

Permissions Required for UPA Tasks

Reference for roles and delegation

PRODUCT

Universal Policy Administrator 3.6

UPDATED

September 2026

AUDIENCE

UPA administrators who set up roles and delegation

This reference lists every permission in Universal Policy Administrator (UPA) and the permissions each task in the console needs. Use it to build roles that give each team exactly what it needs, and nothing more.

1. How UPA permissions work

Access in UPA is built from three parts, all set up under **Administration**:

Part	Answers	Example
Role	What someone can do: a set of permissions	"Editor": create and edit policies, submit them for approval
View	Where they can do it: which OUs and policies	"Global" (everything), or one Delegation OU
Assignment	Who: links a role and one or more views to users or groups	"Global Editors" = Editor role + Global view + the editors group

A user's permissions are the combination of every assignment they are part of. A permission applies only to the objects inside the views of the assignment that grants it.

Roles hold the permissions, arranged as a tree:

**Roles**
Define which actions can be performed

**Views**
Define which things can be seen

**Assignments**
Define who can perform which actions on which things

ROLES
ALL ROLES (4)

New

Edit

Delete

Refresh

Role

 Approver

 Editor

 Full Administrator

 Reviewer

EDITOR
ROLE DETAILS

Role Configuration

 Notifications(0)

Role Permissions

 Full Control

 Full Domain Control

☐ Create New Domain

☐ Delete Domain

☒ Edit Domain Maps

☐ Export To AD

☒ Import From AD

☒ Replicate

☒ View OU

☒ View UP

☒ Audit

☒ View GPO

☐ Modify GPO

☐ Create GPO

 Full OU Control

☒ Create OU

☒ Delete OU

☒ Rename OU

☒ View OU

☒ Audit

 Full UP Control

☐ Approve UP

☒ Submit UP For Approval

☒ Create UP

☒ Delete UP

☒ Modify UP

☒ Modify UP Links

☒ Undo Checkout

☒ Rename UP

☒ Rollback

☒ View UP

☒ Audit

 Full AD Control

☒ View AD

☐ Modify AD

☐ Delete AD

 Full GPO Control

☒ View GPO

☐ Modify GPO

☐ Delete GPO

☐ Create GPO

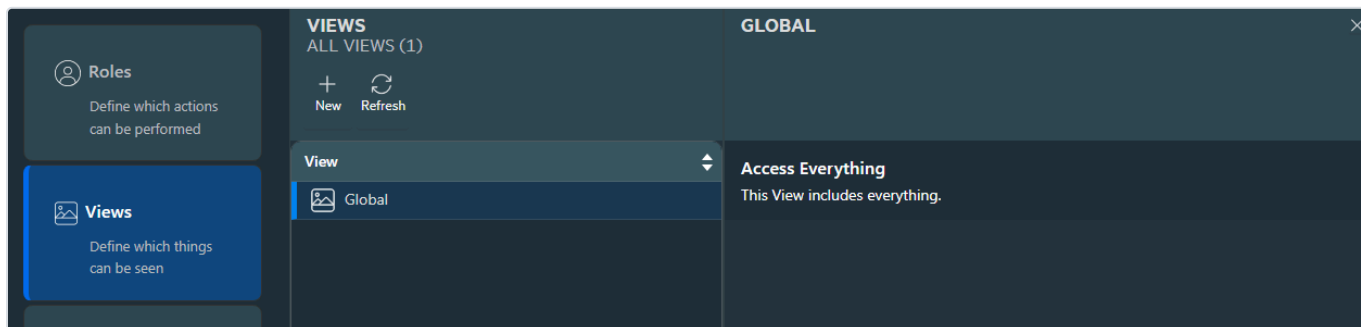
 Full Delegation Control

Universal Policy Administrator

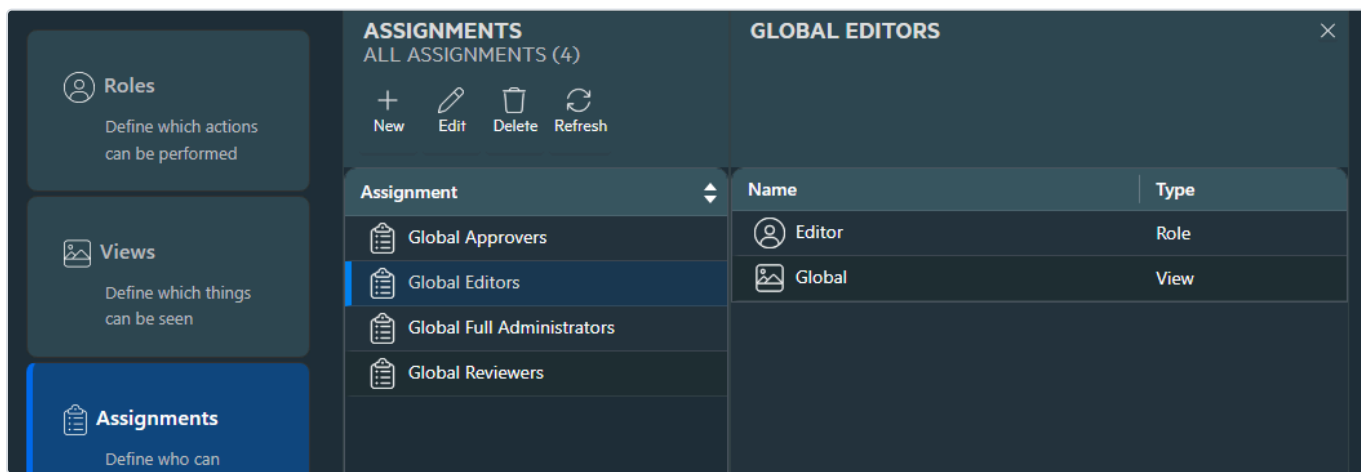
2 of 8

FULLARMOR

Views decide which objects the permissions apply to:



Assignments give a role and view to users or groups:



How the permission tree works

- Ticking a branch, such as **Full UP Control**, ticks every permission under it.
- Most permissions automatically include the matching **View** permission. For example, **Modify UP** includes **View UP**, and **Export To AD** includes **View UP** and **View GPO**.
