User Authorization

XperienCentral has a flexible component for maintaining backend users (casual users, editors, developers, and application managers) and their privileges. The authorizations are assigned at the role level (type of responsibility). The roles determine which websites (or parts thereof) a user may maintain, which functionalities may be used, and which content elements the user may work with. To access the Authorization panel, navigate to **Configuration > Authorization**.

User authentication can also be accomplished by developing a plugin that implements the XperienCentral Credentials Service Provider. This Java class makes it possible to use a credentials provider that is external to XperienCentral. Click here for more information.

Beginning in XperienCentral 10.18, some parts of user management have been changed from previous XperienCentral versions. Expand the section below that corresponds with your version of XperienCentral.

In This Topic

Components

The authorizations within XperienCentral are divided into two types:

- **Users of the Workspace** — XperienCentral backend users such as editors, application managers, and developers, and their privileges to configure settings and define pages. These users belong to one or more roles.
- **Registered website visitors** — You can control which content visitors to an XperienCentral website (frontend) have permission to view. In XperienCentral, these visitors referred to as web users. Web users belong to web groups. Permissions for web users are enforced at the web group level. For complete information on web users, see User Profiles.

In the Workspace environment, authorization management has been further divided into the following components:

- **Authorization - Users** — This component manages users of the Workspace and their privileges. The authorizations are assigned at the role level and determine which operations a user may perform in the various parts of XperienCentral. XperienCentral comes with a standard set of users, roles and permissions.
- **Authorization - Roles & Permissions** — This component enables administrators to modify the basic set of users, roles and permissions. The administrator can create and maintain users, create and maintain roles and assign permissions to roles.

Another related functionality is Workflow. Workflows control the allowed transition from one state to another for content items before they are allowed to be published on the web. The website administrator defines these states and configures their behavior. The states are then linked to user roles, which gives actual shape to the workflow. This XperienCentral functionality is based on the standards defined by the Workflow Management Coalition (WfMC).

Back to top

Role Based Access Control (RBAC)

Many RBAC models exist, but XperienCentral uses the Core RBAC and Hierarchical RBAC models. These models conform to the standard RBAC specification developed by ANSI/INCITS.

Roles and permissions

Role Based Access Control (RBAC) avoids the need to assign permissions to each user individually. Instead, permissions are assigned to roles. A role is a functional or organizational job description in which users sharing the same role share the same tasks. These roles then are assigned to users. The permissions of a role determine which operations a user may perform. RBAC is considerably less labor intensive than assigning permissions to each user individually. A user may have more than one role. An example of a permission is "Edit pages", which grants the permission to modify a page.

In the example above:

- User "John" has the role "Casual user" and therefore has permission to edit pages and maintain forms.
- User "Paula" has role "Editor", therefore she has further the permission to delete pages and maintain form models. Permission assignments may overlap one another, which is the case here for maintaining forms.

XperienCentral comes with a default set of roles and permissions.

Permission groups

Nevertheless, defining proper permissions for each role may be a quite laborious operation. For this reason *permission groups* are introduced. A permission group is a default set of permissions which can be assigned to a role at once. A permission group assigned to a role will implicitly assign all permissions contained by that permission group to that role.

In the example above, role A has permissions b, c, e, f, g and i for the following reasons:

- Permission b and c through permission group A.
- Permission e, f and g through permission group B.
- Permission i through direct assignment.

XperienCentral comes with a standard set of permission groups, see Default Authorizations for more information.

Permission inheritance

Permissions can be assigned in two ways: directly and by means of permission groups. To make things even more flexible, a third way has been introduced: **permission inheritance**.

With permission inheritance, a role has assigned another role to it from which it inherits all permissions which means a child role gets all permissions from its parent role, irrespective of how these permissions have been assigned to the parent role.

In the example above, role B inherits all permissions from role A. So, referring to the example above, role B has the following permissions:

- Permissions b, c, e, f, g and i through inheritance.
- Permission d through direct assignment.

XperienCentral comes with a standard set of roles that inherit from each other, see Default Authorizations for more information.

Back to top

Default Authorizations

XperienCentral comes standard with the users, roles and permission groups listed below.

User	Role	Inherits from role	Permission group
	Casual user	Casual user	Casual user permissions
	Editor	Casual user	Editor permissions
	Main editor	Editor	Main editor permissions
Administrator	Application manager	Main editor	Application manager permissions
Developer	Developer	Application manager	Developer permissions

Developers are treated differently than all other users. Unlike all other users, developers are able to:

- View other users with developer permissions.
- Assign the permission group "Developer permissions" to roles.
- Assign the role "Developer" to users.
- Directly assign to roles the permissions of the category "Developer tools".

