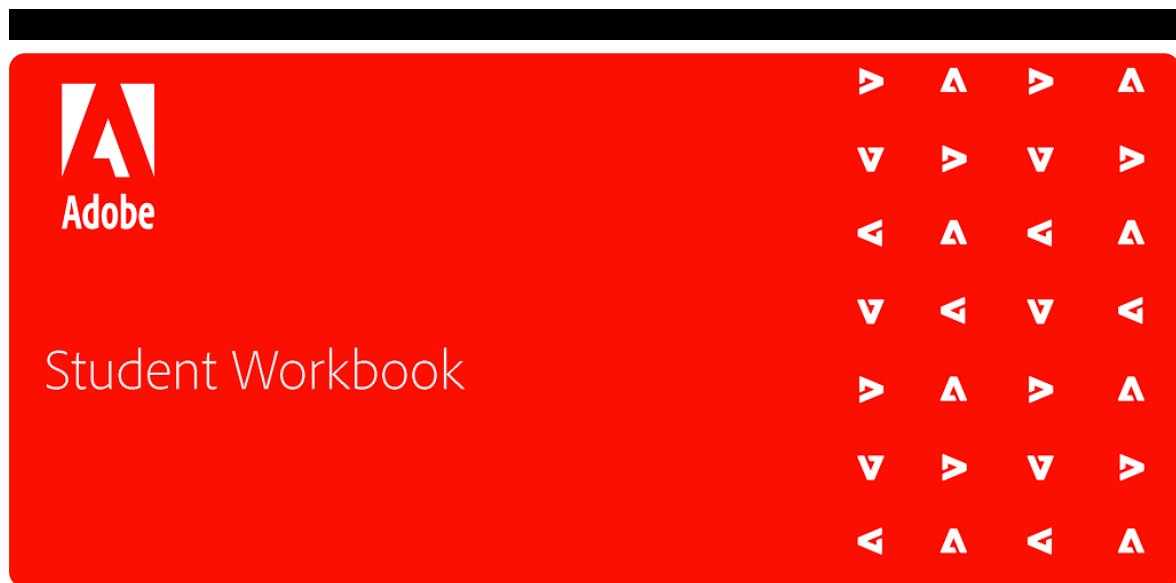


Manage Users, Groups and Permissions in AEM



[Find your journey at learning.adobe.com >](https://learning.adobe.com)

Contents

Manage Users, Groups and Permissions in AEM

Introduction

Identity Management System (IMS)

Architecture

IMS Set up

Users and Groups

Built-in Users and Groups

Permissions and ACLs

Access Consoles for Content

Managing Permissions

Permission States

Managing ACLs

Exercise 1: Create authoring groups

Exercise 2: Assign permissions to groups

Exercise 3: Manage and test group permissions

Exercise 4: Sync permission groups to the Maven project

©2020 Adobe. All rights reserved.

DevOps for AEM as a Cloud Service

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe. Adobe assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

Any references to company names in sample templates are for demonstration purposes only and are not intended to refer to any actual organization.

Adobe, the Adobe logo, Acrobat, the Creative Cloud logo, and the Adobe Marketing Cloud logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Adobe, 345 Park Avenue, San Jose, California 95110, USA.

Notice to U.S. Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

10-14-2020

Introduction

You need to configure users, groups, and permissions when implementing Adobe Experience Manager (AEM). Permissions configuration governs access to content and functionality in AEM. This is a critical task to secure the system, tools, and data. You can configure most users, groups, and permissions in the AEM UI. For some configurations, you need other tools and consoles.

Objectives

After completing this module, you will be able to:

- Describe Identity Management System (IMS)
- Explain the users and groups in AEM
- Explain permissions and Access Control Lists (ACLs)
- Create and configure users and groups in AEM
- Assign permissions to users and groups
- Manage group permissions
- Sync permission groups to the Maven project

Identity Management System (IMS)

Adobe's Identity Management System (IMS) helps admins create and manage user access for applications and services. Adobe offers three types of identities or accounts to authenticate and authorize users. They all use an email address as the user name.

The three identity types are:

- **Federated ID:** Created, owned, and managed by an organization and linked to the enterprise directory through federation. The organization manages credentials and processes Single Sign-On (SSO) through a Security Assertion Markup Language 2 (SAML2) IDP.
- **Enterprise ID:** Created, owned, and managed by an organization. Adobe hosts the Enterprise ID and performs authentication, and the organization maintains the Enterprise ID.
- **Adobe ID:** Created, owned, and managed by the end user. Adobe performs the authentication and the end user manages the identity.

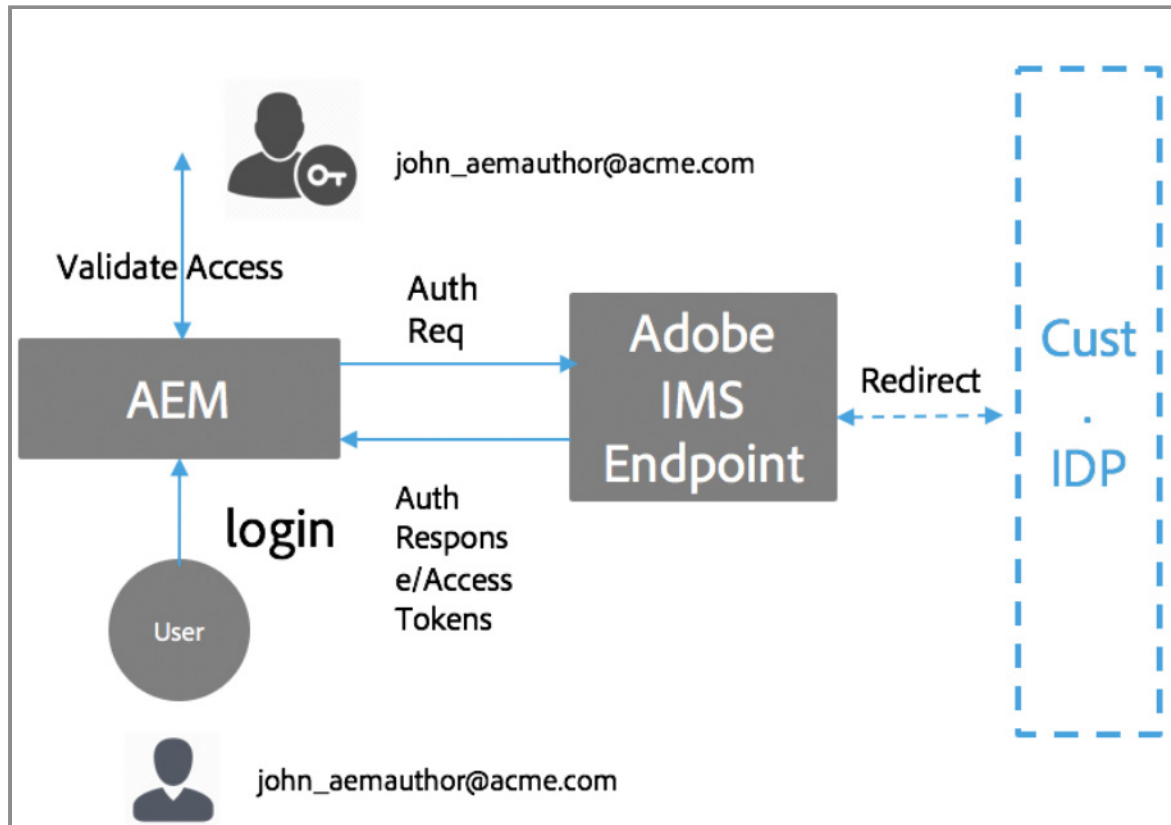
Choosing the correct identity model can have a considerable impact on the way assets are stored and shared by an organization. The Enterprise and Federated ID models are an ideal choice for enterprises, and the Adobe ID is best suited for individuals.

The Federated ID provides multi-factor authentication and is the most secure identity model. The Adobe ID works best when there is no need for internal control. It is user-friendly, but not the best option to leverage the enterprise storage. Because your end users may not always adhere to the best practices, it is advisable to use the Federated and Enterprise IDs. If you are uncertain which identity model is right for you, contact Adobe Customer Care.

Architecture

IMS authentication works by using the OAuth protocol between AEM and the Adobe IMS endpoint. After a user is added to IMS and is assigned an Adobe Identity, the user can log in to AEM Managed Services (AMS) instances by using the IMS credentials.

The user login flow is shown in the following screenshot. The user will be redirected to IMS and optionally to the customer IDP for SSO validation, and then redirected back to AEM.



IMS Set up

The IMS set up consists of two steps:

1. Onboard organizations to the Adobe Admin console
2. Onboard users to the Adobe Admin console

Onboarding Organizations to Admin Console

The Adobe Admin console provides a central location for managing Adobe entitlements across the entire organization. The customer onboarding to the Adobe Admin console is a prerequisite for using Adobe IMS for AEM authentication.

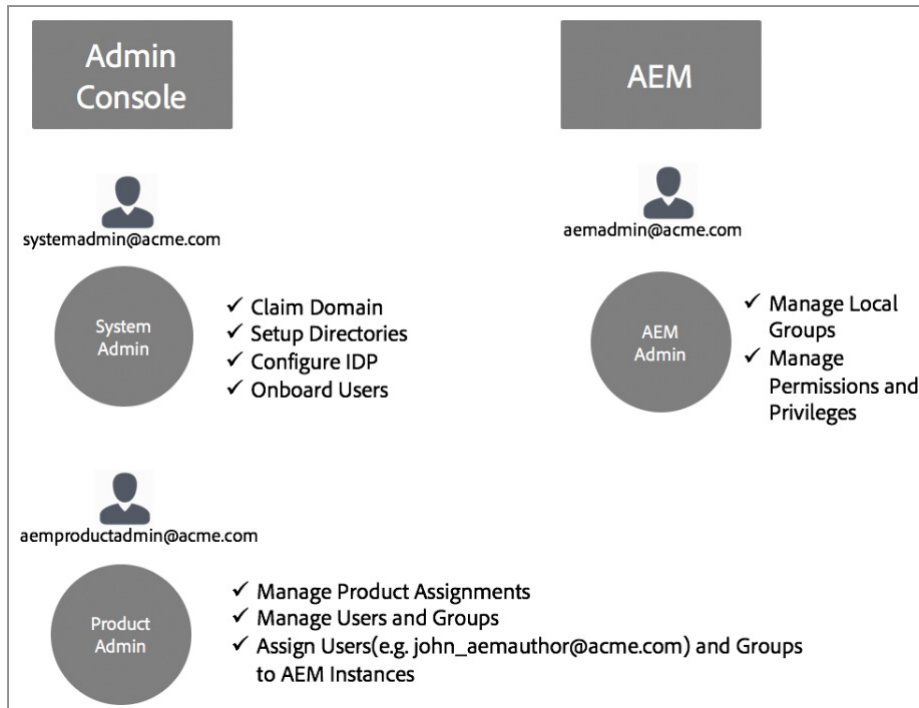
As the first step, customers should have an Organization provisioned in Adobe IMS. Adobe Enterprise customers are represented as IMS Organizations in the Adobe Admin console.

AMS customers have an organization provisioned. As part of the IMS provisioning, the customer instances will be made available in the Admin Console for managing user entitlements and their access.

The steps involved in the onboarding organizations to Adobe Admin console are:

1. The designated System Admin receives an invite to log in to the Admin Console.
2. The System Admin claims the domain to confirm the ownership of the domain (in this example, acme.com).
3. The System Admin sets up user Directories.
4. The System Admin configures the IDP in the Admin Console for SSO setup.

5. The AEM admin manages the local groups, permissions, and privileges.



Onboarding Users to the Adobe Admin console

There are three ways to onboard users to the Adobe Admin console depending on the size of the customer and their preference:

- Create users manually through the Adobe Admin console UI
- Upload the file to the Adobe Admin console
- By using the user sync tool (UST)

Create users manually through the Adobe Admin console UI

You can create users and groups manually in the Adobe Admin console UI. You can use this method if you do not have a large number of users to manage. For example, you can use this method if you have less than 50 AEM users.