- Some permissions appear in more than one branch, such as **View OU** and **Audit**. Ticking one copy ticks them all.
- After changing a role, click **Save** in the role panel. Changes that are not saved are lost when you leave the page.

2. Built-in roles

UPA comes with four roles. You can use them as they are, or copy their permissions into your own roles.

Permission	Full Administrator	Approver	Editor	Reviewer
View OU, View UP, View AD, View GPO, View Delegation, Audit	✓	✓	✓	✓
Create OU, Delete OU, Rename OU	✓	✓	✓	
Create UP, Modify UP, Delete UP, Rename UP, Undo Checkout, Rollback, Modify UP Links	✓	✓	✓	
Submit UP For Approval	✓	✓	✓	

Permission	Full Administrator	Approver	Editor	Reviewer
Import From AD, Replicate, Edit Domain Maps	✓	✓	✓	
Approve UP	✓	✓		
Export To AD, Create GPO, Modify GPO, Delete GPO	✓	✓		
Create New Domain	✓			
Modify Delegation	✓			
Modify AD, Delete AD	✓			

The key differences:

- **Editors** can build and submit policies, but cannot approve them or write them to Active Directory.
- **Approvers** can also approve policies and export them to Active Directory.
- **Reviewers** can only view policies and read the audit trail.
- **Full Administrators** can do everything, including managing domains and delegation.

3. Every permission

This table follows the role editor's tree exactly, branch by branch. Several permissions appear in more than one branch, for example **View OU**, **View GPO** and **Audit**. Each branch lists all of its permissions, so a permission can appear more than once. It is still one permission: ticking it in one branch ticks it everywhere.

Branch	Permission	Allows
Full Domain Control	Create New Domain	Import or re-import a domain, and set its domain credentials
	Delete Domain	Not yet supported. Reserved for a future release.
	Edit Domain Maps	Change domain mappings (PowerShell only)
	Export To AD	Write a policy to its GPO in Active Directory
	Import From AD	Import GPOs and OUs from Active Directory, as a new policy or during a domain import
	Replicate	Copy a policy to another domain
	View OU	See Cloud OUs, Repository OUs and Delegation OUs
	View UP	See policies, their settings and their reports
	Audit	See the Auditing tab, and events recorded by other users
	View GPO	See GPOs in Active Directory
	Modify GPO	Change GPOs directly (PowerShell only)
	Create GPO	Create a new GPO in Active Directory when exporting
Full OU Control	Create OU	Create Cloud OUs and Delegation OUs, and import OUs from Active Directory
	Delete OU	Remove Cloud, Delegation and Repository OUs