Basic set of permission groups by category

XperienCentral comes with five standard permission groups. In the "Roles" tab of the Authorization anel you can see which permissions each role has or can be assigned.

Back to top

Maintaining Roles

Selecting and Viewing a Role

To select and view a role:

1. Navigate to **Configuration > Authorization** and then click the [Roles] tab.
2. Select the desired role from the drop-down list next to "Select a role".
3. Click the [Details] tab to view the details for the role.
4. Click the [Permissions] tab to view the permissions for the role.

Creating a Role

To create a role:

1. Navigate to **Configuration > Authorization** and then click the [Roles] tab and then the [Details] tab.
2. Click [Create new role] in the "Role Selection" section.
3. Enter a name for the new role in the "Role name" text field and then click [Apply].
4. Define the other properties for the role.

Making a Role Available on all channels

To make a role available to all channels in a XperienCentral installation:

1. Select the desired role on the [Roles] - [Details] tab.
2. Select "Available on all Channels".
3. Click [Apply].

Assigning a User to a Role

A role may have one or more users and a user may have one or more roles. You can assign users and roles to one another in two ways:

- From the user point of view, see Assigning a Role to a User.
- From the role point of view.

To assign a user to a role:

1. Select the desired role from the [Roles] - [Details] tab.
2. Select the desired user from the "Add user" drop-down list. The user is added to the list.

Removing a User from a Role

You can also separate users and roles from one another in two ways:

- From the user point of view, see Removing a Role from a User.
- From the role point of view.

To remove a user from a role:

- Select the desired role from the [Roles] - [Details] tab.
- In the list "Users assigned to this role", select the "Delete" checkbox next to the user to be removed.
- Click [Apply]. The user is removed from the list.

Assigning Permissions to a Role

The actual permissions a role gets is determined by the following:

- The permissions it inherits from another selected role.

- The permissions it gets from the assigned permission groups.
- The permissions that have been added directly to the role.

Inherited permissions and group permissions may overlap one another.

To assign permissions to a role:

1. Select the desired role from the [Roles] - [Details] tab.
2. To select the role to inherit from: select a role from the "Inherits all permissions from" drop-down list.
3. To add a permission group, select a permission from the "Add permission group" drop-down list. The permission group is added on top of the drop-down box.
4. To assign a permission directly: select the [Permissions] tab and select the desired permission(s).
5. Click [Apply].

Removing Permissions from a Role

To remove permissions from a role:

1. Select the desired role from the [Roles] - [Details] tab.
2. To remove all inherited permissions, : select "Select a role" from the "Inherits all permissions from" drop-down list.
3. To remove a permission group: in the list "Permission groups" section, select the "Delete" checkbox next to the permission group you want to remove. A pop-up message prompts you to copy the group permissions to the role directly. When you click [OK] the selected permission group is unassigned from the current role and all permissions from the unassigned group are assigned directly to the current role. If you click [Cancel] the permission group is unassigned from the current role and the role loses all permissions from the unassigned group.
4. To remove directly-added permissions: select the [Permissions] tab and clear the permissions to be removed.
5. Click [Apply].

Deleting a Role

To delete a role:

1. Select the role to be deleted from the [Roles] - [Details] tab.
2. Click [Delete role]. The role is removed from the "Select a role" drop-down list.

Finding a User and Viewing their Permission(s)

To find and view a user:

1. Navigate to **Configuration > Authorization** and click the [Users] tab.
2. To show a list of users:
    - Select "All users" to see the full list.
    - Select "Active" to show only active users.
    - Select "Inactive" to show only inactive users.
    - Select a letter range to show users beginning with a specific letter.
    - Click on the arrow in the "Login" column to toggle between alphabetical sorting in ascending (A-Z) and descending (Z-A) order.
3. To view the details for a user: click on the desired user in the list. The user details appear below the user.

Back to top

Maintaining Users

Creating a User

To create an new user:

1. Navigate to **Configuration > Authorization** and click the [Users] tab.
2. Click [Create new user]. A user called "New user" is added to the list.
3. Enter the login name of the new user in the "Login" field. This is the name that will appear in the upper right corner of the Workspace for the user.
4. Enter the password for the new user. For security reasons, it is highly recommended that you create a strong password. A strong password has all of the following characteristics:
    - Is at least 8 characters long.
    - Is significantly different than the previous passwords used by this user.
    - Contains a mix of uppercase and lowercase letters.
    - No string of letters spells out a word that appears in the dictionary of the language of the user.
    - Contains one or more numbers, but the numbers do not represent anything associated with the user such as their birthdate, age, house address, and so forth.
    - Contains one or more special characters. A special character is anything that is not a letter or a number or a space.

