for the account to the Controller UI.
- Duplicate a user. An existing user account may serve as a useful starting point for creating additional accounts, especially with roles and groups assignments.
- Assign the user to a group. Groups are a useful mechanism for administering authorization settings for multiple users collectively. From the user list in the Users tab of the Administration page, select the user whom you want to assign to groups, check the member check boxes for the groups, and then save.
- Assign a role to a user. Roles determine permissions in the Controller UI. You can assign or remove roles for a user in the user settings or from the **Roles** tab.

Warning: Do not remove yourself from all groups or from all roles. Also, if the only roles of which you are a member are custom roles, do not delete those custom roles or remove permissions from them. Doing so can result in being locked out of the AppDynamics UI with no permissions at all. If this happens, use the built in administrator role to restore the account.

Create and Manage Groups

If you are are using LDAP to authenticate all AppDynamics Controller users you do not need to create AppDynamics groups. If using local user accounts for Controller access, you can collect users into groups to manage permissions for the users collectively.

You can create a group as an administrator in the Controller UI, from the **Settings** > **Administration** page. Click the **Groups** tab and use the UI to create the group.

Once you have created the group, you can:

- Assign users to the group by selecting the group and selecting the **Member** check boxes for the users to be added to the selected group or groups.
- Assign a role to the group by selecting the group to which you want to assign roles and selecti ng the **Member** check boxes for the roles to be associated with the selected group or groups .
- Delete a group by selecting it in the group list in the left panel and clicking **Delete**.

Require Strong Passwords

As an account administrator, you can require local users (those authenticated by AppDynamics) to use strong passwords.

By default, strong password requirements are not enforced, which means that users can configure passwords of any length or complexity. With the requirement enabled, passwords must meet the complexity requirements listed in the Controller UI, which include having at least eight characters, containing both upper and lower case letters, and more.

To enforce strong password requirements, select the **Require Strong Passwords** check box in the **Authentication Provider** tab of the **Settings** > **Administration** page.

Passwords set by users after you enable this requirement must meet the requirements listed in the UI. Enabling the option does not affect passwords that are already set.