You can create users manually if the customer is already using this method for administering other Adobe products such as Analytics, Target, or Creative Cloud applications.

Upload the file to the Adobe Admin console

For handling user creation with ease, you can upload a CSV file to add users in bulk.

By using the user sync tool (UST)

The UST enables enterprise customers to create or manage Adobe users utilizing Active Directory or other tested OpenLDAP directory services. The IT Identity administrators can install and configure the tool. UST is an open source tool that can be customized so that the developers of customer organizations can modify it to suit their requirements.

Tip: To learn more about IMS, see ¹

Users and Groups

An AEM user is either a human or an external system connected to AEM. Groups are collections of users and other groups.

Each user will have a user account that holds the details needed to access AEM. The purpose of a user account is to provide the required information for authentication and login process. Each user account is unique and maintains the basic account details of the user, and the privileges assigned to the user. Users are often the members of groups that simplify the allocation of these permissions and/or privileges.

The primary purpose of a group is to simplify the AEM maintenance process by reducing the number of entities to be updated. When a change is made to a group, it is applied to all members of the group.

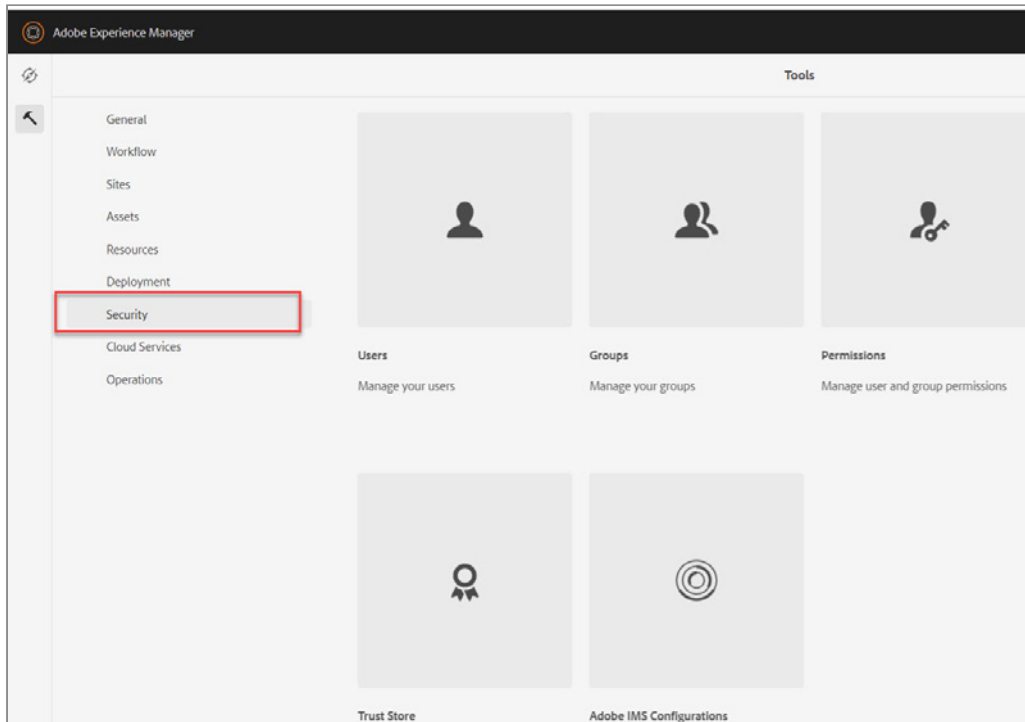
Groups can be:

- A role within the application. For example, someone who can surf the content, or someone who is allowed to contribute content.
- Your own organization. You may want to extend the roles to differentiate between contributors and different departments restricted to different branches in the content tree.

Built-in Users and Groups

AEM has several users and groups installed out-of-the-box. You can see these users and groups from the Security console.

To access the Security console, click Adobe Experience Manager from the header bar and navigate to **Tools > Security**, as shown:



From the Security console, the most commonly used subconsoles are Users, Groups, OAuth Clients, and Permissions.

The following table describes the subconsoles of the Security console:

Consoles	Description
Users	Create and manage users
Groups	Create and manage groups
OAuth Clients	Manage registered clients
Permissions	Manage users & Group permissions

Permissions and ACLs

In AEM, permissions define who can perform actions on a resource. AEM uses ACL to organize the permissions applied to the various resources. ACLs are made up of individual permissions and determines the order in which these permissions are applied. The ACL is formed according to the hierarchy of the resources under consideration. This list is then scanned until the first appropriate permission is found.

AEM provides a set of predefined permissioned groups:

Platform Specific

- Administrators
- User admins
- Contributors (Read only)

The best practice is to use built-in groups as much as possible.

Access Consoles for Content

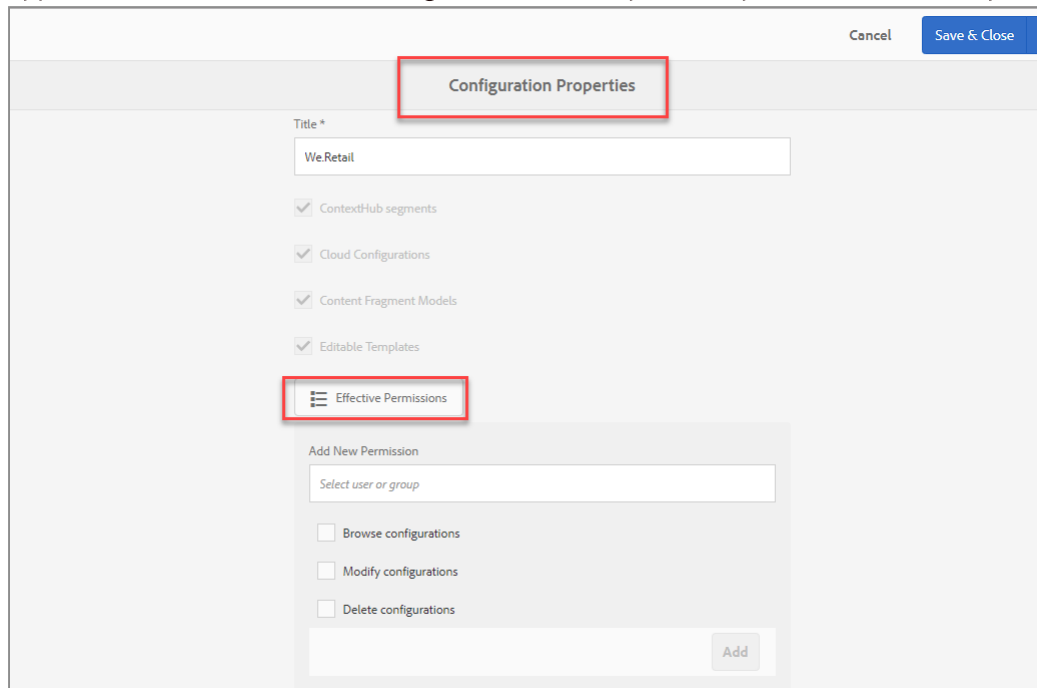
The following table lists the consoles and the permissions that can be assigned to different resources from each console:

Consoles	Permissions
Sites > myPage > Properties > Experience Fragments > myXF > PropertiesConfiguration Browser	Browse, Edit, Delete, Publication, Create sub-page
Assets > myFolder > Properties > Collections > myCollection > Properties > Projects > myProject > Team	Owner, Editor, Viewer
Configuration Browser > myConfig > Properties(editable templates, Content Fragment Models, contexthub, and cloud services)	Browse, Modify, Delete

Organizations generally define multiple roles, with varying skill sets, for the purpose of granting access to AEM resources and functionality. For these purposes, AEM provides multiple tools:

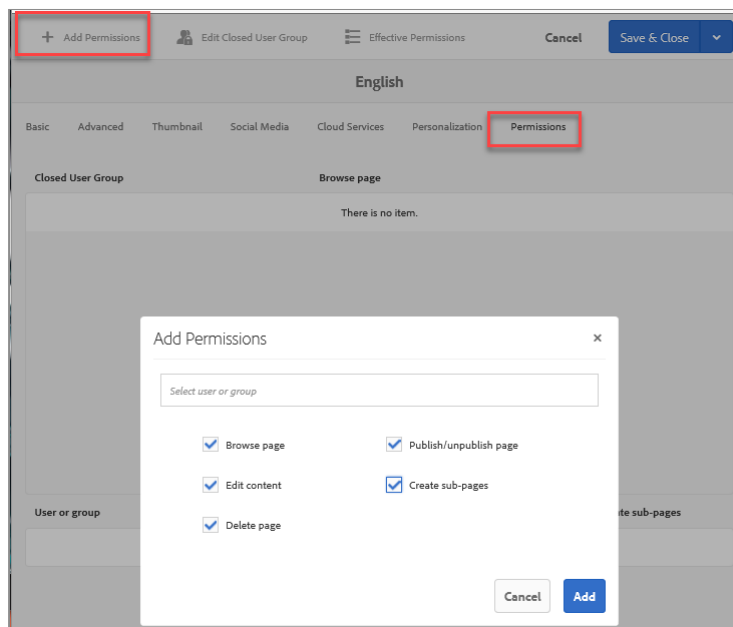
- Configuration Browser – To manage the access to Template Editor, Content Fragment Model Editor, and ContextHub Segment Editor
- Permissions tab in the Properties pane – To manage the access to pages
- Permissions Console – To manage detailed management of Access Control Lists.

The Configuration Browser, found at **Tools > General > Configuration Browser**, enables application administrators to manage access to the 'power/super user' functionality, as shown:



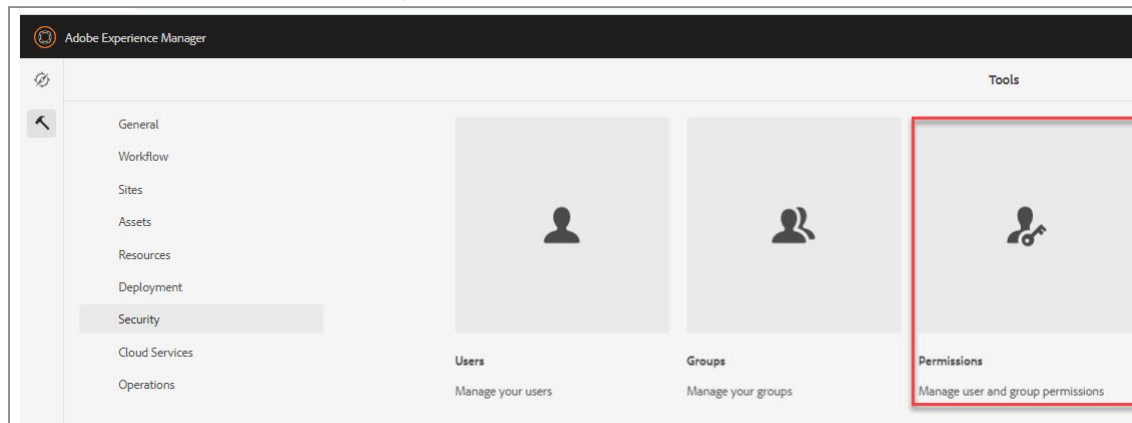
Setting Permissions on Pages

Using the Permissions tab in the Properties pane, an author with the ability to manage users can grant or deny access to a page and all its child pages, as shown:

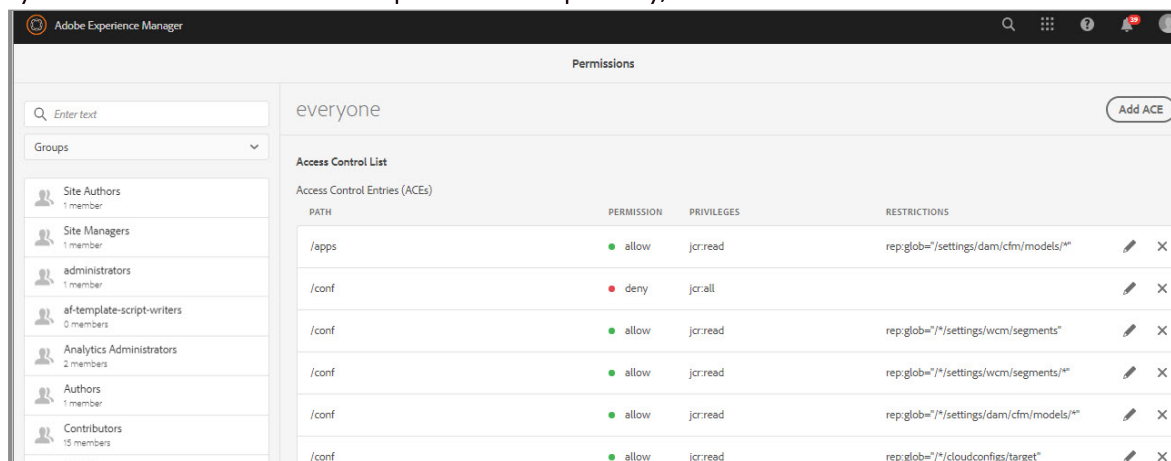


Managing Permissions

You can view and edit user and group permissions from the Permissions console. You can access this console from **Tools > Security > Permissions**, as shown:



In the Permissions console, the tree on the left lists all users and groups currently available in the system. The console includes all paths in the repository, as shown:



Permission States

You can change the permissions granted or denied to a given user from Permission Type, as shown:

ACLs are made up of individual permissions. Access Control Entries (ACE) are used to determine the order in which those permissions are applied. A list of effective permissions is formed by assembling all the ACEs in all of the ACLs in the parent hierarchy. This list is then scanned bottom-up until the first appropriate permission to apply to the specified page, asset, or other resource is found. and that permission is then applied.

