

Search documentation

Search

Appian

User Management

Appian 7.7

The People View in the Designer Interface allows you to view, create, and edit both users and groups. To access the People View, select the **People** tab in the Designer Interface.

Toggle Us

This page lists the name, user name, email, and work phone number of all users within the system. The users displayed are sorted by last name in descending order. This can be changed by selecting any of the column headers to sort the list.

In addition to the People View, there is also a User record type in Tempo that holds the user profiles for users of Appian.

The following sections describe how to use the People View as well as the User record type for user management:

- [Creating a New User](#)
- [Viewing User Details](#)
- [Uploading a User Photo](#)
- [Starring Users and Groups](#)
- [Modifying Users](#)
- [Unlocking a User Account](#)
- [Resetting a User Password](#)
- [Managing User Rights and Security](#)
 - [Account Rights for Basic Users](#)
- [Adding Users to Groups](#)
 - [Adding Group Members Individually](#)
 - [Adding Groups to a Group](#)
 - [Adding Group Administrators](#)
 - [Defining a Rule for Adding Users](#)
 - [Defining a Rule for Adding Groups to a Group](#)
- [Configuring Users for Tempo](#)
 - [Adding Groups to Tempo Message Audience Groups](#)
 - [Adding Users to Tempo Global Message Authors](#)
- [Deactivating Users](#)
- [Reactivating Users](#)
- [Configuring Tempo User Profiles](#)

Creating a New User

Only system administrators can create new users.

To create a new user, complete the following:

1. Log-into Appian as a system administrator.
2. Click the **People** tab.
 - The People View is displayed.
3. Click **Create a User Account** in the left navigation.

▼ I want to:

- [Create a Department](#)
- [Create a Team](#)
- [View Group Types](#)
- [Create a Custom Group Type](#)
- [Create a Custom Group](#)
- [Create a User Account](#)

- The Basic Information dialog of the **Create user account** wizard is displayed.
4. Enter the user's **Username**.
 - A username can only contain up to 35 ASCII letters (a-z, A-Z), numbers, and the special characters listed below.
 - At symbols (@)
 - Periods (.)
 - Underscores (_)
 - Hyphens (-)
 - It must not match an existing username regardless of case. For example, if **john.doe** already exists, you cannot enter **JOHN.doe**.
 - If you plan on creating an application that restricts user visibility, be sure to create a username that is not personally identifiable, as usernames are still visible within the system even when a user's Contact Information and Display Name are restricted. See also: [User Profile Visibility](#)
 5. Enter the remaining Basic Information for the user:
 - First Name
 - Middle Name (Optional)
 - Last Name
 - E-mail Address (Must include the @ symbol and a domain such as .com).

6. Select one of the following options from the **User Type** drop-down:
 - **Basic User:** All users that are not system administrators. See below: [Account Rights for Basic Users](#)
 - **System Administrators:** Users that have access privileges to all tools and capabilities in Appian and can edit user roles. This includes the ability to create new administrators.
7. (Optional) Enter a **Password** and re-enter it in the **Confirmation Password** field.
 - If a password is not entered, it is automatically generated and sent to the user in an email.
 - Passwords may be constrained to certain complexity or length requirements by your Appian administrator. See also: [Setting Password Policies](#).
8. Click **Next**.
 - The **Personal Data** dialog is displayed.
9. (Optional) Enter the name of the user's Supervisor in the **Supervisor** field — OR — Click the **Directory** button to select the supervisor from the **Choose a User** dialog box.
 - An auto-complete list of existing users displays as you type. Press the down arrow to highlight the supervisor and press **ENTER** to populate the Supervisor field.
10. (Optional) Select the user's title from the **Title** list.
11. (Optional) Enter the user's address in the location fields.
12. Click **Next**.
13. Review the user's data on the Confirmation dialog box.
14. Click **Submit** to create the user.
 - Scroll down if necessary to reveal the Submit button.

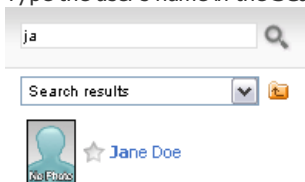
Viewing User Details

When searching for users and groups, the search covers all users in the system, groups that you are a member of, and groups you are permitted to view or join. Other groups do not appear in the result sets.

- Only administrators can view Personal Groups in search result.

To search for and view a user's details, complete the following:

1. Select the **People** tab in the Application Designer.
2. Type the user's name in the **Search** field.



- The search results are displayed in the left navigation.
 - Deactivated users do not appear in search results.
3. Select a user from the search results.
 - The User Details page displays.
4. If you are a System Administrator or a member of the Portal Administrator group, the User Details page allows you to edit a user's profile information, change their password, view groups that the user belongs to, upload a picture, delete a picture, or deactivate the user.
 - View the user's tasks by clicking the **Tasks** tab.
 - View pages created by the user by clicking the **Pages** tab.