- Does not contain any string of letters that spell the user's first or last name, their company name, their job description, their nickname, or any other word that could be associated with them personally.

When you type the new password into the field, the "Password Strength" field indicates the strength of their password using different colors. The following colors are used to indicate the password's strength:

- **Red** — The password is extremely weak (not accepted).
- **Yellow** — The password is moderately weak (not accepted).
- **Blue** — The password is good.
- **Green** — The password is strong.

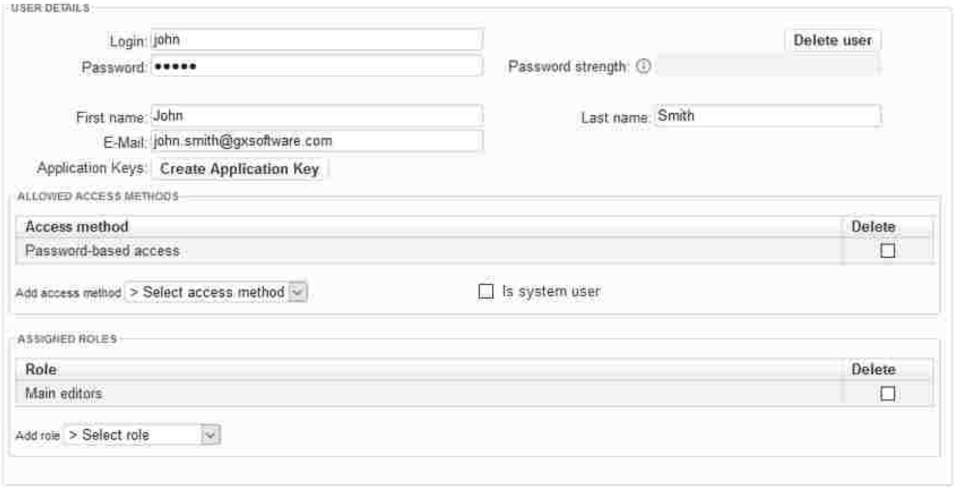
> For security reasons, if you create/modify a user's password, the first time that they log in to XperienCentral after the modification, they must change their password. The only exception to this rule is when you change your own password.

5. Enter the new user's first name in the "First Name" field.
6. Enter the new user's last name in the "Last Name" field.
7. Enter the new user's e-mail address in the "E-Mail Address" field, **Note:** This field is extremely important if you use two factor authentication.
8. Select the method(s) that the user is allowed to use to log in to XperienCentral. The options are:

   Password-based access — The user may log in from the XperienCentral login screen.
   Application key-based access — The user may log in via the XperienCentral REST API. This is mainly used for external applications that want to access XperienCentral content. The application key is associated with a single user and it determines what permissions the external application has. When an application key is generated for the current user, this option wil be automatically added to the list of access options.
   Container-based access — The user many log in from a backend container-based application.
   System user — The user is a system user. See "System User Role" below.

   > This option is only available if the option `enable_backend_container_filter` in the "website_settings" section of the General tab of the XperienCentral Setup Tool is selected.

9. Select one or more roles for the user. For example:



USER DETAILS

Login: john Delete user
Password: ••••• Password strength: ⓘ

First name: John Last name: Smith
E-Mail: john.smith@gxsoftware.com
Application Keys: Create Application Key