Concurrent Permissions in ACLs

When two concurrent (and opposing) permissions are listed on the same ACL for the same resource, the permission at the bottom is applied to the resource. An administrator can modify which permission is applied by changing the order of the conflicting permissions.

Managing ACLs

AEM uses ACLs to organize the permissions being applied to the various pages. ACLs are made up of the individual permissions and are used to determine the order in which these permissions are actually applied.

An administrator can manage access control policies by using the Permissions console, accessed at Tools > Security > Permissions. The ACEs displayed by this console contain granular JCR privileges, as defined in the Java Solution Request (JSR) 283 specification. Each privilege is either Allowed or Denied. To take any action in the repository, the aggregates of privileges are typically required. For example, in order to remove a node, the node must have the jcr:removeNode privilege and the parent node must have the jcr:removeChildNodes privilege.

The screenshot shows a dialog box titled "Add New Entry for 'content-authors'". It has a "Cancel" button and an "Add" button. The dialog contains several sections: "Path" with a text input field "Type a Path" and a checkmark icon; "Privileges" with a text input field "Type to add privileges" containing "jcr:removeNode" (highlighted with a red box) and a close icon; "Permission Type" with radio buttons for "Deny" and "Allow" (selected); and "Restrictions" with a "Select Type" dropdown and a "Restr..." button with a plus icon.

The recommendations to manage ACLs are:

- Do not assign permissions directly to users. Assign them only to groups. It simplifies the maintenance (of users) because the number of groups is much smaller than the number of users and less volatile.
- Do not grant a group or user to create or deny rights if you want them to only modify pages. You can grant them modify and read rights.
- Use the **Deny** option sparingly. As often as possible, use only the **Allow** option.

Note: To learn more about Role-based Permissions, ².

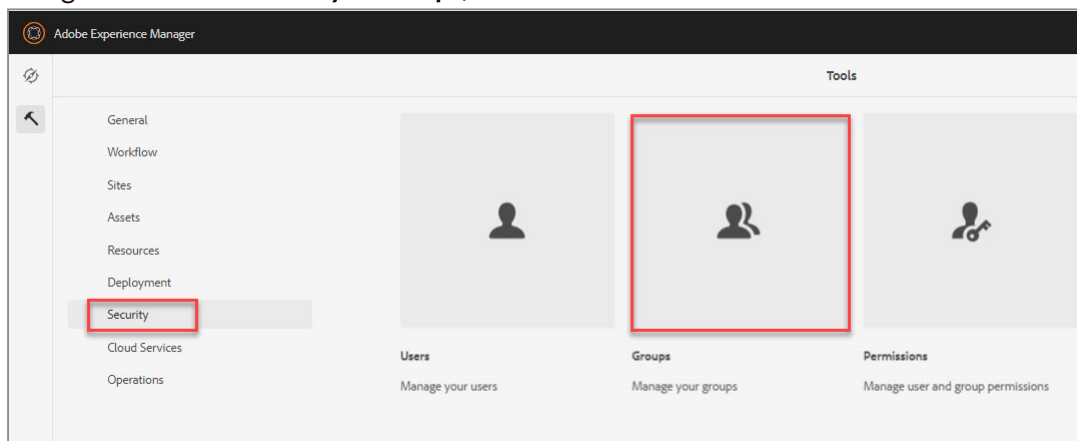
Note: If you are going to be using the Permissions Console to define ACLs, you should read and understand Chapters 9 Permissions and Capabilities and 16 Access Control Management in the JCR v2.0 Specification (known as JSR 283) ³ and ⁴.

Exercise 1: Create authoring groups

Scenario: As an administrator, you need to create, configure, and manage new users and groups. You need to add permissions by assigning roles to users and groups that will help them perform different tasks on resources.

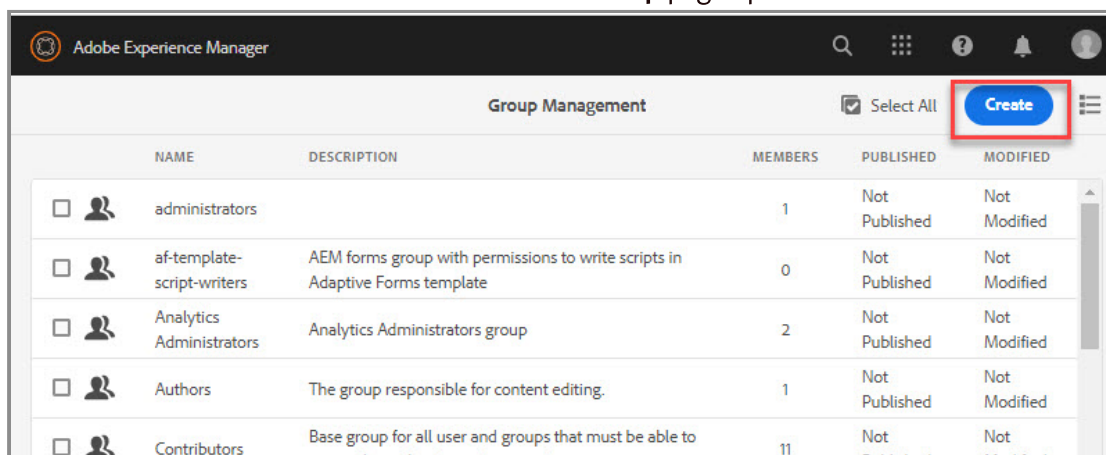
In this exercise, you will create groups in AEM as an administrator from the Security console. You do not need to use any other development or administrative tools.

1. Navigate to **Tools > Security > Groups**, as shown:



The **Group Management** page opens.

2. Click **Create** on the actions bar. The **Create New Group** page opens.



3. Type **Site Authors** in the ID and Name fields.

Create New Group

Cancel Save & Close

Details Members

ID *

Site Authors

Name

Site Authors

Description

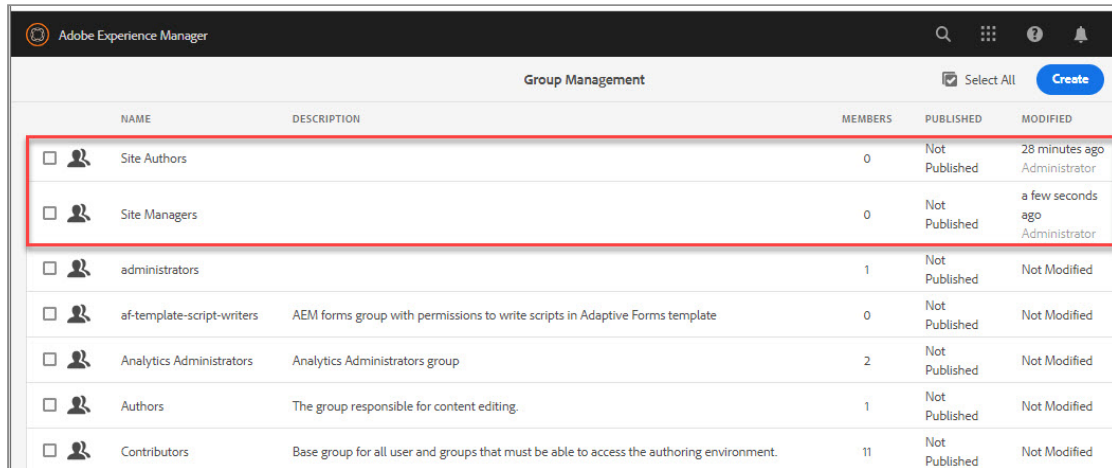
New Photo

4. Click **Save & Close**.

A success message appears on the **Group Management** page. Your group is now created.

5. Perform steps 2 to 4 to create **Site Managers** group.

6. Scroll down on the **Group Management** page to locate your newly created groups, as shown:



The screenshot shows the Adobe Experience Manager Group Management interface. At the top, there's a header with the Adobe Experience Manager logo and navigation icons. Below the header, the title 'Group Management' is centered, with a 'Select All' checkbox and a 'Create' button on the right. The main content is a table with columns: NAME, DESCRIPTION, MEMBERS, PUBLISHED, and MODIFIED. The table lists several groups, with 'Site Authors' and 'Site Managers' highlighted by a red box. The 'Site Managers' group is newly created, as indicated by the 'a few seconds ago' timestamp.

NAME	DESCRIPTION	MEMBERS	PUBLISHED	MODIFIED
<input type="checkbox"/> Site Authors		0	Not Published	28 minutes ago Administrator
<input type="checkbox"/> Site Managers		0	Not Published	a few seconds ago Administrator
<input type="checkbox"/> administrators		1	Not Published	Not Modified
<input type="checkbox"/> af-template-script-writers	AEM forms group with permissions to write scripts in Adaptive Forms template	0	Not Published	Not Modified
<input type="checkbox"/> Analytics Administrators	Analytics Administrators group	2	Not Published	Not Modified
<input type="checkbox"/> Authors	The group responsible for content editing.	1	Not Published	Not Modified
<input type="checkbox"/> Contributors	Base group for all user and groups that must be able to access the authoring environment.	11	Not Published	Not Modified

Exercise 2: Assign permissions to groups




Scenario: In this exercise, you will give basic access to Site Authors and Site Managers. You will also give Workflow user access to Site Authors. This will enable users to use workflows to request things such as publishing, deleting, moving.