To filter users and groups within the system, select one of the options below from the Search Results drop-down. By default, the **Groups I belong to** option is selected.

Select ...	To ...
Starred Groups	All departments that you have marked as a favorite
Starred Users	All users that you have marked as a favorite
All Groups	All groups that you have access to
Groups I belong to	All groups in which you are a member
Search Results	Search for a particular user or group in the system

Alternatively, you can view limited user details using the User record type in Tempo. End users can view the user profiles of other users in Tempo using the User record type. System administrators can prevent users from viewing each other's profiles by configuring User Profile Visibility.

See also: [User Profile Visibility](#)

Uploading a User Photo

System administrators can upload user photos for other users using the following steps. End users can, however, upload their own user photos from

their User record in Tempo.

To upload a user's photo as a system admin, complete the following:

1. Search for and select the user.
2. From the User Details page, click **Upload Picture** on the toolbar.
 - The **Upload Picture** dialog box is displayed.
3. Click the **Browse** button to select a JPG image for uploading.
4. Click **Upload**.
 - If larger, the selected image is cropped to a size of 80 pixels high and 60 pixels wide.

Starring Users and Groups

The star option appears next to users listed in the search results of the People tab.

- To add a user or group to your starred list, click the star that appears next to the name.
- To remove a user or group from your starred list, click the star again.

Once a user or group has been added to your starred list, you can access the user or group by selecting **Starred Users** or **Starred Groups** from the search list. You can also move between any of the options on the display list without losing your search results.

Modifying Users

Only system administrators can modify another user's profile using the following steps. However, end users can modify their own profiles from their User record in Tempo. From their User record, end users can modify their name, email address, office phone, mobile, profile photo, cover photo, and blurb. System administrators cannot modify other users' blurbs. While system administrators can modify users' profiles, they cannot prevent end users from modifying their own profiles.

To modify a user's profile as a system admin, complete the following:

1. Select the **People** tab in the Designer Interface.
2. Search for the user in the left navigation.
3. Click the user name.
 - The user's profile is displayed.
4. Modify the fields in the profile that need to be updated or modified.
5. After completing desired changes, click **Update**.

NOTE: If the account for the selected Supervisor has been deactivated since the last time the user's profile was updated, an error occurs and a valid user or no user must be added to the field.

Unlocking a User Account

Only system administrators can unlock user accounts. When a user account is locked according to a password policy (such as having too many failed login attempts within the designated time frame) the **Unlock User** button is displayed on the user's profile:



To unlock a user, complete the following:

1. Click **Unlock User** to permit additional attempts for the user account.
 - The following message is displayed: **This user account has been locked due to failed login attempts. Are you sure you want to unlock this user account immediately?**
2. Click **OK**.
 - Clicking **OK** immediately breaks the lock and allows the user to login on the next attempt.

Resetting a User Password

Only system administrators can reset a user's password. End users can, however, change their own password at any time from their Profile page in the Portal Interface or from their Settings page in Tempo.

To change a user's password, complete the following:

1. Select the **People** tab in the Designer Interface.
2. Search for the user in the left navigation.
3. Click the user name.
 - The user's profile is displayed.
4. Click **Reset Password**.
 - A new password is emailed to the user.

Managing User Rights and Security

System administrators assign certain rights to a user by making the user a **Basic User** or a **System Administrator**.

- All System Administrator users have administrative rights (the highest level of rights).
- Rights for Basic Users are listed below: [Account Rights for Basic Users](#)

To modify a user's type after creating the user, complete the following:

1. From the **People View**, search for a user.

2. Click the username.
 - The user's profile is displayed.
3. Select the user from the list.
4. Select **Basic User** or **System Administrator** from the **User Type** List.
5. Click **Update**.
 - The user's rights are updated throughout the system.

Other User Rights

All user actions are verified using access control lists prior to execution. Individual objects can be secured by granting rights to individual users, groups, teams, or departments based on group membership and user role maps.

Best Practice: Rather than assign rights for various objects to each individual user, as a best-practice, create a custom group for each role within your organization. Assign rights in the system according to group and then add the users in that role to the associated group.

See also: [System Roles and Security](#), [Configuring Security for Groups](#), and [User Roles](#).

Account Rights for Basic Users

As Basic User accounts interact with Appian, they are frequently assigned additional roles. These roles are granted the necessary rights to perform various tasks, such as administering the objects they create. Basic users must be given the [Designer Role](#) in order to access the designer environment.

Navigation Tabs

Upon login to the designer environment, a Basic User is presented with the following options:

- Home
- Tasks
- People
- Processes
- Rules
- Reports
- Documents
- Feeds
- Applications
- Discussions
- Preferences
- Alerts
- Tempo

Each tab or toolbar option displays a different product view. (The Preferences and Alerts buttons appear on the toolbar.)