ALLOWED ACCESS METHODS

Access method	Delete
Password-based access	□

Add access method > Select access method □ Is system user

ASSIGNED ROLES

Role	Delete
Main editors	□

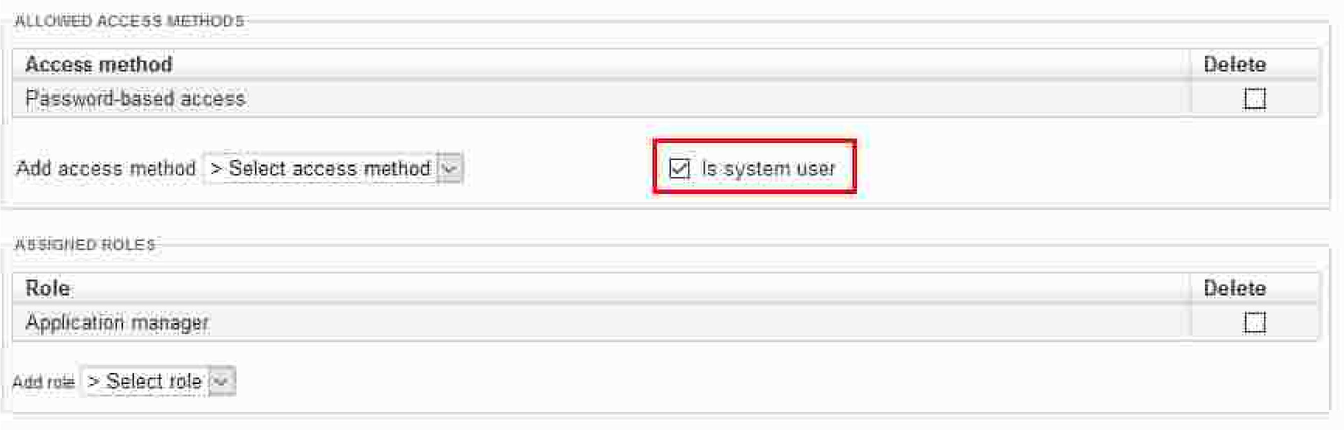
Add role > Select role

10. Click [Apply].

System Users

The ability to define system users was introduced in XperienCentral R28.

In XperienCentral, a special designation of system user is required for automating the content item Import/Export functionality. Import/Export automation executes import/export jobs on a scheduled basis and requires access to XperienCentral at the system user level. To designate a user a system user, select "Is system user":



ALLOWED ACCESS METHODS

Access method	Delete
Password-based access	□

Add access method > Select access method ☑ Is system user

ASSIGNED ROLES

Role	Delete
Application manager	□

Add role > Select role

All users designated a system user can be selected from the user drop-down lists in the Import/Export configuration. The rest of the configuration for the system user is the same as for a normal user. In general, a system user account is not meant to be used for purposes other than executing the import /export jobs. GX recommends that you give system users the role of Application Manager and that you use an application key if possible. See Import /Export Configuration.

Modifying a User

To modify a user's details, follow the steps below. You cannot modify a user's details when they are in an inactive state.

1. Select the desired user by navigating to **Configuration > Authorization** and then click the [Users] tab.
2. Modify the user's details.
3. Click [Apply].

For security reasons, if you modify a user's password, the first time that they log in to XperienCentral after the modification, they must change their password. The only exception to this rule is when you change your own password in the Authorization Management panel.

Assigning a Role to a User

In order to have access to XperienCentral, every user must have at least one role. You can assign users and roles to one another in two ways:

- From the role point of view, see Assigning a User to a Role.
- From the user point of view.

To assign a role to a user:

1. Select the desired user by navigating to **Configuration > Authorization** and then click the [Users] tab.
2. Select the desired role from the "Add role" drop-down list. The role is added to the list.

Removing a Role from a User

You can separate roles and users from one another in two ways:

- From the role point of view, see Removing a User from a Role.
- From the user point of view.

To remove a role from a user:

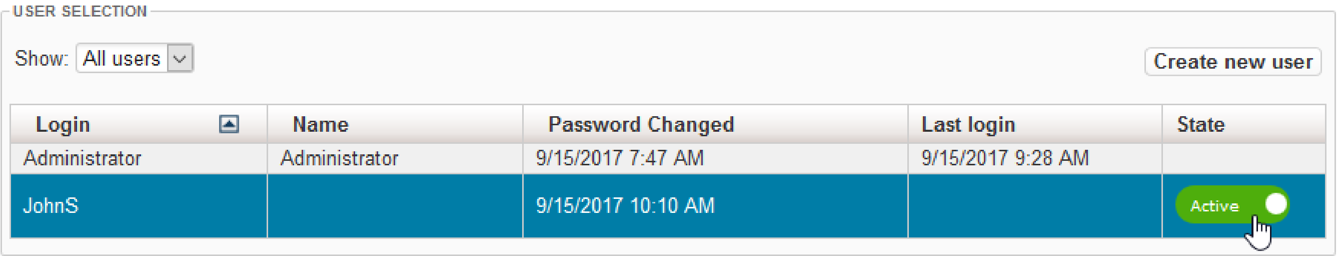
1. Display the desired user by navigating to **Configuration > Authorization** and then clicking the [Users] tab.
2. In the "Assigned roles" list, select the "Delete" checkbox of the role that is to be removed.
3. Click [Apply]. The role is removed from the list.

Deleting a User

Beginning in XperienCentral version 10.18, users can no longer be deleted from XperienCentral but only made inactive.