This exercise includes the following tasks:

1. Provide basic read access to Site groups
2. Provide Workflow user access to Site Authors
3. Provide permission control to Site Managers

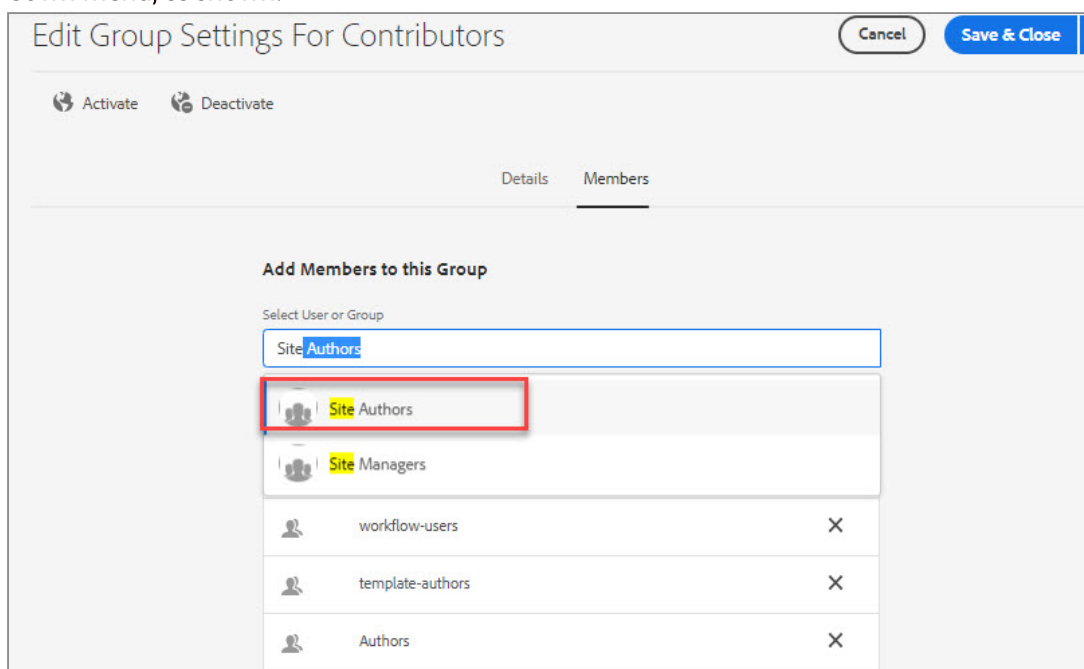
Task 1: Provide basic read access to Site groups

1. Navigate to **Tools > Security > Groups**. The **Group Management** page opens.
2. On the **Group Management** page, locate and click on the **Contributors** group, as shown:

Group Management				
		<input checked="" type="checkbox"/> Select All	Create	
Name	Description	Members	Published	Modified
 Authors	The group responsible for content editing.	8	Not Published	Not Modified
 Contributors	Base group for all user and groups that must be able to access the authoring environment.	23	Not Published	Not Modified
 DAM Users	Users of the DAM system	4	Not Published	Not Modified

The **Edit Group Settings For Contributors** page opens.

3. Click the **Members** tab.
4. Type **Site Authors** in the **Select User or Group** field and select **Site Authors** from the drop-down menu, as shown:



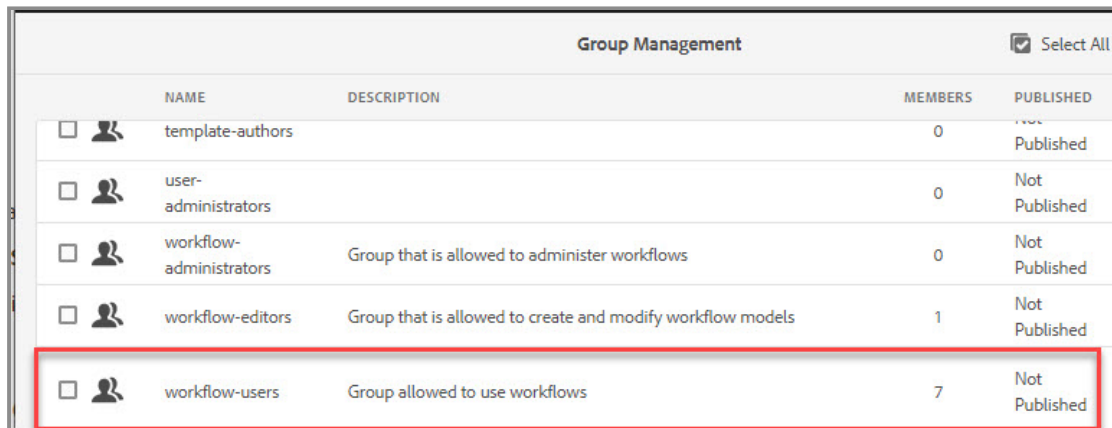
5. Similarly add the **Site Managers** to the **Contributors** group.

6. Click **Save & Close**.

A success message appears on the **Group Management** page. The Site groups are now added to the **Contributors** group.

Task 2: Provide Workflow user access to Site Authors

1. On the **Group Management** page, locate and click the **workflow-users** group, as shown:



Group Management				<input checked="" type="checkbox"/> Select All
	NAME	DESCRIPTION	MEMBERS	PUBLISHED
<input type="checkbox"/>	template-authors		0	Not Published
<input type="checkbox"/>	user-administrators		0	Not Published
<input type="checkbox"/>	workflow-administrators	Group that is allowed to administer workflows	0	Not Published
<input type="checkbox"/>	workflow-editors	Group that is allowed to create and modify workflow models	1	Not Published
<input type="checkbox"/>	workflow-users	Group allowed to use workflows	7	Not Published

The **Edit Group Settings For workflow-users** page opens.

2. Click the **Members** tab.

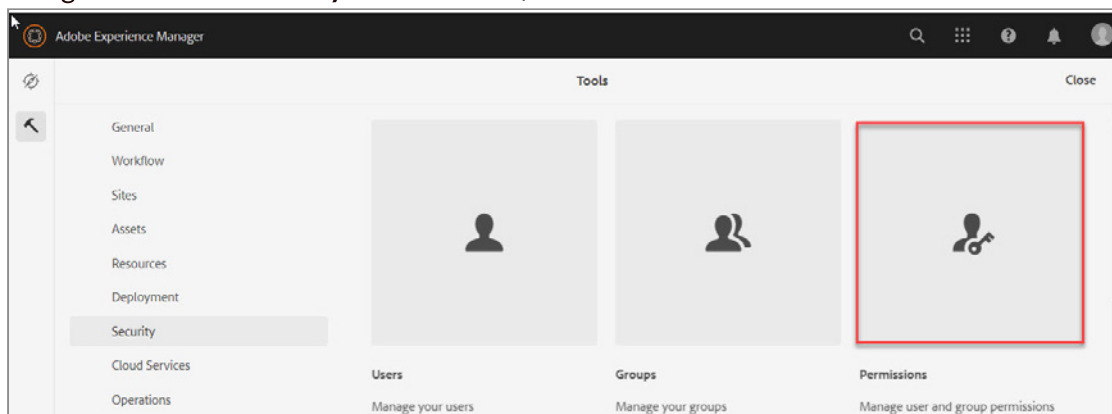
3. Type **Site Authors** in the **Select User or Group** field and select **Site Authors** from the drop-down menu. The **Site Authors** group gets selected.

4. Click **Save & Close**.

A success message appears on the **Group Management** page. The **Site Authors** group is now added to the **workflow-users** group.

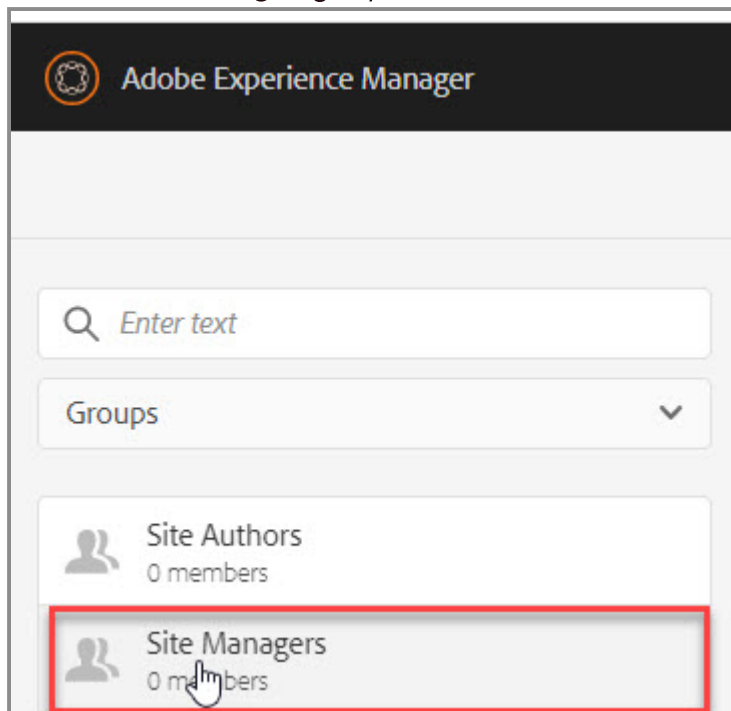
Task 3: Provide permission control to Site Managers

1. Navigate to **Tools > Security > Permissions**, as shown:



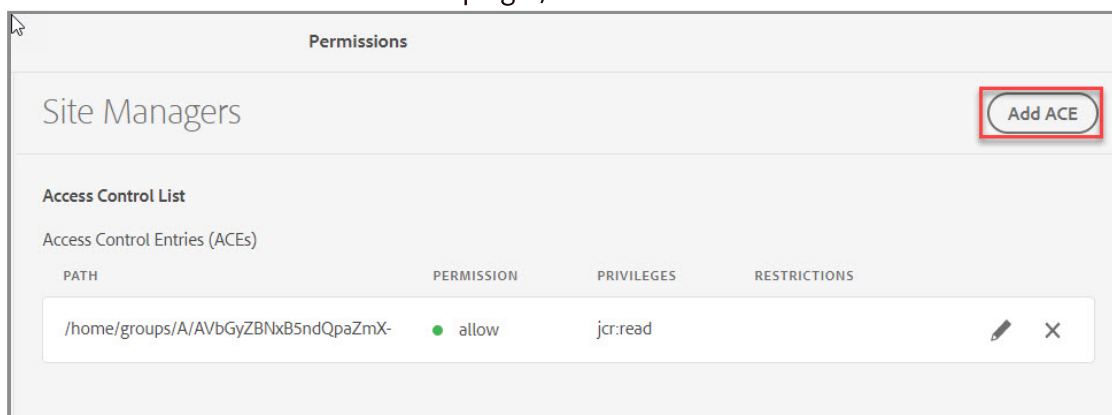
The **Permissions** page opens.

2. Select the **Site Managers** group, as shown:



The **Access Control List** for **Site Managers** page opens.

3. Click **Add ACE** button located at the top right, as shown:



The **Add New Entry for "Site Managers"** screen is displayed.

4. Enter the value for Path and select Privileges from the drop-down list, as shown:

Path: **/content** (Click Open Selection Dialog and select the path)

Privileges: **jcr:readAccessControl; jcr:modifyAccessControl;**

Add New Entry for "Site Managers"

Path: /content

Privileges: jcr:readAccessControl, jcr:modifyAccessControl

Permission Type: Deny, Allow

5. Click the **Add** button at the top, as shown:

Add New Entry for "Site Managers"

Path: /content

Privileges: jcr:readAccessControl, jcr:modifyAccessControl

Permission Type: Deny, Allow

The **Permissions** are added.

6. Click **Add ACE** to give more permissions to **Site Managers**. The Add New Entry for "Site Manager" page opens.

7. Enter the value for Path and select Privileges from the drop-down list, as shown:

Path: **/home** (Click Open Selection Dialog and select the path)

Privileges: **jcr:read**

The screenshot shows a dialog box titled "Add New Entry for 'Site Managers'". It has a "Cancel" button and an "Add" button. Inside the dialog, there is a "Path" field with the value "/home" and a "Privileges" field with the value "jcr:read". Both fields are highlighted with red boxes. The "Privileges" field is a dropdown menu with a small "x" icon next to the selected value.

The **Permissions** are added, as shown:

The screenshot shows the "Site Managers" page. It has an "Add ACE" button. Below the button is the "Access Control List" section, which contains a table of "Access Control Entries (ACEs)". The table has four columns: "PATH", "PERMISSION", "PRIVILEGES", and "RESTRICTIONS". The first two rows of the table are highlighted with a red box. The first row shows the path "/content" with the permission "allow" and the privileges "jcr:modifyAccessControl, jcr:readAccessControl". The second row shows the path "/home" with the permission "allow" and the privilege "jcr:read". The third row shows the path "/home/groups/A/AVbGyZBNxB5ndQpaZmX-" with the permission "allow" and the privilege "jcr:read".

