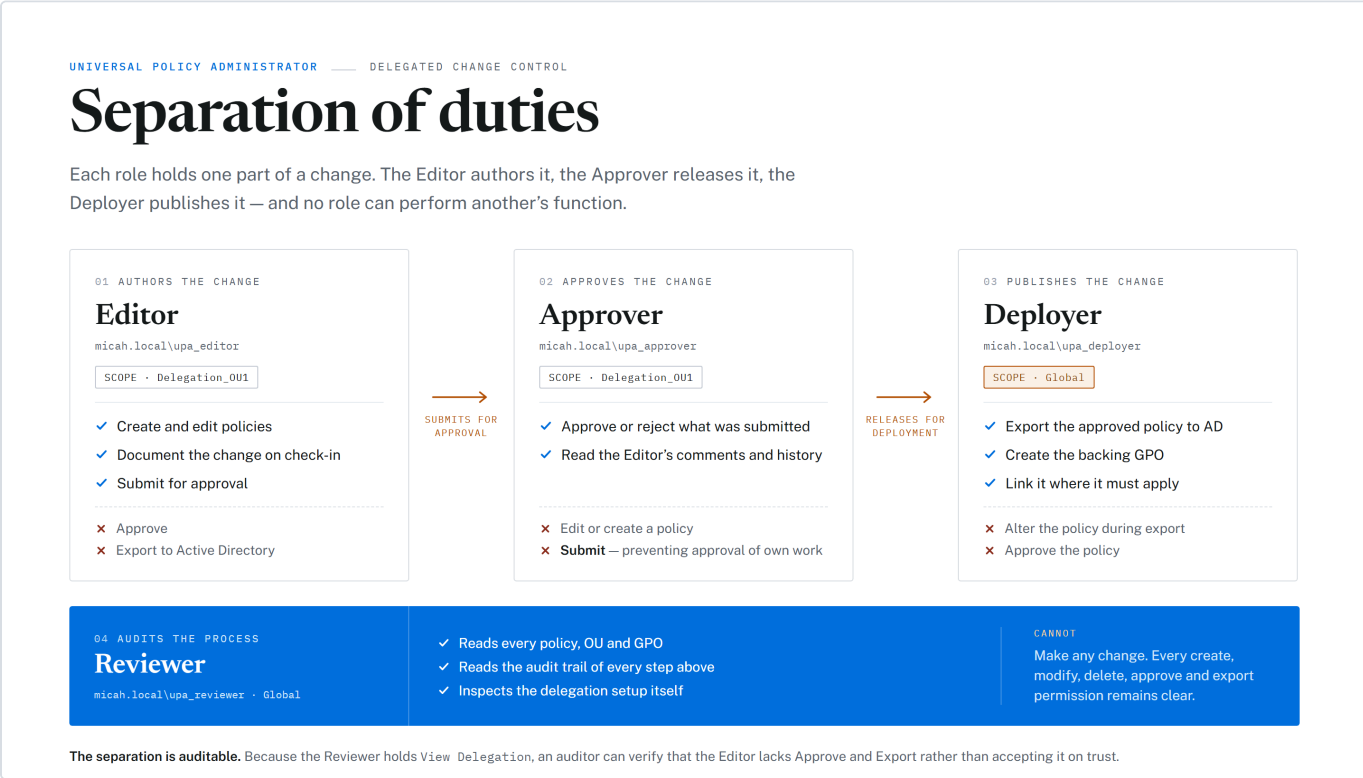


Delegated Administration and Change Approval

Universal Policy Administrator — Delegation Guide

This guide sets up four people who each own one step of a policy change. The Editor writes it, the Approver signs it off, the Deployer publishes it to Active Directory, and the Reviewer can read everything but change nothing. Nobody does two of those jobs, and that separation of duties means every change passes through more than one pair of hands before it reaches a workstation. The Editor and the Approver only see the policies you put in a Delegation OU, so a team can work on its own policies without touching anyone else's.

It also gives you a clean answer when an auditor asks who changed what. UPA records each change against the account that made it and each approval against a different account, and keeps the history of both. The Reviewer can open the delegation setup and show that the Editor really has no rights to approve or export — the part most auditors would rather see for themselves than take your word for. If you need to demonstrate documented, independently reviewed change control, this covers it.



production is what the Approver signed off, unchanged.