The primary tabs can be hidden by the System Administrator from Basic User accounts (and can be targeted to specific groups or users).

Hiding a tab from a user does not necessarily restrict access to the items in a product view, only the direct navigation is disabled. If a user has permission to view an object, an intuitive URL can be used to access it, even when a navigation button is hidden.

Intuitive URLs are available in Appian to replace cryptic URLs with human-readable URLs for various objects. Any user can type an intuitive URL in their browser to access any of the above-listed objects (if they have the authority to view the object and know the object ID).

See also: [Quick Links Using Intuitive URLs](#)

Home View

The Home view of the Application Designer, displays a left navigation that includes two sections: Shortcuts, and I want to... actions.

The following Basic User Home View **Shortcuts** are displayed:

- **My Pages:** Click this link to view a list of links to portal pages that you have created (if any).
- **My Bookmarks:** Click this link to display any pages that you have bookmarked.
- **Favorite Documents:** Click this link to display any documents, folders, or Knowledge Centers that you have bookmarked.
- **My Profile:** Click this link to update your user profile within the system. All user attributes except first name, last name, supervisor and title can be modified here. You can also change your password by clicking Change Password. Browse Content
- **Categories:** Clicking this link displays a report listing all portal pages to which you have access, sorted by content category. New content categories can only be created by a Portal Administrator.
- **My Start Page:** Click this link to access your portal start page. Basic User accounts and System Administrator accounts can change their start page by viewing the desired page and clicking **Options > Make this my start page** on the toolbar.

The following Basic User **I want to** actions are displayed:

- **Design a Process:** Click this button to launch the Process Modeler, which allows you to create a new process model. Creating a process model adds a Basic User to the Process Administrator role for that process model.
- **Create a Page:** This link launches the Portal Page Creation wizard, which allows you to create a page, load page content, select a layout, and change security settings. After creating a Team or Department page, it is possible to make the page Public by selecting Options > Page Sharing on the toolbar. Public pages can be viewed by all user accounts (including anonymous user accounts) from the intuitive URL.
- **Upload a Document:** This link displays an Upload Document wizard, from which you can select a location in the Appian Document Management interface and upload files to that location. As a Basic User you can only upload a document to a Knowledge Center where you have write privileges. By default, Basic User accounts are only given write privileges to **My Private Knowledge Center**. To upload a document to another location, a Document Administrator must explicitly grant author rights to a folder or a Knowledge Center.

Tasks View

Selecting the Tasks button on the toolbar allows you to view all tasks assigned to you.

A Basic User cannot view any tasks that are assigned to other users through this interface. However, a Basic User can be granted Process Administrator rights to a process or process model, which then permits the user to view tasks assigned to other users assigned by that particular process or process model.

Different task views can be generated through the reporting framework built into Appian.

Apart from viewing and submitting a task, users with adequate rights can also reassign a task, add notes and attachments to a task, or add notes and attachments to a process model. The actions that can be performed on a task, apart from task completion, depend on the access a user has to the underlying process instance.

For more information on Process Security, see also: [Configuring Process Security](#).

For more information on how to configure task reassignment, see also: [Assignment Tab](#).

People View

All registered users can be viewed by Basic User and System Administrator accounts unless the User Visibility functionality is configured against this. Basic user accounts are allowed to create Teams, which they can also administer. Upon creation of a Team, you can add or remove other users from the Team. A Basic User cannot create new users or groups for other group types.

See also: [User Visibility](#)

Processes View

The Process Modeler can be launched by Basic User and System Administrator accounts. To access the Process Modeler, click Launch Process Modeler in the left navigation. As a Basic User, you can only save your process models under the **My Models** folder, unless you are granted access to other folder

There are many ways in which a process model can be shared with other users in the system. The ability to make changes to a process model or even start a new process instance however is dependent on the rights granted to each user account. For example, in order to start a new process instance, user must have at least Initiator level access to the process model. The security for a process model folder (apart from the My Models folder), process model, and process instance can be configured by clicking the Security button on the appropriate process model or process instance dashboard. You can also click **File > Security** in the Process Modeler.

See also: [Configuring Process Model Security](#), [Configuring Process Security](#), and [Process Folder Security](#)

Rules View

Basic User accounts and System Administrator accounts are allowed to create rules and constants.

All rules and constants must be stored in a subfolder beneath the Rules and Constants root folder. Basic User accounts are also allowed to create folders within the root folder. Upon creating a folder, Basic User accounts can choose to inherit folder security from the parent folder, or they can assign the users and groups that are allowed to view and edit rules stored in the folder.

Appian does not place any restrictions on the execution of a rule or constant, for Basic User accounts. If a (non-anonymous) user knows the name of a rule or constant in the system but does not have permission to view it, that user is still able to utilize the rule or constant.