PATH	PERMISSION	PRIVILEGES	RESTRICTIONS
/content	allow	jcr:modifyAccessControl, jcr:readAccessControl	
/home	allow	jcr:read	
/home/groups/A/AVbGyZBNxB5ndQpaZmX-	allow	jcr:read	

Exercise 3: Manage and test group permissions

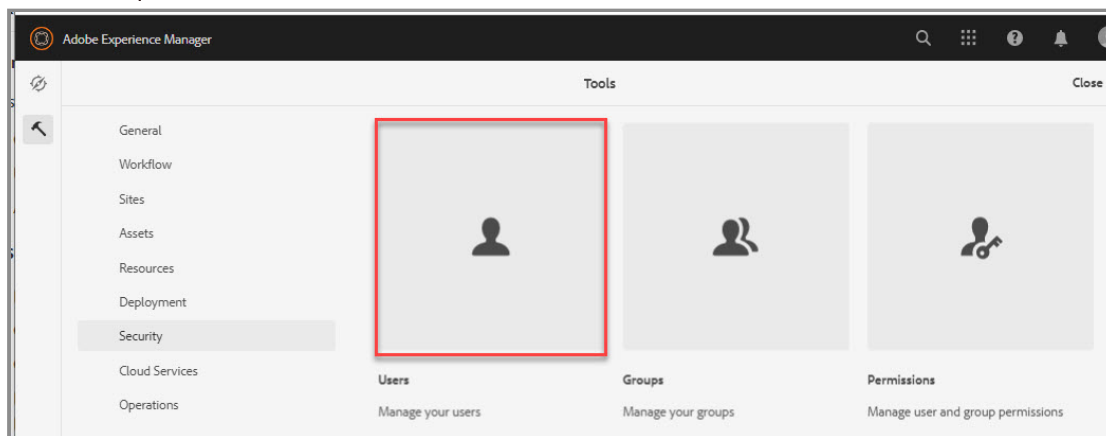
Scenario: In this exercise, you will create QA user accounts and add them to appropriate groups.

This exercise includes the following tasks:

1. Provide permissions to QA user accounts
2. Provide Site permissions by using a Site Manager
3. Author a page as a Site Author user

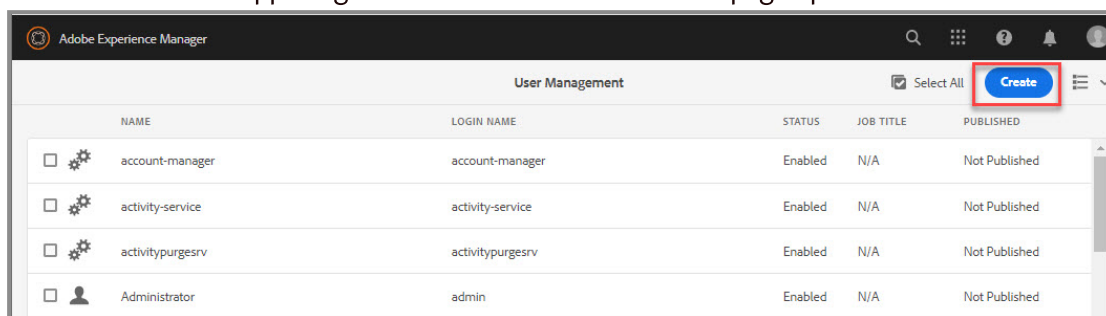
Task 1: Provide permissions to QA user accounts

1. In **AEM**, navigate to **Tools > Security**.
2. Click **Users**, as shown:



The **User Management** page opens.

3. Click **Create** at the upper-right corner. The **Create New User** page opens.



4. Provide the following new user details on the **Create New User** page. Ensure all required fields are populated, as shown:

- a. ID: **cgrant**
- b. Password: **cgrant**
- c. First Name: **Chuck**
- d. Last Name: **Grant**

The screenshot shows the 'Create New User' form with the 'Details' tab selected. The form has a 'Cancel' button and a 'Save & Close' button at the top right. The 'Details' tab is active, and the following fields are populated with red boxes around them:

- ID *: cgrant
- Password *: cgrant
- Retype Password *: cgrant
- First Name: Chuck
- Last Name: Grant

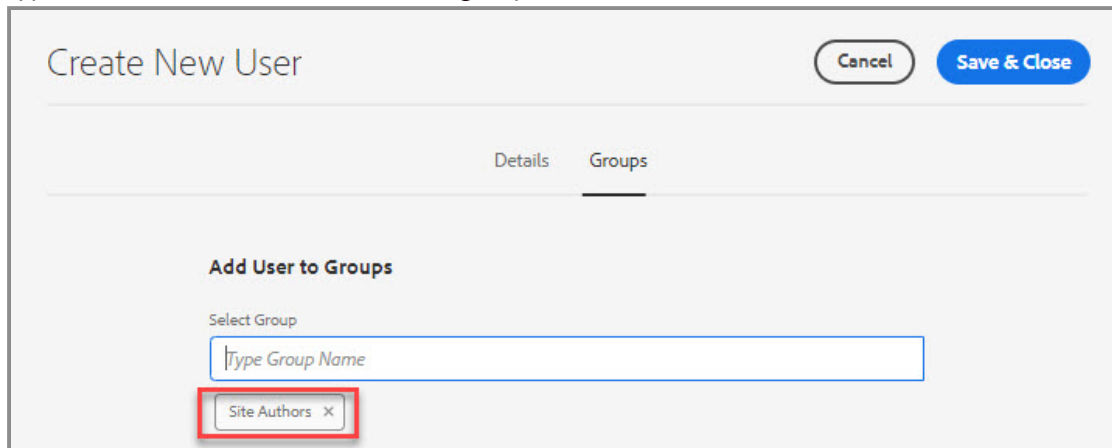
Other fields like Email and Title are empty.

5. Click the **Groups** tab, as shown:

The screenshot shows the 'Create New User' form with the 'Groups' tab selected. The 'Groups' tab is highlighted with a red box. Below the tabs, there is a section titled 'Add User to Groups' with a 'Select Group' dropdown menu. The dropdown menu is open, showing a search bar with the placeholder text 'Type Group Name'.

The **Add User to Groups** window opens.

6. Type Site into the **Add User to Groups** field. This will retrieve the user you created by auto-type in AEM. Select the **Sites Authors** group, as shown:

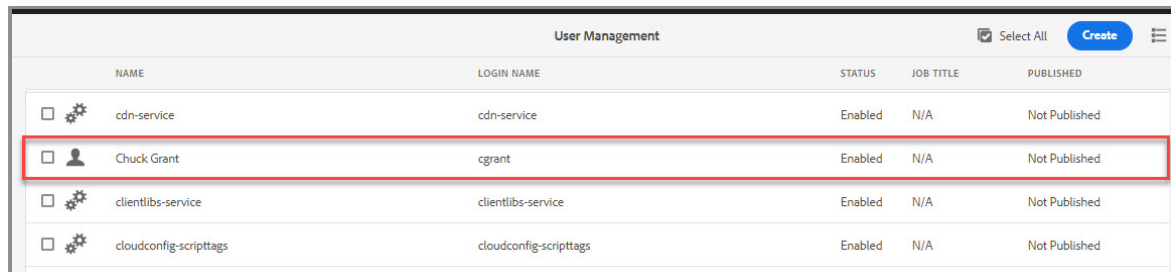


The screenshot shows the 'Create New User' dialog box with the 'Groups' tab selected. Under the 'Add User to Groups' section, there is a 'Select Group' label above a text input field containing 'Type Group Name'. Below the input field, a dropdown menu is open, showing 'Site Authors' with a red box around it. The 'Save & Close' button is visible in the top right corner.

You should see Chuck Grant's user account now added to the group, as displayed above.

7. Click **Save & Close** in the upper right. Your new user (Chuck Grant) is now created. A success message displays on the **User Management** page.
8. Scroll down on the **User Management** page to locate your newly created user, as shown:

Note: By default, all users are displayed alphabetically by ID (Login Name).



User Management					
<input checked="" type="checkbox"/> Select All Create					
	NAME	LOGIN NAME	STATUS	JOB TITLE	PUBLISHED
<input type="checkbox"/>	cdn-service	cdn-service	Enabled	N/A	Not Published
<input type="checkbox"/>	Chuck Grant	cgrant	Enabled	N/A	Not Published
<input type="checkbox"/>	clientlibs-service	clientlibs-service	Enabled	N/A	Not Published
<input type="checkbox"/>	cloudconfig-scripttags	cloudconfig-scripttags	Enabled	N/A	Not Published

Tip: To locate a user (or group), use the built-in search feature. For example, if you want to locate Virginia Armstrong's user account, type "/" to search within AEM and type "Virginia". This will retrieve the corresponding user account.

9. Similarly, perform steps 3 and 4 to create another user named Jane Brown by providing the following details:
- a. ID: **jbrown**
 - b. Password: **jbrown**
 - c. First Name: **Jane**
 - d. Last Name: **Brown**

10. Click the **Groups** tab. The **Add User to Groups** window is displayed.

11. Type Site into the **Add User to Groups** field. This will retrieve the user you created by auto-type in AEM. Select the **Sites Managers** group.

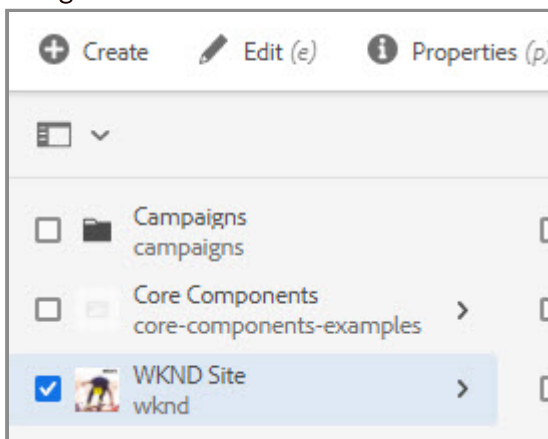
You should see Jane Brown's user account now added to the group.

12. Click **Save & Close** at the upper right. Your new user (Jane Brown) is now created. A success message is displayed on the **User Management** page.

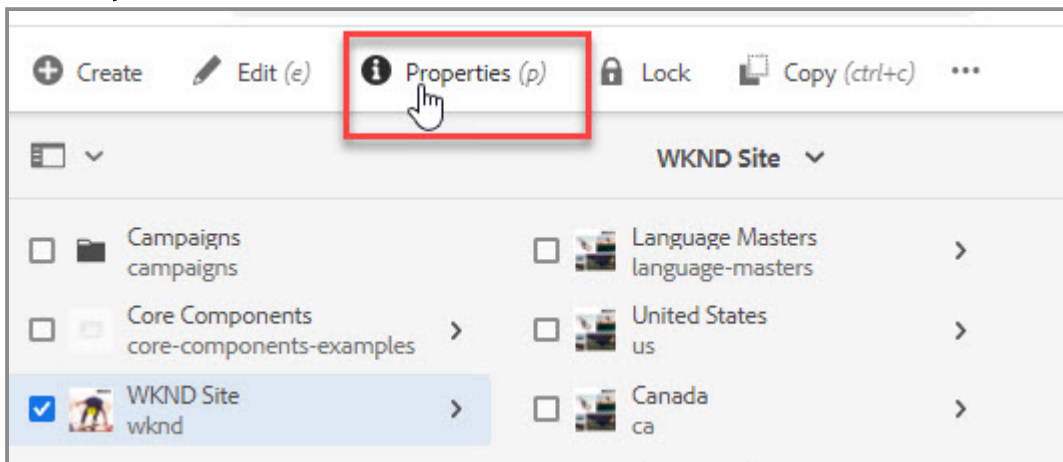
Note: So far, you have created two new users and added your new users to appropriate site groups. Recall that these groups are added to the built-in contributors group in AEM. This ensures these users have the basic authorization to navigate the consoles in AEM. Technically, the contributors group provides read-only access to everything. This allows a user to navigate in AEM but without performing any actions on the repository (such as editing a page).

Next you will give Jane full access to the WKND site so that she can manage permissions for other users. As a best practice you will give full permissions to the Site Managers group rather than the user Jane.