Branch	Permission	Allows
	Rename OU	Rename Cloud OUs and Delegation OUs
	View OU	See Cloud OUs, Repository OUs and Delegation OUs
	Audit	See the Auditing tab, and events recorded by other users
Full UP Control	Approve UP	Approve or reject a policy that is waiting for approval
	Submit UP For Approval	Submit a checked-in policy for approval
	Create UP	Create a new policy
	Delete UP	Delete a policy
	Modify UP	Check out, edit, check in, merge, synchronize, and change security filtering
	Modify UP Links	Link policies to OUs, and change link order
	Undo Checkout	Revert a checkout, discarding the changes
	Rename UP	Rename a policy
	Rollback	Return a policy to an earlier version
	View UP	See policies, their settings and their reports
	Audit	See the Auditing tab, and events recorded by other users
Full AD Control	View AD	Browse users, groups and GPOs in Active Directory (needed to pick them in dialogs)
	Modify AD	Change Active Directory objects (PowerShell only)
	Delete AD	Delete Active Directory objects (PowerShell only)
Full GPO Control	View GPO	See GPOs in Active Directory
	Modify GPO	Change GPOs directly (PowerShell only)
	Delete GPO	Delete GPOs (PowerShell only)
	Create GPO	Create a new GPO in Active Directory when exporting
Full Delegation Control	View Delegation	See roles, views, assignments and notification settings
	Modify Delegation	Create, change and delete roles, views and assignments, and configure notifications

PowerShell only: these permissions control actions that are available through the UPA PowerShell cmdlets. They do not change anything in the console.

4. Permissions by task

Administration tab

Task	Permissions needed
See roles, views, assignments and notification settings	View Delegation
Create, edit or delete a role	Modify Delegation
Create or edit a view	Modify Delegation, plus View OU and View UP to see the objects to add
Delete a view	Modify Delegation
Create, edit or delete an assignment	Modify Delegation, plus View AD to find the users and groups to add
Configure notifications for a role	Modify Delegation

Organization tab

Task	Permissions needed
See the OU tree	View OU
Import a domain, or re-import it	Create New Domain, Create OU, Import From AD, View AD, View OU
Set the domain credentials	Create New Domain
See the import history	No extra permission
Create a Cloud OU or a Delegation OU	Create OU
Rename a Cloud OU or a Delegation OU	Rename OU
Remove a Cloud, Delegation or Repository OU	Delete OU
Link or unlink policies to an OU, or change the link order	Modify UP Links
Edit domain mappings	Edit Domain Maps (PowerShell only)

Universal Policies tab

UPA

ADMINISTRATION

ORGANIZATION

UNIVERSAL POLICIES

AUDITING

ABOUT

UNIVERSAL POLICIES (1)

WINDOWS

+

New

🗑

Delete

🛡

Replicate

🔄

Refresh

Default Domain Policy

✕

🔍

🏠

Universal Policy

⬆⬆

Status

⬆⬆

🛡

Default Domain Policy

✓

GPO: Default Domain Policy

contoso.com

Checked In (v1 r0)

UPA Admin

Sep 28 2026

DEFULT DOMAIN POLICY

✕

RELEASE 0, VERSION 1 CHECKED IN

📄

Checkout

➡

Submit for Approval

🔄

Merge

PLATFORMS

📱

Windows Group Policy

📋

Policies (10)

⚙

Preferences

ACTIONS

📤

Export to Active Directory

(Available after release 1)

DETAILS

🔗

Linked OUs (0)

🛡

Synchronization

⚡

Events

Task	Permissions needed
See policies and their settings	View UP
Create a new (blank) policy	Create UP. The view decides whether it is global, per domain, or in a Delegation OU.
Create a new policy from a GPO	Create UP, Import From AD
Create a new policy with a WMI filter	Create UP (or Import From AD), View GPO
Check out, edit settings, check in	Modify UP
Add administrative templates (Manage Policy Templates)	Modify UP, on a checked-out policy
Revert a checkout (discard the changes)	Undo Checkout
Roll back to an earlier version	Rollback

Task	Permissions needed
Submit for approval	Submit UP For Approval. The policy must be checked in, with no duplicate settings.
Approve or reject	Approve UP
Rename	Rename UP
Delete	Delete UP
Replicate to another domain	Replicate, Create UP, Modify UP, View AD, View GPO
Merge into other policies	Modify UP
Link to OUs	Modify UP Links
Export to Active Directory (existing GPO)	Export To AD
Export to Active Directory (new GPO)	Export To AD, Create GPO
Update synchronization targets, or synchronize now	Modify UP
Change security filtering	Modify UP, plus View AD to find the users and groups
Reports: Settings, Differences, Conflicts, Export history	View UP
Events	View UP. Seeing events recorded by other users also needs Audit.

Auditing tab

Task	Permissions needed
See the Auditing tab and audit events	Audit

5. Example: an Editor for one team

To let a team build policies only for its own Delegation OU, without approving or deploying them:

1. **Role:** tick **View OU, View UP, Create UP, Modify UP, Undo Checkout, Submit UP For Approval** and **View AD**. Leave **Approve UP** and **Export To AD** clear. Click **Save**.
2. **View:** add the team's Delegation OU.
3. **Assignment:** combine the role and the view, and add the team's group.

The team can then create, edit and submit policies in their OU. An Approver approves them, and someone with **Export To AD** deploys them.

For help, contact your Full Armor representative or email support@fullarmor.com.