Changing the State of a User

Users in XperienCentral have a state which is either "active" or "inactive". Active users are able to log in and work in XperienCentral. Inactive users are not allowed to log in to XperienCentral. When an inactive user tries to log in, they will receive an error message which states that their username and/or password are invalid. To change the state of a user, click the "Active" or "Inactive" button in the "State" column next to the user's name. For example:



Login	Name	Password Changed	Last login	State
Administrator	Administrator	9/15/2017 7:47 AM	9/15/2017 9:28 AM	
JohnS		9/15/2017 10:10 AM		Active

The state will change to the opposite of what it currently is. When you change a user from the inactive state to the active state, they will once again be allowed to log in to XperienCentral. The last password that they used is their valid password.

- You cannot set your own state to inactive. This ensures that there is always at least one active user.
- When a user is made inactive, their application key is deleted if one has been generated for them.
- When a user is switched from inactive to active, they must change their password the first time they log in.

Importing Users from Other Websites

To allow users of another website (channel) to access to the current website, their user data can be imported. Imported users maintain the same user name and password. Different websites, however, can have different permissions assigned to their roles.

To import users:

1. Navigate to **Configuration > Authorization** and then click the [Import] tab.
2. Select the website to import users from
3. Check the users to be imported to your current site and click [Apply].

Back to top

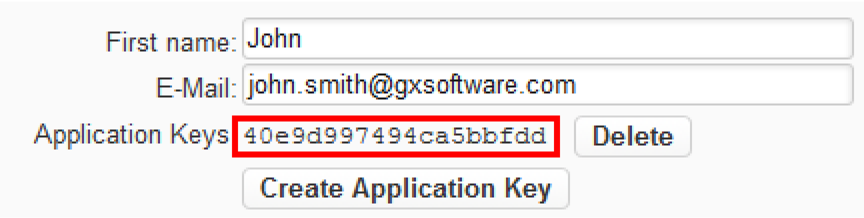
Generating an Application Key for a User

An external application can log in to XperienCentral via the REST API. This makes it possible for external applications to access XperienCentral content. In order to be able to do so, you have to generate an application key for a user.

An application key is tied to a user, which means that the application key used by an external application inherits the role and permissions from the user for whom the application key is generated. For this reason, be sure that you generate an application key with sufficient permission(s) in order for the external application to be able to perform the task(s) for which it is designed. When performing REST calls, the application key should be placed in the custom `X-GX-AppKey HTTP` header.

To generate an application key for a user, follow these steps:

1. Select the user for whom you want to generate an application key from the list.
2. Click [Create Application Key] next to the "Application Keys" field. The application key is generated:


First name: John

E-Mail: john.smith@gxsoftware.com

Application Keys 40e9d997494ca5bbfdd

3. Highlight the application key and copy it to the application that will access content within XperienCentral. Place the application key in the custom `X-GX-AppKey HTTP` header.

Back to top

In This Topic

Components

The authorizations within XperienCentral are divided into two types:

- **Users of the Workspace** — XperienCentral backend users such as editors, application managers, and developers, and their privileges to configure settings and define pages. These users belong to one or more roles.
- **Registered website visitors** — You can control which content visitors to an XperienCentral website (frontend) have permission to view. In XperienCentral, these visitors referred to as web users. Web users belong to web groups. Permissions for web users are enforced at the web group level. For complete information on web users, see User Profiles.

In the Workspace environment, authorization management has been further divided into the following components:

- **Authorization - Users** — This component manages users of the Workspace and their privileges. The authorizations are assigned at the role level and determine which operations a user may perform in the various parts of XperienCentral. XperienCentral comes with a standard set of users, roles and permissions.
- **Authorization - Roles & Permissions** — This component enables administrators to modify the basic set of users, roles and permissions. The administrator can create and maintain users, create and maintain roles and assign permissions to roles.

Another related functionality is Workflow. Workflows control the allowed transition from one state to another for content items before they are allowed to be published on the web. The website administrator defines these states and configures their behavior. The states are then linked to user roles, which gives actual shape to the workflow. This XperienCentral functionality is based on the standards defined by the Workflow Management Coalition (WfMC).

Back to top

Role Based Access Control (RBAC)

Many RBAC models exist, but XperienCentral uses the Core RBAC and Hierarchical RBAC models. These models conform to the standard RBAC specification developed by ANSI/INCITS.