13. Navigate to **Sites > WKND Site** and select **WKND Site**, as shown:

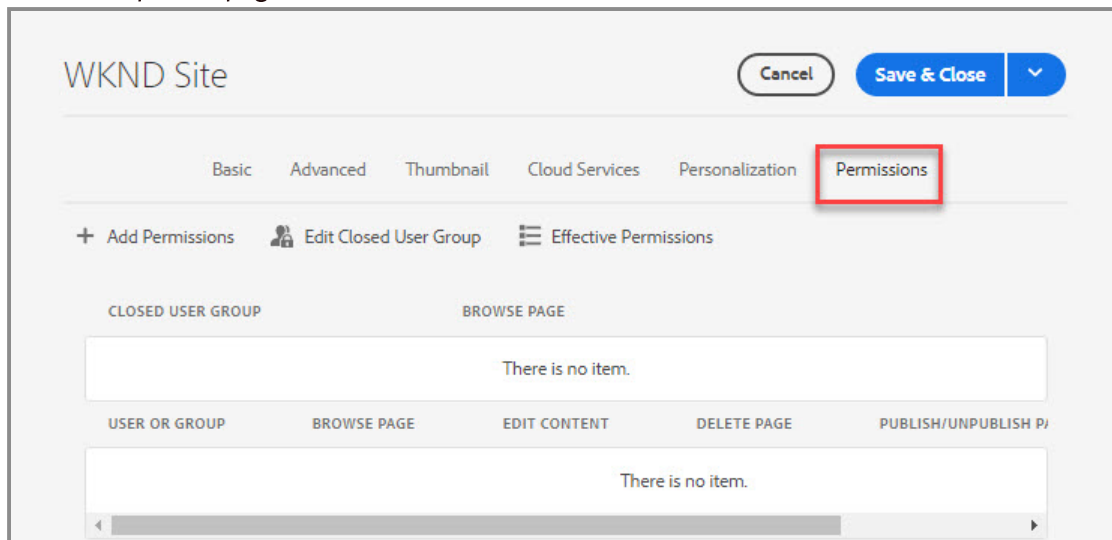


14. Click **Properties** from the actions bar, as shown:



The Configuration Properties page opens.

15. On the Properties page, select the **Permissions** tab, as shown:

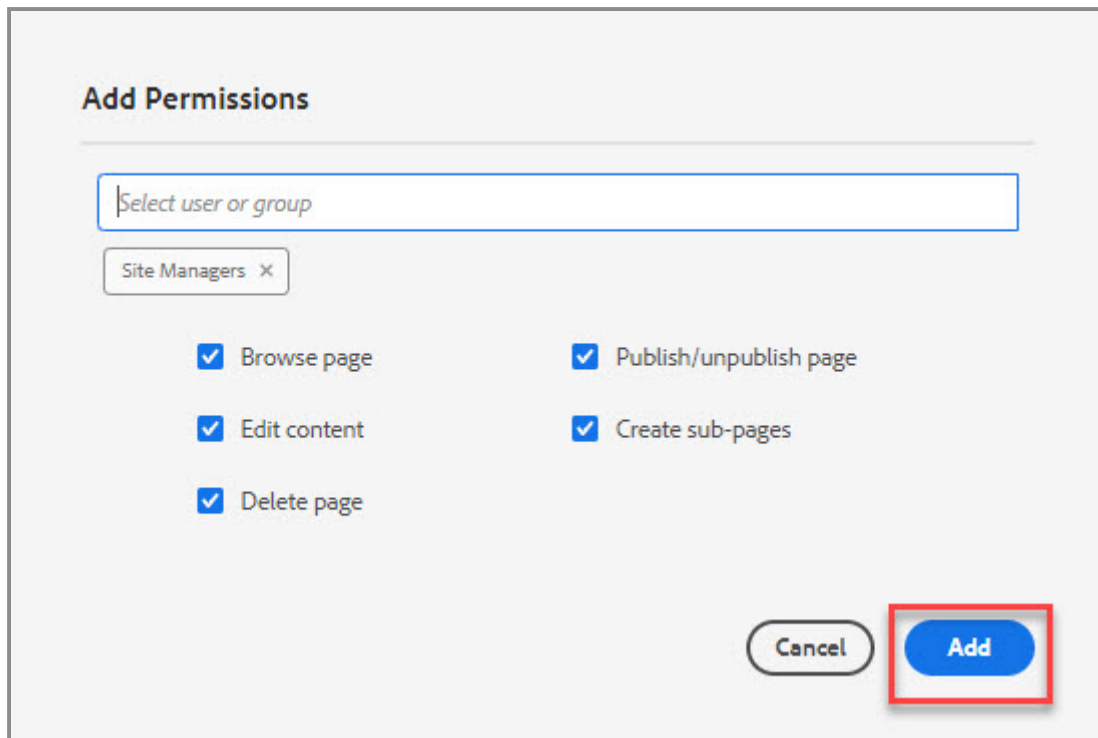


The Permissions page opens.

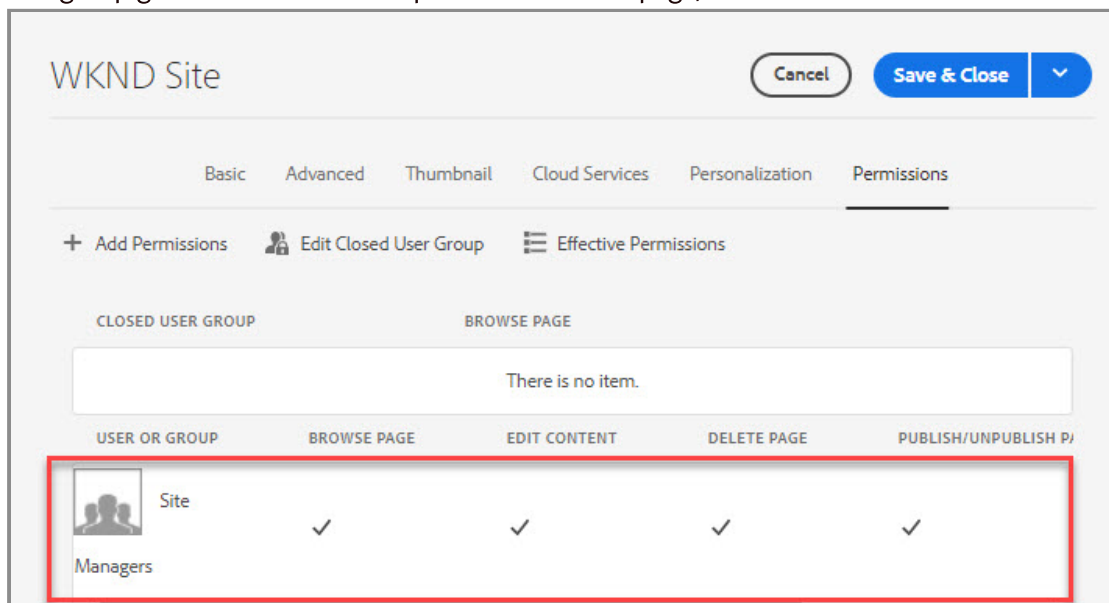
16. Click **Add Permissions**. The **Add Permissions** window opens.

17. Type Site into the **Select User or group** field. This will retrieve the group you created by auto-type in AEM. Select the **Sites Managers** group.

18. Select all Permissions and click **Add**, as shown:



The group gets added with all the permissions to the page, as shown:



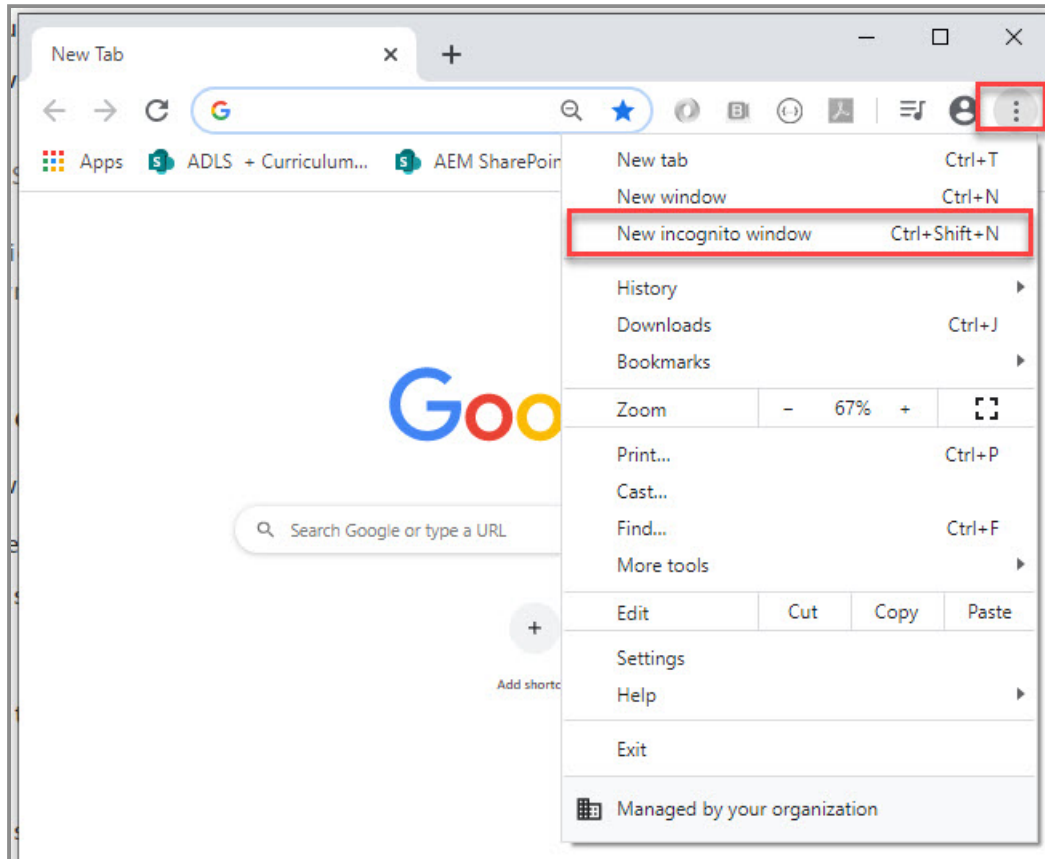
19. Click **Save & Close** at the upper right. A success message displays on the page.

Note: Now the Site Managers group has the access to give permission control to Site Authors. This means, the user Jane Brown will have the permission to browse the website, edit the website or publish pages.

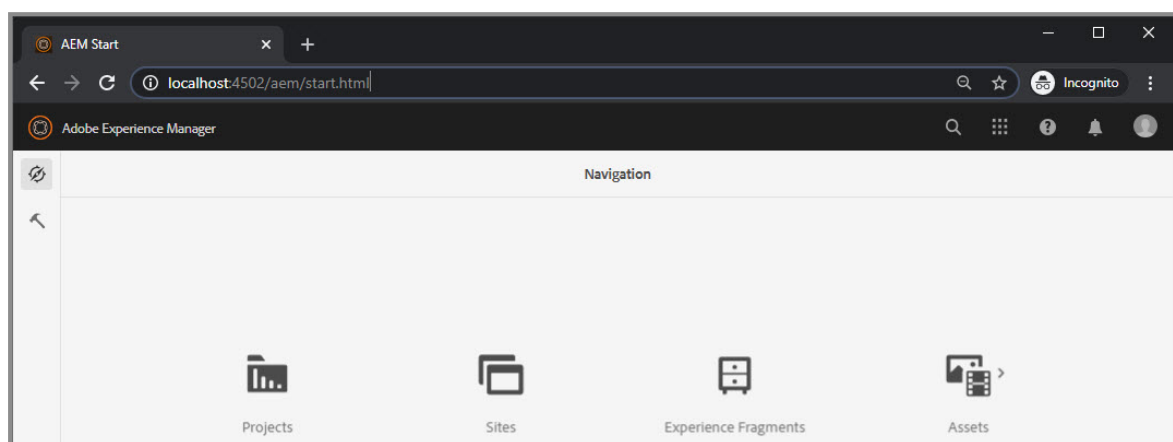
Task 2: Provide Site permissions by using a Site Manager

Open a browser window in Incognito mode.