The System Administrator can restrict access to the Rules folder so that Basic User accounts have no access by default. Doing so prevents Basic User accounts from viewing rules, creating new rules, or creating new folders within the Rules section.

Reports View

The Reports view allows Basic User and System Administrator accounts to create and view reports that display process or process model data from the system. The data made available in a report is entirely dependent on a user's access level for a process or process model. If a user is granted Manager access to a process or process model he/she is allowed to report on all data from the process/process model. If a user has Initiator access, the data is not visible to the user in a report.

See also: [Configuring Process Model Security](#) and [Configuring Process Security](#)

Documents View

Appian Document Management is divided into Communities, Knowledge Centers, and folders.

All files must be stored within a folder inside a Knowledge Center, inside a Community. Basic User accounts can create a new Knowledge Center by clicking Advanced Interface in the left navigation and clicking the New KC button on the toolbar. Basic User accounts are given the Administrator role for any Knowledge Center they create.

Basic Users have full access to the default Personal and Teams Community. Within this Community you can create a new Knowledge Center, add new files, and control the security of all Knowledge Centers and folders that you create.

Every Basic User has his or her own Personal and Teams Community. One Basic User cannot view files and folders in another Basic User's Personal and Teams community unless the files and folders have been explicitly shared. Apart from files that reside within the Personal and Teams community, Document Administrators can grant Basic User accounts access to Knowledge Centers and folders that reside in other communities. The three different Document Management roles (access levels) are: Administrator, Author, and Read-Only.

When a Knowledge Center is created, it can be assigned Low, Medium, High, or Custom security. With Low Security, all documents default to Read Only access for all users. When a document is in a Low Security Knowledge Center it can be accessed by Basic User accounts, it appears in search results, and it can be viewed by any user account (including an anonymous or guest user account) by typing the document's intuitive URL.

Medium security Knowledge Centers require the explicit assignment of rights to the users and groups that have access to the Knowledge Center. The Knowledge Center is included in user and group searches; and file updates and uploads are posted without approval.

High security Knowledge Centers require the explicit assignment rights to users and groups that have access to the Knowledge Center. It is not included

in user and group searches. All file updates and uploads require approval.

Basic User accounts can delete, rename, view download statistics, change approval options, set file expiration options, change the security settings, add or remove users, and add or remove groups for Knowledge Centers (KCs) that they create. These options are displayed in the Advanced Interface by selecting the parent Community for the KC, then selecting the checkbox next to the KC; which enables the Properties button. Click Properties in the toolbar.

See also: [Document Management Roles and Security](#) and [Knowledge Center Security](#)

Feeds View

Basic users can access and work with the functionality available on the Feeds Tab in the same manner as a system administrator user, except as noted.

- System administrators have administrator rights for all feeds.
- Basic users have administrator rights for the feeds they create.
- Feeds can be viewed by a Basic User.
- A Basic user must be assigned editor or administrator rights in order to edit or administer a feed created by another user.

See also: [Feeds Tab](#)

Applications View

The Applications View allows all accounts with the appropriate rights to complete the following:

- Define exportable applications as collections of Appian objects
- Edit application definitions
- Publish applications to the Application Portal
- Export applications for deployment on other systems
- Import applications to create new Appian objects or update existing Appian objects

User rights must be explicitly defined for applications *and* all of their associated objects. For example, in order to add a page to an application, a user must be an editor of the application as well as a viewer of the page.

See also: [Application User Rights](#) and [Application Deployment Guidelines](#)

System View

Basic users can be given the right to view the System Administration console.

See also: [System Administration Security](#)

Preferences

A Basic User can select your preferred time zone, language, calendar settings by clicking the **Preferences** button on the toolbar. The System Administrator can override your preferred settings through the Administration Console.

Alerts

All portal and email notifications issued by the application can be configured by Basic User and System Administrator accounts. The server administrator can configure email notification settings for the entire site, but each individual user can override these settings for their own account.

A Basic User account can select a component to display its associated alerts (the alert type). Selecting an alert type displays its associated alert rules, which can be edited.

See also: [Notifications](#)

Tempo

The following user rights are available to viewers of the Tempo interface:

Ability	System Administrator	Basic User
View public events (events that are not targeted to any specific user).	Yes	Yes
View events targeted to a group the user belongs to.	Yes	Yes
View posts added by users the user is following.	Yes	Yes
Search for posts added by users the user does not have viewer rights to.	Yes	No
Post to his or her followers.	Yes	Yes
Post a comment on any visible feed entry.	Yes	Yes
Send a message to everyone.	Yes	No
Send a message to a user he or she does not have viewer rights to.	Yes	No
Send a message to a Tempo Message Audience Group the user is a part of.	Yes	Yes
Create a task for a user the user does not have viewer rights to.	Yes	No

View tasks assigned to the user or sent by the user.	Yes	Yes
View tasks assigned to other users.	No	No
Give kudos to other users.	Yes	Yes
View kudos given to other users.	Yes	Yes
View an action without view rights to the associated process model.	Yes	Yes
Take an action that is in a viewable process model and application.	Yes	Yes
Take an action without view rights to the associated process model.	No	No
Open a case without view rights to the associated process model.	No	No
View his or her own profile.	Yes	Yes
View a profile of a user they do not have viewer rights to.	Yes	No

NOTE: System Administrators have viewer rights to all users.

