Users: Roles and Permissions

The Security node in ApplinX allows managing users, groups and their permissions. It is possible to define certain permissions for a group, and then associate users with this group, giving the user the permissions defined for this group. For example, a specific application that has a list of users who can develop the application and a list of users who can only view the application will have two groups with relevant permissions, and users will be associated to the relevant group. A change in the group permissions will take affect on all users belonging to this group. Users will inherit the permissions from all the groups to which they have been associated. Specific permissions given to a user, will override group permissions. For example, if a user inherits edit permission for 'CompositeDemo' but also has view permission, he will have view permission only.

Users with Administrator or Supervisor permissions, can access the Security node and manage users and groups.

- Multiple Developers Working on the same Application
- New User Properties
- Defining User Permissions
- Defining Passwords
- Disabling a User's Account
- Adding a New Group

Multiple Developers Working on the same Application

ApplinX applications are typically developed by more than one user. This can sometimes cause conflicts on the ApplinX server. Working methodologically and investing time and effort in planning the development and design of the application can help prevent such conflicts:

- Divide responsibilities between the developers (such as developers working on specific entity types, or workflows).
- Provide each user with a unique user name and determine permissions according to user names.
- Work with folders: Permissions can be given to specific folders or users. These permissions can be defined for specific entities/processes.

Typical conflicting scenarios and outcomes:

- More than one developer editing the Application Properties: ApplinX will save the changes of the first developer who saves the changes.
- More than one developer editing an entity:

  When more than one developer edits the same entity, and one of the developers saves the entity, the other developers receive a message indicating that this entity has been saved by another developer. You are required to determine whether you would like to work on the newly saved entity (and update

your editor to reflect the newly saved entity) or to continue working on the outdated editor.

If you choose to continue working on the outdated editor then when trying to save the entity, you will be informed of the name of the user who made the changes and you will be able to decide whether to either:

- Overwrite the changes that the other developer has made.
- Save the entity with a different name. Note that references that pointed to the original entity will not point to this entity and need to be added manually. References that this entity referred to will be maintained.
- Discard the changes that you made.

New User Properties

The *New User* dialog box is used to define new users, their permissions and passwords. Access this dialog box by selecting **Management>Security>Users** in the ApplinX Explorer and then clicking on the **New** icon in the Toolbar. The *New User* dialog box is displayed. Fill in the **Name**, **Full Name** and **Description** and define associated groups and permissions.

Note:
If you do not associate a group to a user, the user will, by default, be associated with Everyone.

Name

The unique identifier of the user. Can contain only digits, English letters (upper or lower case), underscore and spaces. (Obligatory field)

Full Name

The full name of the user.

Description

A suitable description of the user.

Associated groups

The user belongs to these groups. If you do not associate a user with a group, the user will, by default, be associated with Everyone.

Add

Allows you to add one or more groups to the list of groups associated with the user.

Remove

Allows you to remove a group from the list of associated groups by first selecting the group name and then clicking on the Remove button.

Permissions

Displays a dialog box where the folders the user can view and/or edit are defined. Refer to Defining User Permissions.

Password

User password, required when accessing ApplinX. Refer to Defining Passwords.

Account is disabled

Determines if the account will be disabled.

System Administrator

When checked, provides the user/group with System Administrator permissions.

Defining User Permissions

To view or edit a user's permissions

1. Select Management>Security>Users in the ApplinX Explorer and select the relevant user. The User dialog box is displayed.
2. Click Permissions. The User Permissions dialog box is displayed.
3. To add a permission, click the Add button. The Select Folder dialog box appears. Select from the list of applications or folders in order to define the user's permissions for this application or folder and click OK.

   ApplinX

   Top-level permission for all ApplinX features and operations.

   Management

   Permission for runtime monitoring and managing.

   Applications (previously Composer)

   Development permission for all applications.

   <Application Name>

   Per application permission.

   Note:
   The Administrator's permissions cannot be changed.
4. Check the Edit or View check boxes to change the selected permissions level.
5. To remove a permission, select a permission and click Remove.

Defining Passwords

To change a user's password

1. Select Management>Security>Users node in the ApplinX Explorer.
2. Double-click on the relevant user or define a new user. The User dialog box is displayed.

   Note:
   It is highly recommended to changing the Administrator's password often.
3. In the User dialog box click on the Password button. The User Permissions dialog box is displayed.
4. In the New password field, enter the new password.
5. In the Confirm new password field, enter the new password again and click OK.

Disabling a User's Account

To disable a user's account

1. Select Management>Security>Users node in the ApplinX Explorer.
2. Double-click on the relevant user. The Information dialog box is displayed.
3. Click the Account is disabled check box to disable a user account.

Adding a New Group

To add a new group

1. Select Management>Security>Groups node.
2. Either click the New button on the toolbar or right-click the Groups node and select New. The New Group dialog box appears.
3. Fill in the Name (can contain only digits, English letters (upper or lower case), underscore and spaces) and Description and define the users registered in this group.
4. Click the Add or Remove buttons to add or remove users to or from this group. There are four built in users.

   Administrator

   Built-in account for administering the ApplinX Server.

   sysDeveloper

   Built-in account for configuring and developing the ApplinX Server.

sysOperator

Built-in account for monitoring and managing the ApplinX Server.

sysUser

Built-in account with all administrator rights except managing groups and users.

Note:
System (pre-defined) groups and users cannot be deleted.

There are a number of predefined groups:

Everyone

System group that includes all ApplinX users.

Developers

System group with full access to all the applications on the ApplinX Server.

Supervisors

System group with complete and unrestricted access to the ApplinX Server.

Note:
System (pre-defined) groups and users cannot be deleted.