1. To test the permissions groups, you need to open a new browser session using a different Internet browser or incognito mode which most modern browsers have.

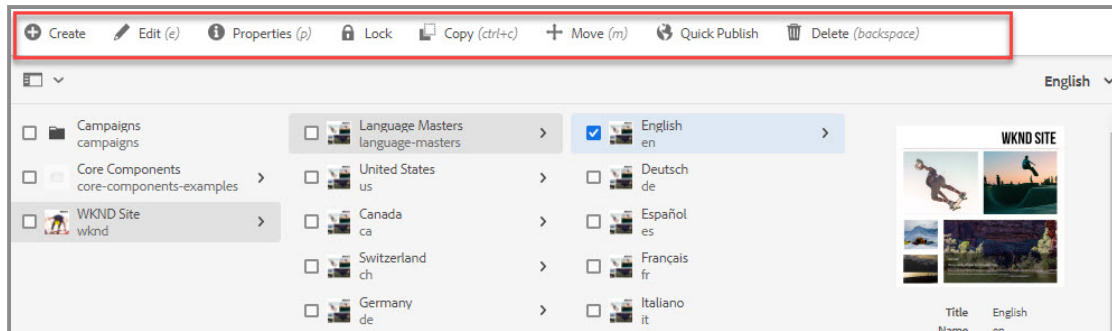


2. On the new browser session, navigate to <http://localhost:4502/aem/start.html>, as shown:



3. Sign in to **AEM** as **jbrown/jbrown**.

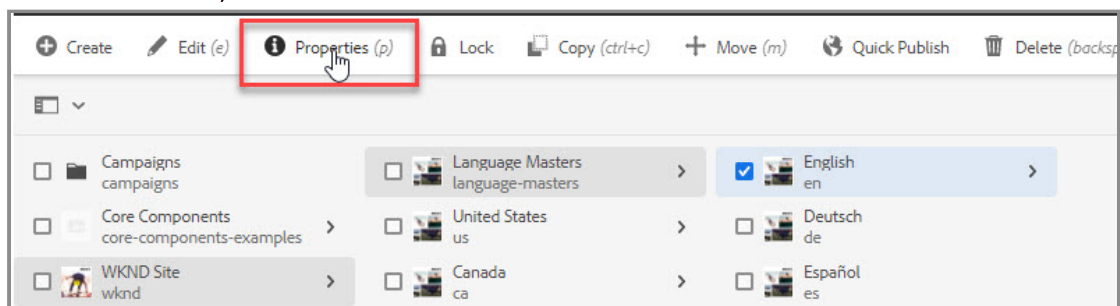
4. Navigate to **Sites > WKND Site > Language Masters** and select **English**, as shown:



Notice the user **jbrown** as a Site Manager has all the basic permissions to the **WKND Site** and its sub-pages.

To provide permissions to Site Authors to edit a webpage:

5. Navigate to **Sites > WKND Site > Language Masters** and select **English** and click **Properties** on the actions bar, as shown:



The **Properties** for English page opens.

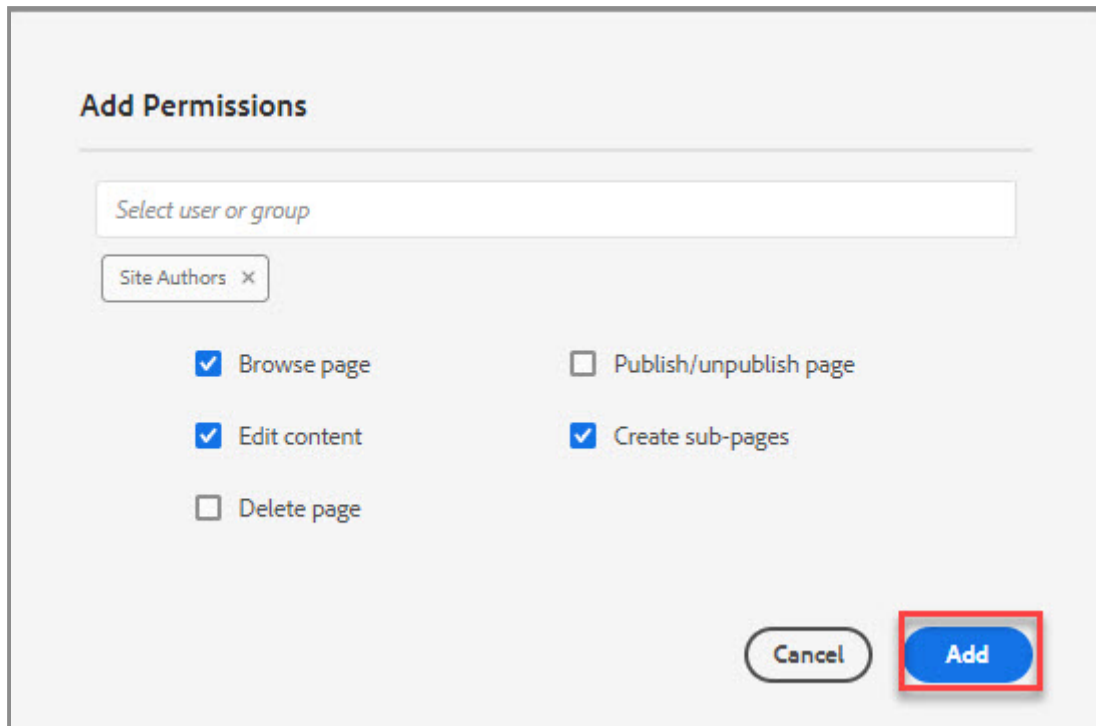
6. On the **Properties** page, select the **Permissions** tab. The Permissions page opens.

7. Click **+Add Permissions**. The **Add Permissions** window opens.

Note: If you do not see **+ Add Permissions**, you need to go back to the **Permissions** console and check the ACEs created for the Site Managers group.

8. Type **Site** into the **Select User or group** field. This will retrieve the group you created by auto-type in AEM. Select the **Sites Authors** group.

9. Select the following Permissions (**Browse Page, Edit Content, Create sub-pages**) and click **Add**, as shown:



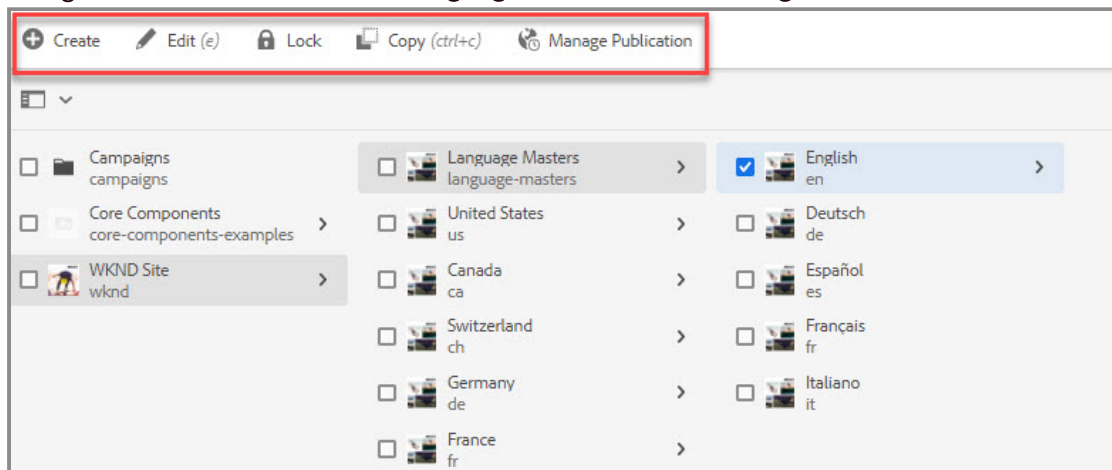
The **Site Authors** group is added to the **Browse Page, Edit Content, Create sub-pages** permissions to the English page.

10. Click **Save & Close** at the upper right. A success message displays on the page.

Note: Now any user that is added to the Site Authors group, will be able to browse, edit and delete the English Page and its sub-pages.

Task3: Author a page as a Site Author user

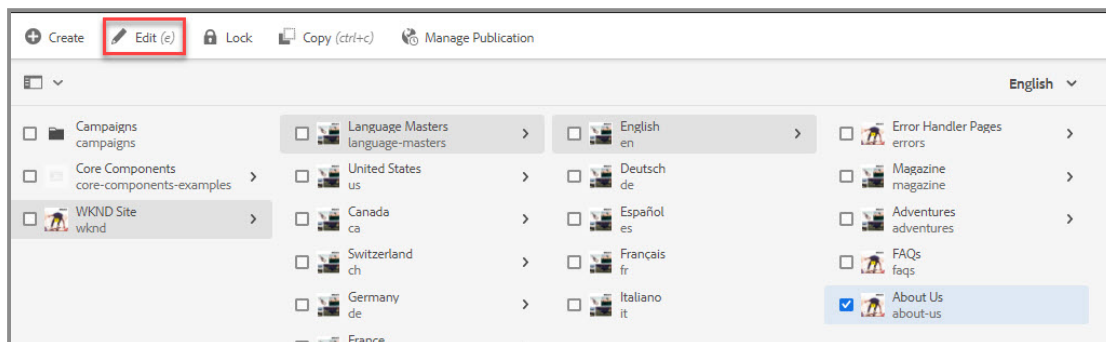
1. In the Incognito window, log out of **Jane Brown** and log on to AEM as **cgrant/cgrant**.
2. Navigate to **Sites > WKND Site > Language Master** and select **English**, as shown:



Notice the user **cgrant** as a Site Author has no permissions to delete or publish the page.

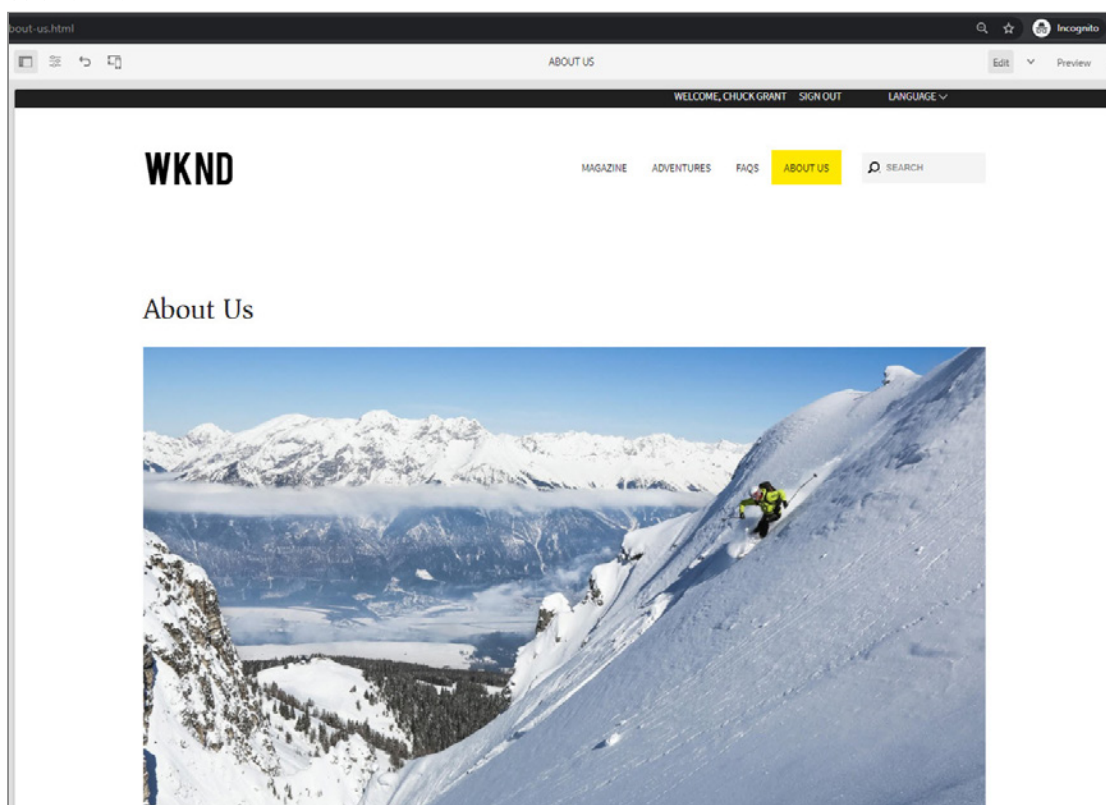
To author a page:

3. Navigate to **Sites > WKND Site > Language Master > English**. Select **About Us** and click **Edit**, as shown:



The page opens in Edit mode.