Adding Users to Groups

When viewing the Group Details, you can add group members (both users and groups) individually, add group administrators individually, or define rule that automatically add users that meet certain criteria.

See also: [Group Details](#) and [Configuring Security for Groups](#)

Adding Group Members Individually

To add group members individually, complete the following:

1. Click **Add Users** on the **Members** tab of the group details view.
 - The **Choose Users** combination box is displayed.
2. Browse for users by selecting a group that the user belongs to, or type the username in the autocomplete field — OR — Click the **Search** tab of the **Choose Users** dialog box to search for a user by username, first name, or last name.

When saved, these changes are automatically reflected to logged-in users.

Adding Groups to a Group

To add groups to a group, complete the following:

1. Click **Add Groups** on the **Members** tab of the group details view.
 - The **Choose Groups** combination box is displayed.
2. Browse for groups, or type the group's name in the autocomplete field — OR — Click the **Search** tab of the **Choose Groups** dialog box to search for a group by name.

When saved, these changes are reflected to users when they log back into the system.

Adding Group Administrators

To add users as a group administrator to a group, complete the following:

1. Assign users administrative rights for the group by clicking **Add Users** on the **Administrators** tab of the group details view — OR — Click **Add Groups** to select a desired group of users.
 - The **Choose Users** combination box is displayed.

When saved, these changes are automatically reflected to logged-in users.

Defining a Rule for Adding Users

You can create rules for adding users and adding groups.

To define a rule that adds individual users, complete the following:

1. From the Group Details view, click the **Rules** tab.
 - The **Edit group membership rules** page is displayed.
2. Click add **users**.
 - Two lists and a text field appear for you to define the rule parameters.
 - The first list displays the following properties from the user's profile:
 - Username
 - First name

- Middle name
 - Last name
 - Preferred name
 - E-mail
 - Office phone
 - Mobile phone
 - Home phone
 - Address 1
 - Address 2
 - Address 3
 - City
 - State
 - Province
 - Zipcode
 - Country
 - User Type
 - Title
 - Supervisor Name
 - Field01 - Field10
3. In the first field, select the user's profile property you want to match in your rule.
 4. In the second field, select one of the following comparison operators:
 - equals
 - does not equal
 - contains
 - starts with
 - ends with
 5. In the third field, type the value you want to use for your comparison.
 6. To add another condition to the rule, click **more**.
 7. Click **done** to list the rule on this page.
 - When listed, the rule displays options to **edit** the rule, **delete** the rule, create a new rule to add **users**, or create a new rule to add **group**.
 8. Click **Apply**.
 - Users are automatically added to your group according to the rule parameters you've defined.

When saved, these changes are reflected to users when they log back into the system.

Rules are case-sensitive and take priority over members added explicitly.

The same attribute cannot be used more than once in a rule. For example, `username like a* AND username like *b`.

Dates must be entered in the format `M/d/yyyy`.

Adding All Users

If you want to add all users in the system to a group, use the following rule:

Username equals *

When saved, these changes are reflected to users when they log back into the system.

Defining a Rule for Adding Groups to a Group

1. From the Group Details view, click the **Rules** tab.
 - The **Edit group membership rules** page is displayed.
2. Click add **groups**.
 - The choose a type list appears.
3. Select **Custom**, **Departments**, or **Teams** from the **choose a type** list.
 - Two lists and a text field appear for you to define the rule parameters.
4. Select one of the following group properties from the first list:
 - Name
 - Group Type Name
 - Parent Group's Name
 - Group Security Type
 - Group Creator's Username
5. In the second field, select one of the following comparison operators:
 - equals
 - does not equal
 - contains
 - starts with
 - ends with
6. In the third field, type the value you want to use for your comparison.
7. To add another condition to the rule, click **more**.
8. Click **done** to list the rule on this page.
 - When listed, the rule displays options to **edit** the rule, **delete** the rule, create a new rule to add **users**, or create a new rule to add **group**.
9. Click **Apply**.

- Users are automatically added to your group according to the rule parameters you've defined.

See also: [Comparison Operators](#)

When saved, these changes are reflected to users when they log back into the system.

Configuring Users for Tempo

All users can add posts to the News feed. All users can also send messages targeted to specific users if they have viewer rights to them.

The list of groups available for a user to send a message to, however, is configured using the Tempo Message Audience Groups and the Tempo Global Message Authors system groups.

