

Configuring Security for Groups

Appian 7.6

Appian allows you to tailor user rights to the needs of your groups and your overall organization.

Toggle JS

The following factors affect the security for users within a group and users not within a group:

1. [Types of Group Membership](#)
2. [Group Security Settings](#)
3. [Group Membership Policy](#)
4. [Group Privacy Policy](#)
5. [System Groups](#)

Types of Group Membership

Four types of membership determine the user rights available for a group - Administrator, Group Creator, Member and Viewer.

Administrator

Group Administrators have the following rights within a group. They can modify group properties, add administrators and members, edit administrators and members, set-and-modify membership rules, and delete the group.

Group Creator

The Group Creator has administrator rights over the group.

Member

These users have been approved for membership either by the Administrator or automatically by a rule depending on the Group Membership Policy selected. The rights given to members depend on the Group Security Setting selected.

See below: [Group Membership Policy](#) and [Group Security Settings](#)

Viewer

Viewer rights depend on the Group Security Settings selected as described in the next section.

Group Security Settings

Appian defines three security settings - Public, Personal, and Restricted. These settings have implications in group directory lists, group searches, group membership, and group administration.

These settings can be modified from the Group Details page.

See also: [Group Details](#)

Public

Public groups can only be created by the Administrator user or a System Administrator user account. Public groups appear when browsing groups or group search results. All users who want to join a group can view these groups in group search results. Group membership may require approval by Administrator.

When Public groups are added to the Tempo Message Audience Groups system group, all users can select and send messages to those groups.

Personal

All users can create a group with Personal security, but only the Group Creator can work with and modify the group. He/she can add other users as administrators and members, but members cannot see this group.

These groups are useful when organizing contact lists or assigning tasks. This security feature allows the members in your group to be aware of the group's existence, yet they cannot use the group or view other members.

Users, including group administrators, cannot send Tempo messages to a Personal group, even if the group is added to the Tempo Message Audience Groups system group.

Restricted

All users can create a group with Restricted security. This setting exposes the group to its members and administrators only.

Group members and administrators can view the group when browsing. The group appears for these users within group search results.

If a Restricted group is added to the Tempo Message Audience Groups system group, and a member sends an open message to that group, non-members may still see the message, but the Restricted group's name will display as [\[Group Name Not Available\]](#). To avoid confusion for your users, you

may want to limit the number of Restricted groups added to the Tempo Message Audience Groups system group.

- This also applies if the message is sent to multiple Restricted groups and a user is a member of one group, but not all. The user will see the message, but the groups the user is not a part of will be listed as **[Group Name Not Available]**.

See also: [Send a Message](#)

Group Membership Policy

The Group Membership Policy selected for a group determines whether or not users are free to join a group and whether or not approval is required before the user can be added to the group.

The possible policies are discussed below.

Closed

Only Group Administrators can add or remove members to the group. For the **Team** and **Personal** security settings, the membership policy is always **Closed**.

Exclusive

Users can only join the group with approval from a Group Administrator.

To join an Exclusive group, complete the following:

1. When viewing the group, locate the **Join** button on the toolbar.
2. Click the **Join** button to send an alert to the group administrators with an explanation of your request.
3. When viewing the alert, the group administrators can view your explanation, **Approve** or **Deny** the request, and provide a comment that is sent back to you.
4. When the administrator approves or denies the request, an alert is sent to you with his/her decision along with any comments.

Automatic

Users who can see groups with this policy do not need the Group Administrator's permission. This option exists only for groups with the **Public** group security setting.

Group Privacy Policy

This determines whether members can see group members in the group profile. There are two settings for viewing policy:

Low

All members can see each other.

High

The members cannot see each other. Only **Group Administrators** and the **Group Creator** can see all the members. For the **Personal** security setting, viewing policy is always set to **High**.

System Groups

Certain system groups are available to assist you with administering components of the application suite.

The following system groups are available:

- Document Administrators
- Portal Administrators
- Process Model Creators
- Tempo Global Message Authors
- Tempo Message Audience Groups

System groups can be modified by the **Administrator** user account, **System Administrator** users, or the **Group Administrator(s)**, with the following restrictions:

- They cannot be deleted through the user interface.
- Their names cannot be changed from the user interface.
- They have the same UUID on all systems.

Document Administrators

Members of this group can administer the document-management module of the application. These members can perform various administrative functions such as creating, modifying, deactivating, and reactivating departments. They can modify documents, users, and move knowledge centers. Members of this group see an administration link that allows them to perform these tasks.

The **Document Administrators** group has the following security settings:

- Restricted

- The ability to view the group itself is restricted to members and administrators.
- Closed membership policy
 - Group administrators must select members.
- Low privacy
 - Members of the group can view each other.

Portal Administrators

Members of this group can perform certain content administration functions - such as editing the Application Designer home page, administering portal pages, authorizing and approving content, and publishing content.

The **Portal Administrators** group has the following security settings:

- Restricted
 - The ability to view the group itself is restricted to members and administrators.
- Closed membership policy
 - Group administrators must select members.
- Low privacy
 - Members of the group can view each other.

Process Model Creators

Basic Users must be a member of the **Process Model Creators** group in order to create new process models or configure the Query Database or Call Web Service Smart Services.

- You can create a group membership rule that automatically grants all basic users the right to create process models, if you prefer.
- System Administrator users do not need to be members of this group to create process models.

See also: [Adding All Users](#)

The **Process Model Creators** group has the following security settings:

- Restricted
 - The ability to view the group itself is restricted to members and administrators.
- Closed membership policy
 - Group administrators must select members.
- Low privacy
 - Members of the group can view each other.

Users added to the Process Model Creators Group are automatically added to the Designer Role which gives them access to design all aspects of an application.

See also: [User Roles](#)

Tempo Message Audience Groups

This system group is used to define available target groups for Tempo messages.

- This group is used solely for targeting groups of users.
- Individual users are ignored, when present.

See also: [Enabling Target Audiences for Tempo Messages](#).

The Tempo Message Audience Groups system group has the following security settings:

- Personal security
 - It can only be viewed by administrators.
- Closed membership policy
 - Group administrators must select members.
- High privacy
 - Only administrators can view group members.

Tempo Global Message Authors

This system group is used to provision users with the right to post global messages (messages to everyone) in [Tempo](#).

The **Tempo Message Authors** system group has the following security settings.

- Personal security
 - It can only be viewed by administrators.
- Closed membership policy
 - Group administrators must select members.

- High privacy
 - Only administrators can view group members.

See also: [Enabling Target Audiences for Tempo Messages](#).

© [Appian Corporation](#) 2002-2014. All Rights Reserved. • [Privacy Policy](#) • [Disclaimer](#)