Roles and permissions

Role Based Access Control (RBAC) avoids the need to assign permissions to each user individually. Instead, permissions are assigned to roles. A role is a functional or organizational job description in which users sharing the same role share the same tasks. These roles then are assigned to users. The permissions of a role determine which operations a user may perform. RBAC is considerably less labor intensive than assigning permissions to each user individually. A user may have more than one role. An example of a permission is "Edit pages", which grants the permission to modify a page.

In the example above:

- User "John" has the role "Casual user" and therefore has permission to edit pages and maintain forms.
- User "Paula" has role "Editor", therefore she has further the permission to delete pages and maintain form models. Permission assignments may overlap one another, which is the case here for maintaining forms.

XperienCentral comes with a default set of roles and permissions

Permission groups

Nevertheless, defining proper permissions for each role may be a quite laborious operation. For this reason *permission groups* are introduced. A permission group is a default set of permissions which can be assigned to a role at once. A permission group assigned to a role will implicitly assign all permissions contained by that permission group to that role.

In the example above, role A has permissions b, c, e, f, g and i for the following reasons:

- Permission b and c through permission group A.
- Permission e, f and g through permission group B.
- Permission i through direct assignment.

XperienCentral comes with a standard set of permission groups, see Default Authorizations for more information.

Permission inheritance

Permissions can be assigned in two ways: directly and by means of permission groups. To make things even more flexible, a third way has been introduced: **permission inheritance**.

With permission inheritance, a role has assigned another role to it from which it inherits all permissions which means a child role gets all permissions from its parent role, irrespective of how these permissions have been assigned to the parent role.

In the example above, role B inherits all permissions from role A. So, referring to the example above, role B has the following permissions:

- Permissions b, c, e, f, g and i through inheritance.
- Permission d through direct assignment.

XperienCentral comes with a standard set of roles that inherit from each other, see Default Authorizations for more information.

Back to top

Default Authorizations

XperienCentral comes standard with the users, roles and permission groups listed below.

User	Role	Inherits from role	Permission group
	Casual user	Casual user permissions	
	Editor	Casual user	Editor permissions
	Main editor	Editor	Main editor permissions
Administrator	Application manager	Main editor	Application manager permissions
Developer	Developer	Application manager	Developer permissions

Developers are treated differently than all other users. Unlike all other users, developers are able to:

- View other users with developer permissions.
- Assign the permission group "Developer permissions" to roles.
- Assign the role "Developer" to users.
- Directly assign to roles the permissions of the category "Developer tools".

Basic set of permission groups by category

XperienCentral comes with five standard permission groups. In the "Roles" tab of the Authorization anel you can see which permissions each role has or can be assigned.

Back to top

Maintaining Roles

Selecting and Viewing a Role

To select and view a role:

1. Navigate to **Configuration > Authorization** and then click the [Roles] tab.
2. Select the desired role from the drop-down list next to "Select a role".
3. Click the [Details] tab to view the details for the role.
4. Click the [Permissions] tab to view the permissions for the role.

Creating a Role

To create a role:

1. Navigate to **Configuration > Authorization** and then click the [Roles] tab and then the [Details] tab.
2. Click [Create new role] in the "Role Selection" section.
3. Enter a name for the new role in the "Role name" text field and then click [Apply].
4. Define the other properties for the role.

Making a Role Available on all channels

To make a role available to all channels in a XperienCentral installation:

1. Select the desired role on the [Roles] - [Details] tab.
2. Select "Available on all Channels".
3. Click [Apply].

Assigning a User to a Role

A role may have one or more users and a user may have one or more roles. You can assign users and roles to one another in two ways:

- From the user point of view, see Assigning a Role to a User.
- From the role point of view.

To assign a user to a role:

1. Select the desired role from the [Roles] - [Details] tab.
2. Select the desired user from the "Add user" drop-down list. The user is added to the list.

Removing a user from a role

You can also separate users and roles from one another in two ways:

- From the user point of view, see Removing a Role from a User.
- From the role point of view.

To remove a user from a role:

- Select the desired role from the [Roles] - [Details] tab.
- In the list "Users assigned to this role", select the "Delete" checkbox next to the user to be removed.
- Click [Apply]. The user is removed from the list.

Assigning Permissions to a Role

The actual permissions a role gets is determined by the following:

- The permissions it inherits from another selected role.
- The permissions it gets from the assigned permission groups.

- The permissions that have been added directly to the role.

Inherited permissions and group permissions may overlap one another.

To assign permissions to a role:

1. Select the desired role from the [Roles] - [Details] tab.
2. To select the role to inherit from: select a role from the "Inherits all permissions from" drop-down list.
3. To add a permission group, select a permission from the "Add permission group" drop-down list. The permission group is added on top of the drop-down box.
4. To assign a permission directly: select the [Permissions] tab and select the desired permission(s).
5. Click [Apply].