The Reviewer answers "who changed what, and when", reading every policy, OU and GPO in the policy environment together with the full audit trail, and changing nothing. **View Delegation** lets them inspect the delegation itself, so an auditor can verify the Editor's limits rather than take them on trust.

The Editor and Approver are scoped to one Delegation OU; the Deployer and Reviewer are global, for reasons given in Steps 10 and 11. Step 12 sets the whole boundary out as a grid.

Scope and conventions

A **Delegation OU** is a container created inside UPA to group the policies one team may work on. It is what the Editor's and Approver's Views point at, and creating one changes nothing in Active Directory; Step 1 covers how.

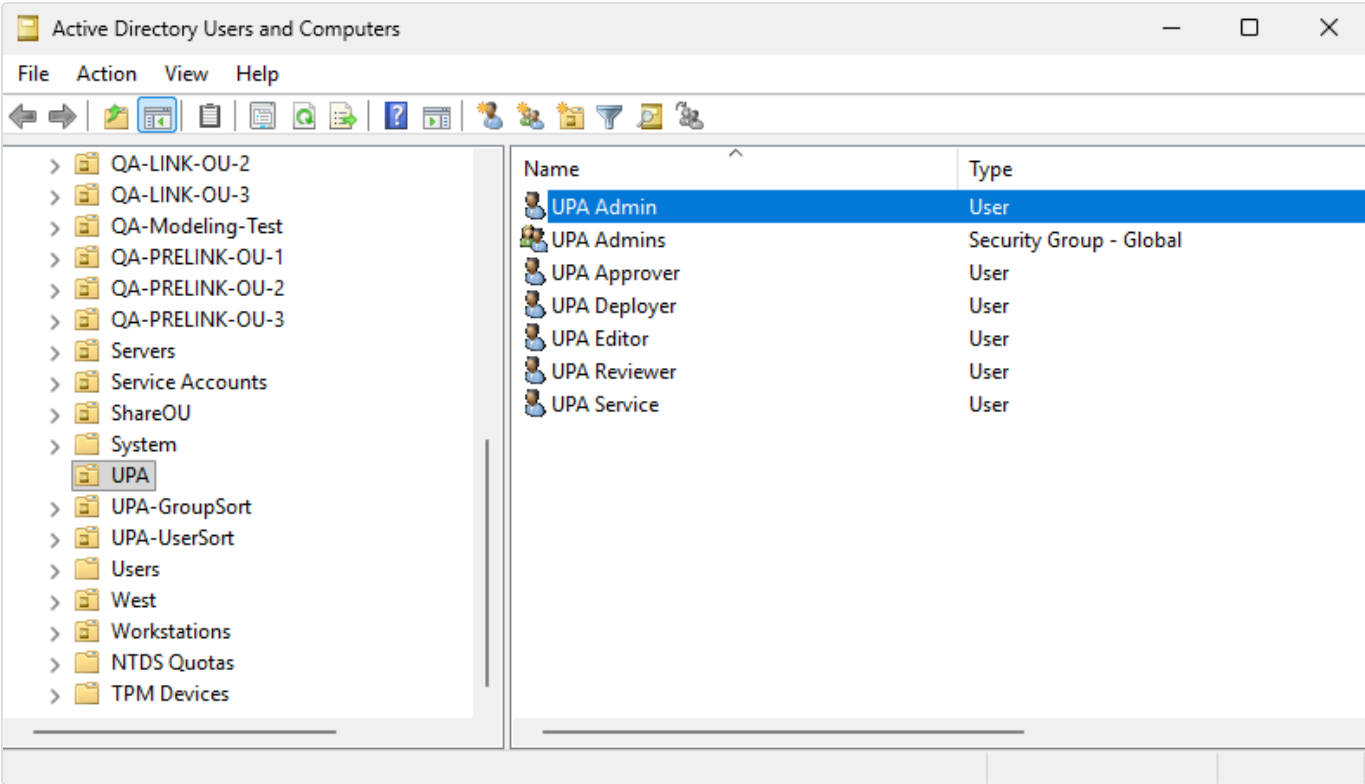
The worked example uses a Delegation OU named **Delegation_OU1** on the domain `micah.local` — substitute your own names as you go. You will work in two tabs: **Organization** to create the Delegation OU and link policies into it, and **Administration** to build the Roles, Views and Assignments.

Before you begin

- Sign in to UPA with an account that has **Full Administrator** rights.
- Allow about forty minutes for all four roles, or fifteen for the Editor alone.