4. If a Modes dialog box appears, select **Don't show this again** (if not already selected), and click **Close**.
5. Drag Image and Text components onto the page and add an image and content to the page, as shown:



6. Click the Page Information icon and notice Chuck cannot publish the page.
7. Click **Request to Publish**. This will start the **Request to Publish** workflow.

Note: Chuck is able to do the request because he is a part of the workflow-users group.

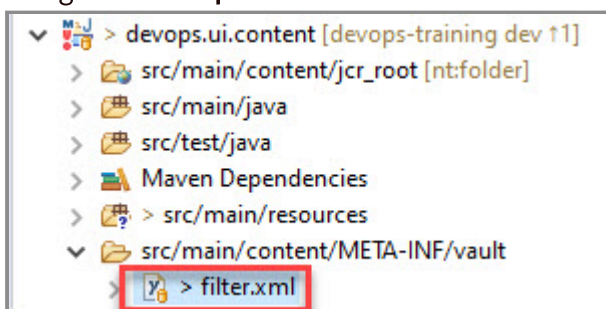
Exercise 4: Sync permission groups to the Maven project

Scenario: In the previous exercise, you set users, groups and permissions within your local AEM instance. Depending on the requirements of your project you need to add the users, groups, or permissions back to your maven project so they can be deployed elsewhere.

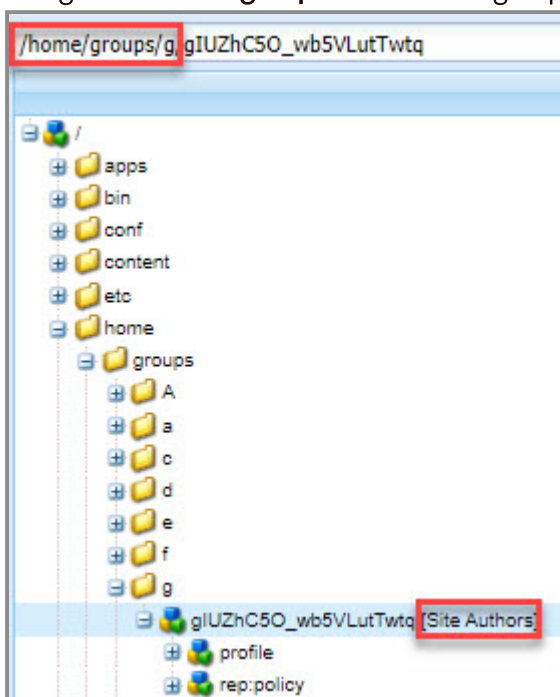
In this exercise you will learn how to find the nodes needed to import them back into your maven project.

To complete this exercise, you need to ensure in Eclipse you have a Server connected to your local AEM instance.

1. Open **Eclipse**.
2. Navigate to: **devops.ui.content > src/main/content/META-INF/vault > filter.xml**, as shown:

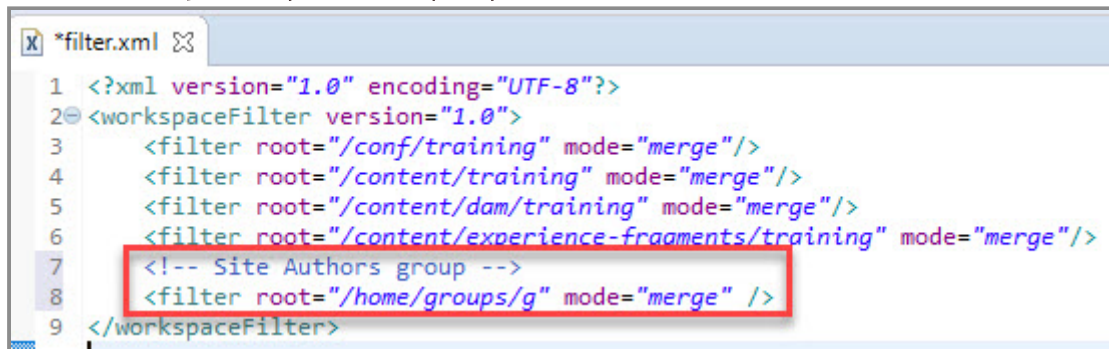


3. Double-click **filter.xml** to open it and view the current filter that will be synchronized with this module.
4. Keep the file open.
5. On the **AEM** browser tab where you have logged as **admin**, go to **CRXDE Lite**.
6. Navigate to **/home/groups/** and find the group **Site Authors**, as shown:



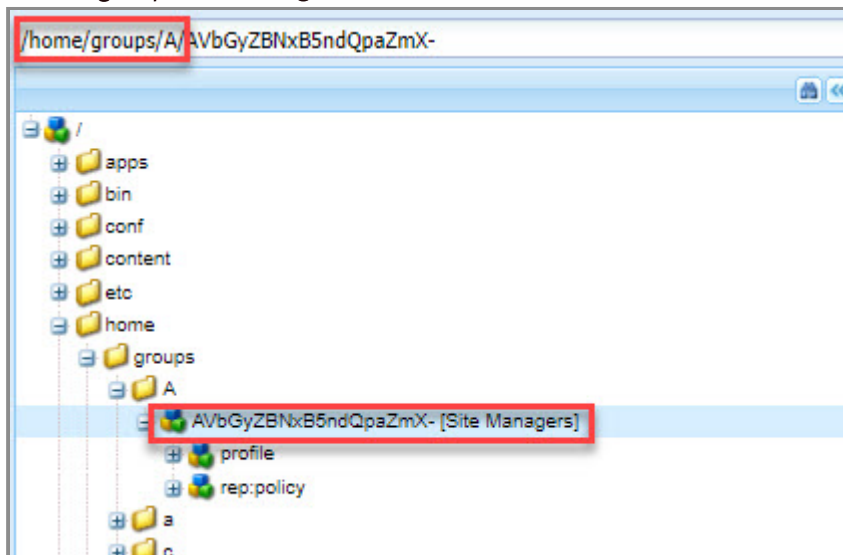
Note: When groups are created, the node name is a hash. More than likely your group node name will not be the same as in the screenshot. Just keep looking in the /home/groups subfolders to find Site Authors.

7. Copy the parent path of the **group** which is **/home/groups/g** (The user node might be different for you).
8. Go back to **Eclipse** and paste the copied path to the **filter.xml**, as shown:



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <workspaceFilter version="1.0">
3   <filter root="/conf/training" mode="merge"/>
4   <filter root="/content/training" mode="merge"/>
5   <filter root="/content/dam/training" mode="merge"/>
6   <filter root="/content/experience-fragments/training" mode="merge"/>
7   <!-- Site Authors group -->
8   <filter root="/home/groups/g" mode="merge" />
9 </workspaceFilter>
```

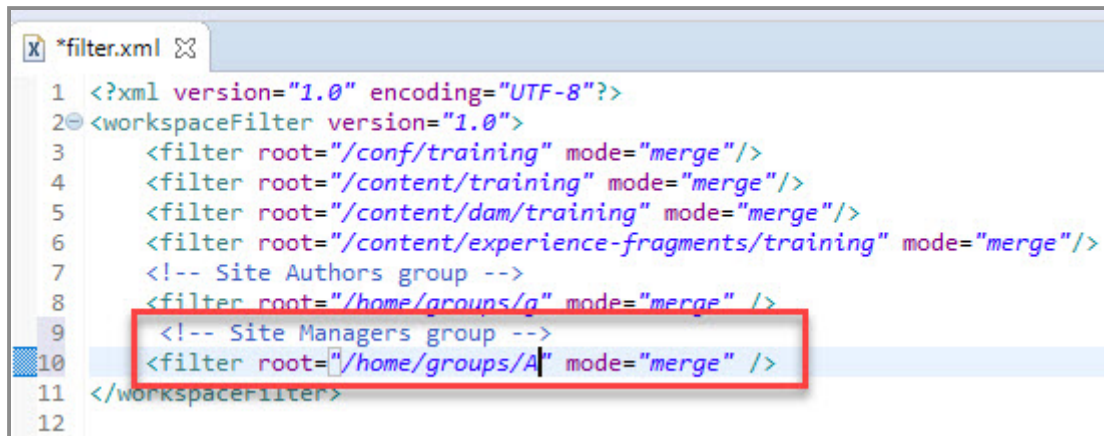
9. Save the changes.
10. Keep the file open.
11. Go to **CRXDE Lite** and navigate to **/home/groups/**.
12. Find the group **Site Managers** , as shown:



13. Copy the parent path of the group which is **/home/groups/A** (The user node might be different for you).

Note: When groups are created, the node name is a hash. More than likely your group node name will not be the same as in the screenshot. Just keep looking in the /home/groups subfolders to find Site Managers.

14. Go back to **Eclipse** and paste the copied path to the **filter.xml**, as shown:



```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <workspaceFilter version="1.0">
3   <filter root="/conf/training" mode="merge"/>
4   <filter root="/content/training" mode="merge"/>
5   <filter root="/content/dam/training" mode="merge"/>
6   <filter root="/content/experience-fragments/training" mode="merge"/>
7   <!-- Site Authors group -->
8   <filter root="/home/groups/g" mode="merge" />
9   <!-- Site Managers group -->
10  <filter root="/home/groups/A" mode="merge" />
11 </workspaceFilter>
12
```

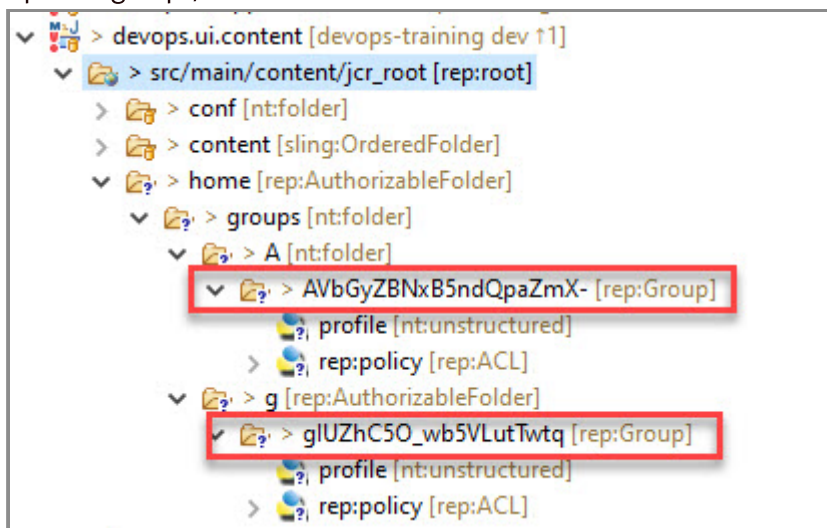
15. Save the changes.

16. Right-click **devops.ui.content** > **src/main/content/jcr_root** and select **Import from server**.

17. Click **Finish**.

Note: If you had any changes in AEM (based on filter.xml), those nodes and properties are now imported to your project.

18. In **Eclipse**, navigate to **devops.ui.content** > **src/main/content/jcr_root** > **home** and verify the imported groups, as shown:



You have successfully synced the permission groups to the Maven project.

References

1. IMS: <https://docs.adobe.com/content/help/en/experience-manager-cloud-service/security/ims-support.html> ↵
2. Role based Permissions: <https://docs.adobe.com/content/help/en/experience-manager-cloud-manager/using/requirements/role-based-permissions.html> ↵
3. JSR: <https://jcp.org/en/jsr/detail?id=283> ↵
4. JCR: <https://docs.adobe.com/docs/en/spec/jcr/2.0/index.html> ↵