- **Tempo Message Audience Groups:** Determines which groups users can target for messages. Groups added to this system group will display options when a user is creating a message if that user has rights to view that group.
- **Tempo Global Message Authors:** Determines which users can target messages to Everyone. Users added to this system group can select the Everyone group when creating messages.

NOTE: Any users or groups added to these system groups also gain the same functionality within Appian for Mobile Devices applications.

Adding Groups to Tempo Message Audience Groups

NOTE: Before adding a new group to receive Tempo messages, consider whether existing groups can be used instead.

See also: [Tempo Best Practices](#)

Initially, only a System Administrator can access the Tempo Message Audience Groups, add/remove groups to it, and add group administrators for it.

Only Public and Restricted groups can be added to the Tempo Message Audience Groups system group. Each group added becomes available for its members to select and send messages to it on the News Feed. Whether or not non-members can select the enabled groups or see messages sent to these groups depends on the security settings for the group and message.

- **Public Groups:** If the group is Public, all users can see and send messages to the group.
 - If the message is **open**, all users can search for and see it in their News feed.
 - If the message is **locked**, only members of the group and the message author can search for and see it in their News feed.
- **Restricted Groups:** If the group is Restricted, only members and administrators are able to see and send messages to the group.
 - If the message is **open**, all users can search for and see it in their News feed, but the group name displays as [Group Name Not Available] for non-members.
 - If the message is **locked**, only members of the group and the message author can search for and see it in their News feed and the group name displays correctly.

To avoid confusion for your users that may see [Group Name Not Available], you may want to limit the number of Restricted groups added to Tempo Message Audience Groups.

See also: [Send a Message](#)

To add a group to the Tempo Message Audience Groups, complete the following:

1. In the Designer, select the **People** tab.
2. Type **Tempo Message Audience Groups** in the Search field — or — from the list in the left navigation, select **All Groups**, expand the **Custom** folder, and select **Tempo Message Audience Groups**.
3. From the toolbar, select **Add Groups**.
 - The Choose Groups dialog box is displayed.
4. Select a group (or multiple groups in a semi-colon separated list) that you want to enable for message targeting.
5. Click **OK**.

The selected group(s) are listed as members of Tempo Message Audience Groups.

When saved, these changes are reflected to users when they log back into the system.

NOTE: Only groups are recognized in this system group. If you add any individual users as members of this group, they are ignored.

Adding Users to Tempo Global Message Authors

Adding a user or group to the Tempo Global Message Authors system group gives those users the option to select the Everyone group as the target audience when sending messages on the News feed.

- The Everyone group contains all active users in the system.

Initially, only a System Administrator can access the Tempo Global Message Authors system group to add or remove groups to it and add other users and administrators.

To add users and groups to the Tempo Global Message Authors Group, complete the following:

1. In the Designer Interface, select the **People** tab.
2. Type **Tempo Message Audience Groups** in the Search field — OR — from the list in the left navigation, select **All Groups**, expand the **Custom** folder, and select **Tempo Global Message Authors**.
3. To add groups, select **Add Groups** on the toolbar.
 - The Choose Groups dialog box is displayed.
4. Select a group (or multiple groups in a semi-colon separated list) that you want to grant the right to target messages to all users and click **OK**.
 - The selected group(s) are listed as members of Tempo Global Message Authors parent group.

5. To add users, select **Add Users** on the toolbar.
 - The Choose Users dialog box is displayed.
6. Select a user (or multiple users in a semi-colon separated list) that you want to grant the right to target messages to all users and click **OK**.
 - The selected user(s) are listed as members of Tempo Global Message Authors parent group.

When saved, these changes are automatically reflected to logged-in users.

Deactivating Users

Deactivating a user means the user account is still present in the system memory, but is not able to log in.

Only system administrators can deactivate users.

To deactivate a user, complete the following:

1. Click the **People** tab on the Designer Interface.
2. In the left navigation, search for a user.
3. Click the user name of the user you want to deactivate.
4. Click the **Deactivate User** button on the toolbar.
 - You are prompted to verify that you do want to deactivate the user in question. Click **OK**.

NOTE: The **Administrator** user account cannot be deactivated.

Reactivating Users

When a user account is reactivated, its **last login time** is set to the current date and time to prevent the user from being immediately deactivated (if a policy is in place to do so for users who do not log into the system within a certain amount of time). See also: [Setting Password Policies](#)

Only system administrators can reactivate users.

To reactivate a user, complete the following:

1. Click the **People** tab on the Designer Interface.
2. On the left navigation, search for a user.
3. In the **User Search Results** pane, click **View De-activated Users**.
4. Select the checkbox next to the user(s) you wish to reactivate.
5. Click **Reactivate** button.

The user is now reactivated and is able to log in to the system. Expired passwords must be reset when attempting to log in.