Removing Permissions from a Role

To remove permissions from a role:

1. Select the desired role from the [Roles] - [Details] tab.
2. To remove all inherited permissions, : select "Select a role" from the "Inherits all permissions from" drop-down list.
3. To remove a permission group: in the list "Permission groups" section, select the "Delete" checkbox next to the permission group you want to remove. A pop-up message prompts you to copy the group permissions to the role directly. When you click [OK] the selected permission group is unassigned from the current role and all permissions from the unassigned group are assigned directly to the current role. If you click [Cancel] the permission group is unassigned from the current role and the role loses all permissions from the unassigned group.
4. To remove directly-added permissions: select the [Permissions] tab and clear the permissions to be removed.
5. Click [Apply].

Deleting a Role

To delete a role:

1. Select the role to be deleted from the [Roles] - [Details] tab.
2. Click [Delete role]. The role is removed from the "Select a role" drop-down list.

Finding a User and Viewing their Permission(s)

To find and view a user:

1. Navigate to **Configuration > Authorization** and click the [Users] tab.
2. To show a list of users:
    - Click "All users" to see the full list.
    - Click on a letter range to get a partial list of login names.
    - Click on the arrow in the "Login" column to toggle between alphabetical sorting in ascending (A-Z) and descending (Z-A) order.
3. To view the details for a user: click on the desired user in the list. The user details appear below the user.

Back to top

Maintaining Users

Creating a User

To create an new user:

1. Navigate to **Configuration > Authorization** and click the [Users] tab.
2. Click [Create new user]. A user called "New user" is added to the list.
3. Enter the login name of the new user in the "Login" field. This is the name that will appear in the upper right corner of the Workspace for the user.
4. Enter the password for the new user. For security reasons, it is highly recommended that you create a strong password. A strong password has all of the following characteristics:
    - Is at least 8 characters long.
    - Is significantly different than the previous passwords used by this user.
    - Contains a mix of uppercase and lowercase letters.
    - No string of letters spells out a word that appears in the dictionary of the language of the user.
    - Contains one or more numbers, but the numbers do not represent anything associated with the user such as their birthdate, age, house address, and so forth.
    - Contains one or more special characters. A special character is anything that is not a letter or a number or a space.
    - Does not contain any string of letters that spell the user's first or last name, their company name, their job description, their nickname, or any other word that could be associated with them personally.

When you type the new password into the field, the "Password Strength" field indicates the strength of their password using different colors. The following colors are used to indicate the password's strength:

- **Red** — The password is extremely weak.
- **Yellow** — The password is moderately weak.
- **Blue** — The password is good.
- **Green** — The password is strong.

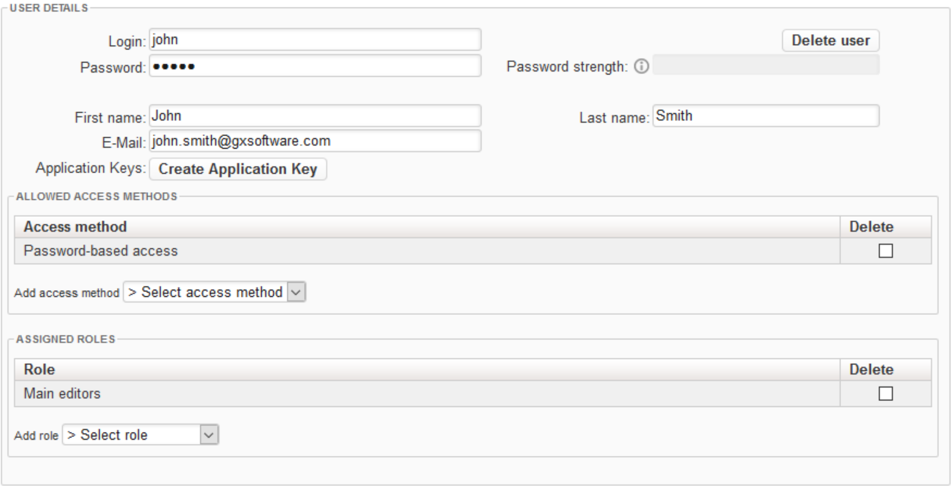
For security reasons, if you create/modify a user's password, the first time that they log in to XperienCentral after the modification, they must change their password. The only exception to this rule is when you change your own password.