Configuring Tempo User Profiles

A directory of Appian users is available as a record type in the Tempo interface. This directory is accessible by end users by navigating to the "Users" record type in Tempo and browsing or searching the record list.

Each user in Appian has a User record, which by default has a Summary view and News and Related Actions views, just like designer-configured records. The sections below describe the aspects of this record type that you can modify and/or extend to best meet the specific needs of your organization.

1. [Edit User Record Type](#)
2. [Modify Name and Description](#)
3. [Modify Security](#)
4. [Modify List View](#)
5. [Add User Filters](#)
6. [Add Related Actions](#)
7. [Add Record Views](#)
8. [UserProfile Record Fields](#)
9. [Deploy Changes](#)

The content below assumes a basic familiarity with record design and focuses more on the specifics of configuring the User record type. Consider familiarizing yourself with the Record Design and Records Tutorial pages before proceeding.



See also: [Record Design](#) and [Records Tutorial](#)

Edit User Record Type

Since user profiles are records, you can configure the format of user profiles by configuring the corresponding User record type. Take the following steps to do so:

1. In the Designer environment, navigate to the System tab and from the left navigation select **System Administrator Home > Data Management > Data Management**.
2. Select the **Record Types** tab.
3. Find the record type named **User** and click on the name.

You will see the following screen, from which you can edit the record type:



Save

Properties

Singular Record Type Name

The name that end users see in record tags

Description

A description that end users see in the list of record types

Plural Record Type Name

The name that end users see in the list of record types

URL

Data

Source

Data Type

The fields of the selected data type are record fields available under the rfi expression context. You can use these fields to configure the filters, record list, views, and related actions for the record type.

Record List

List View

Sort Field

☒ Ascending
☐ Descending

Enter an expression to define how each item in the record list view appears. Because this expression is repeated for every item, unless it can be evaluated quickly the overall list view may have poor performance. Use a listViewItem()

Views

Configure views to display information about a record

View Name	Interface	Visibility	Related Action Shortcuts
No items available			

[+ New View](#)

Related Actions

Related actions allow end users to take action in the context of a record

Process Model	Context	Visibility
No items available		

[+ New Related Action](#)

Security

Viewers
☒ All Users - Any authenticated user can view this record type
☐ Restricted - Members of the selected groups can view this record type
Users must have Viewer or higher privileges on the record type source in order to view the record type in the end user interface

Auditors

Auditors can view the record type in the end user interface and its configuration in the design interface, but they cannot change anything

Editors

Editors can see everything Auditors can as well as update the record type's configuration, except for the security configuration

Administrators

Administrators can view and modify all configurations of a record type

See also: [Editing Record Types](#)

Modify Name and Description

You may need to modify the name and description of the User record type, especially if you need to translate it to a different language to fit the locale of your users. The **Singular Record Type Name**, **Plural Record Type Name**, and **Description** fields of the User record type are all editable. If your user base speaks multiple languages, populate the fields accordingly with all relevant languages. For example:

- **Singular Record Type Name:** User / Usuario
- **Plural Record Type Name:** Users / Usuarios
- **Description:** Directory of users / Directorio de usuarios

Modify Security

The **Viewers** field of the User record type is set to "All Users", which means that all users who can access Tempo can see the Users record type from the Records tab. This cannot be changed. However, you can configure the following fields that are relevant to security:

- Auditors
- Editors

- Administrators

See also: [Record Type Security](#) and [Security](#)

Modify List View

The record list view for the Users record type is set to use the system function `a!userRecordListViewItem` by default. This default list view displays the first and last names, email, office phone, and mobile phone for each user in the Users record list.



John Doe
john.doe@example.com
888.123.4567 (Office)
555.321.6789 (Mobile)

You can replace the system function with your own rule that defines a different list view for the User record type. For example, you could create a rule with the following expression to display each user's city and state instead of email and phone numbers:

```
a!listViewItem(  
  title: rf!firstName & " " & rf!lastName,  
  details: rf!city & ", " & rf!state,  
  image: touser(rf!username)  
)
```

In this expression, we used record fields available in the `UserProfile` CDT (the source data type for the User record type) by using the `rf!` domain to access them. See the [UserProfile Record Fields](#) section below for the full list of record fields available in the `UserProfile` CDT. The above expression result in a different looking list view:

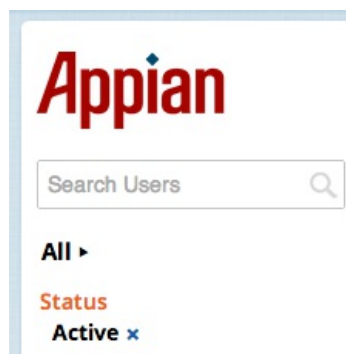


John Doe
Reston, VA

See also: `a!userRecordListViewItem()`, [Record List View](#), and [Configure the Record List View](#)

Add User Filters

The **User Filters** field of the User record type is set to use the system function `a!userRecordFacets` by default. This default function contains a "Status" user filter with filter options "Active" and "Inactive", with "Active" selected by default. As a result, users see only active users in the Users record list by default. Inactive users are users whose accounts have been deactivated.



Removal of the default "Status" user filter is not recommended. Doing so will result in the Users record list displaying all inactive users, with no way for users to filter out the inactive users. However, you can add your own user filters in addition to the default "Status" user filter. For example, if your users span multiple countries, you could add a "Country" user filter.

To do so, create an expression rule called `userRecordUserFiltersExtension`. Define the rule with the following:

```
a!facet(  
  name: "Country",  
  options: {  
    a!facetOption(  
      id: 3,  
      name: "China",  
      filter: a!queryFilter(  
        field: "country",  
        operator: "=",  
        value: "China"  
      )  
    ),  
    a!facetOption(  
      id: 4,  
      name: "France",
```

```

    filter: a!queryFilter(
      field: "country",
      operator: "=",
      value: "France"
    )
  ),
  a!facetOption(
    id: 5,
    name: "United States",
    filter: a!queryFilter(
      field: "country",
      operator: "=",
      value: "USA"
    )
  )
}
)

```

Notice that the IDs used for the filter options in the above expression start with 3. That is because IDs 1 and 2 are already being used for the filter options for the "Status" user filter. Filter option IDs cannot be reused across multiple user filters for the same record type.

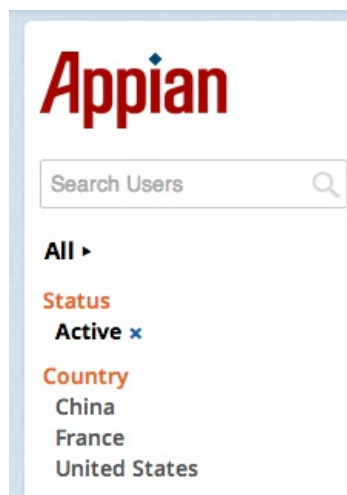
Now edit the User record type to modify the **User Filters** field to include your expression rule:

```

{
  a!userRecordFacets(),
  rule!userRecordUserFiltersExtension()
}

```

After saving the record type, you will see your new "Country" user filter in the left-hand navigation when viewing the record list.



See also: [a!userRecordFacets\(\)](#), [User Filters](#), and [Add User Filters](#)

Add Related Actions

The User record type does not have any related actions defined by default, but you can add related actions to this record type just as you would any other record type. Additionally, you can configure related action shortcuts from any record view for the User record type.

You have access to the record fields in the **rf!** domain to define the **Context Expression** fields for related actions.

See also: [Related Actions](#) and [Add Related Actions](#)

Add Record Views

The Summary record view for the User record type is defined by default. While the Summary view is not editable, you can define additional record view to display more user information on user profiles.

Adding record to the User record type is the same as adding record views to any other record type. You have access to the record fields in the **rf!** domain to define the record view interfaces.

See also: [Record Views](#) and [Add Record Views](#)

UserProfile Record Fields

If you edit the User record type in the Designer interface, you will notice that the **Source Data Type** for the record type is **UserProfile**. All the fields of the UserProfile CDT are available to you as record fields in the **rf!** domain. The fields of UserProfile are as follows:

- *active* (Boolean): Indicates whether the user is active or not.
- *username* (Text): The unique username with which the user logs into Appian.
- *firstName* (Text): The user's first name.

- *middleName* (Text): The user's middle name.
- *lastName* (Text): The user's last name.
- *displayName* (Text): The user's nickname.
- *email* (Text): The user's email address.
- *address1* (Text): The first line of the user's address.
- *address2* (Text): The second line of the user's address.
- *address3* (Text): The third line of the user's address.
- *city* (Text): The city of the user's location.
- *state* (Text): The state of the user's location.
- *zipCode* (Text): The zip code of the user's location.
- *province* (Text): The province of the user's location.
- *country* (Text): The country of the user's location.
- *phoneHome* (Text): The user's home phone number.
- *phoneMobile* (Text): The user's mobile phone number.
- *phoneOffice* (Text): The user's office phone number.
- *supervisor* (User): The user's supervisor.
- *blurb* (Text): The user's blurb as provided on his/her profile Summary view.

See the previous sections for examples of how to make use of these field values for the User record type.

Deploy Changes

Once you have made changes to the User record type in one environment, you may need to deploy those changes to other environments. For example, you might make changes in a development environment that you need to deploy in a test or production environment.

The steps for deploying changes to the User record type are the same as those for deploying changes to any other record type. Simply create an application containing the User record type and any dependencies, export the application, and import it to the new environment.

See also: [Application Management](#)

See Also:

- [Process-Driven User Management](#)
- [Group Management](#)

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