5. Enter the new user's first name in the "First Name" field.
6. Enter the new user's last name in the "Last Name" field.
7. Enter the new user's e-mail address in the "E-Mail Address" field,
8. Select the method(s) that the user is allowed to use to log in to XperienCentral. The options are:

9. **Password-based access** — The user may log in from the XperienCentral login screen.
10. **Application key-based access** — The user may log in via the XperienCentral REST API. This is mainly used for external applications that want to access XperienCentral content. The application key is associated with a single user and it determines what permissions the external application has. When an application key is generated for the current user, this option wil be automatically added to the list of access options.
11. **Container-based access** — The user many log in from a backend container-based application.

This option is only available if the option `enable_backend_container_filter` in the "website_settings" section of the General tab of the XperienCentral Setup Tool is selected.

12. Select one or more roles for the user. For example:



USER DETAILS

Login:	john		Delete user
Password:	●●●●●	Password strength: ⓘ	
First name:	John	Last name:	Smith
E-Mail:	john.smith@gxsoftware.com		
Application Keys:	Create Application Key		

ALLOWED ACCESS METHODS

Access method	Delete
Password-based access	□

Add access method > Select access method

ASSIGNED ROLES

Role	Delete
Main editors	□

Add role > Select role

13. Click [Apply].

Modifying a User

To modify a user's details, follow these steps:

1. Select the desired user by navigating to **Configuration > Authorization** and then click the [Users] tab.
2. Modify the user's details.
3. Click [Apply].

For security reasons, if you modify a user's password, the first time that they log in to XperienCentral after the modification, they must change their password. The only exception to this rule is when you change your own password.

Assigning a Role to a User

In order to have access to XperienCentral, every user must have at least one role. You can assign users and roles to one another in two ways:

- From the role point of view, see Assigning a User to a Role.
- From the user point of view.

To assign a role to a user:

1. Select the desired user by navigating to **Configuration > Authorization** and then click the [Users] tab.
2. Select the desired role from the "Add role" drop-down list. The role is added to the list.

Removing a Role from a User

You can separate roles and users from one another in two ways:

- From the role point of view, see Removing a User from a Role.
- From the user point of view.

To remove a role from a user:

1. Display the desired user by navigating to **Configuration > Authorization** and then clicking the [Users] tab.
2. In the "Assigned roles" list, select the "Delete" checkbox of the role that is to be removed.
3. Click [Apply]. The role is removed from the list.

Deleting a User

To delete a user:

1. View the user that is to be deleted by navigating to **Configuration > Authorization** and then clicking the [Users] tab.
2. Do one of the following:
    - In the list of users, select the "Delete" checkbox next to the user that is to be removed. Click [Apply].
    - In the "User details" section, click [Delete user].

Importing Users from Other Websites

To allow users of another website (channel) to access to this website, their user data can be imported. Imported users maintain the same user name and password. Different websites, however, can have different permissions assigned to their roles.

To import users:

1. Navigate to **Configuration > Authorization** and then click the [Import] tab.
2. Select the website to import users from
3. Check the users to be imported to your current site and click [Apply].

Back to top

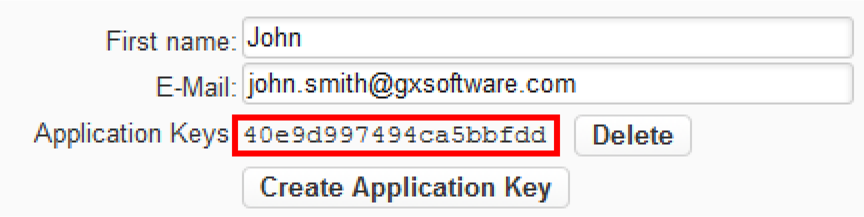
Generating an Application Key for a User

An external application can log in to XperienCentral via the REST API. This makes it possible for external applications to access XperienCentral content. In order to be able to do so, you have to generate an application key for a user.

An application key is tied to a user, which means that the application key used by an external application inherits the role and permissions from the user for whom the application key is generated. For this reason, be sure that you generate an application key with sufficient permission(s) in order for the external application to be able to perform the task(s) for which it is designed. When performing REST calls, the application key should be placed in the custom `X-GX-AppKey HTTP` header.

To generate an application key for a user, follow these steps:

1. Select the user for whom you want to generate an application key from the list.
2. Click [Create Application Key] next to the "Application Keys" field. The application key is generated:



First name: John

E-Mail: john.smith@gxsoftware.com

Application Keys 40e9d997494ca5bbfdd

3. Highlight the application key and copy it to the application that will access content within XperienCentral. Place the application key in the custom `X-GX-AppKey HTTP` header.

Back to top