These are ordinary Active Directory accounts

UPA does not create users. Each role is assigned to a domain account that already exists in Active Directory — here they are grouped in a `UPA` organizational unit:



Account	Used for
micah.local\upa_editor	the Editor
micah.local\upa_approver	the Approver
micah.local\upa_deployer	the Deployer
micah.local\upa_reviewer	the Reviewer
micah.local\upa_admin	the UPA administrator doing this setup
micah.local\upa_service	the service account UPA uses to read and write Active Directory

Create these accounts in Active Directory first, however your organisation normally does. Nothing in this guide changes them — UPA only references them by name when you build an Assignment.

The three pieces you will create in Administration

Piece	Sets	Created in
Role	which actions can be performed	Administration → Roles
View	which things can be seen	Administration → Views
Assignment	who can do which actions on which things	Administration → Assignments

A Role alone grants nothing and a View alone shows nothing — the Assignment joins them to a person.

The thirteen steps

Steps	What they cover
1	Create the Delegation OU
2 – 7	The Editor — two Roles, two Views, two Assignments
8	Link Universal Policies into the Delegation OU
9 – 11	The Approver, the Deployer and the Reviewer
12 – 13	How a change flows, and verifying the result

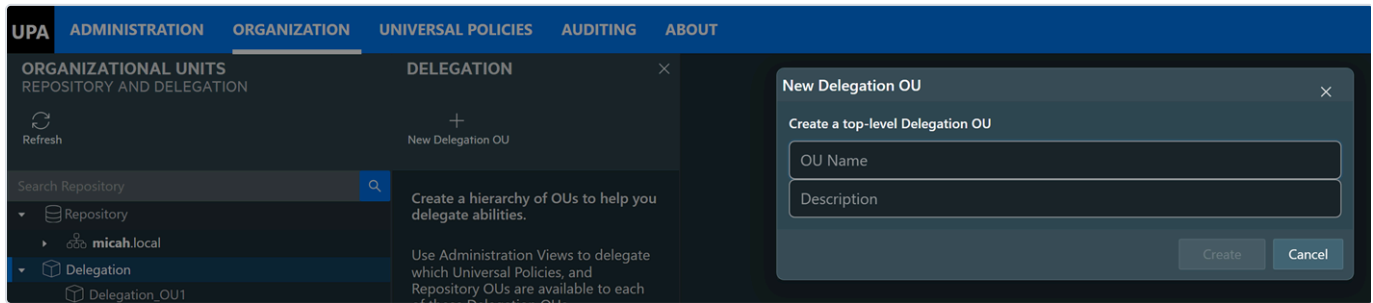
If you only need the scoped Editor, stop after Step 8 — that part is complete on its own, and Steps 9 to 11 are three independent roles you can add later in any order.

Step 1 — Create the Delegation OU

Create the container the Editor and Approver will be scoped to. It does not need a counterpart in Active Directory.

1. Go to the **Organization** tab.
2. In the tree on the left, select **Delegation**.
3. Click **New Delegation OU**.
4. Enter an **OU Name** — `Delegation_OU1` in this example — and optionally a **Description**.

5. Click **Create**.



The new OU appears under **Delegation** in the tree. Leave it empty for now; policies go in at Step 8.

The tree separates **Repository** — your real Active Directory structure — from **Delegation**, which is this grouping layer. Creating a Delegation OU changes nothing in Active Directory.

Step 2 — Editor: create the Role

1. Go to **Administration** → **Roles** and click **New**.
2. Name the role **Editor - View, Edit, and Create UPs**.
3. Tick the permissions listed below, and nothing else.
4. Click **Save**.

Under Full Domain Control

Tick **View OU** and **View UP** only. **Leave Export To AD clear** — this is what prevents the Editor publishing to Active Directory.

UPA

ADMINISTRATION

ORGANIZATION

UNIVERSAL POLICIES

AUDITING

ABOUT

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 (7)

New

Edit

Delete

Refresh

Role

Approver

Approver - Approve only

Editor

Editor - Create UPs

Editor - View, Edit, and Create UPs

Full Administrator

Reviewer

EDITOR - VIEW, EDIT, AND CREAT... X

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

Under Full OU Control

Tick **View OU**. Leave everything else clear.

Under Full UP Control

Tick the working set, and **leave Approve UP clear**.

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

Universal Policy Administrator

5 of 23

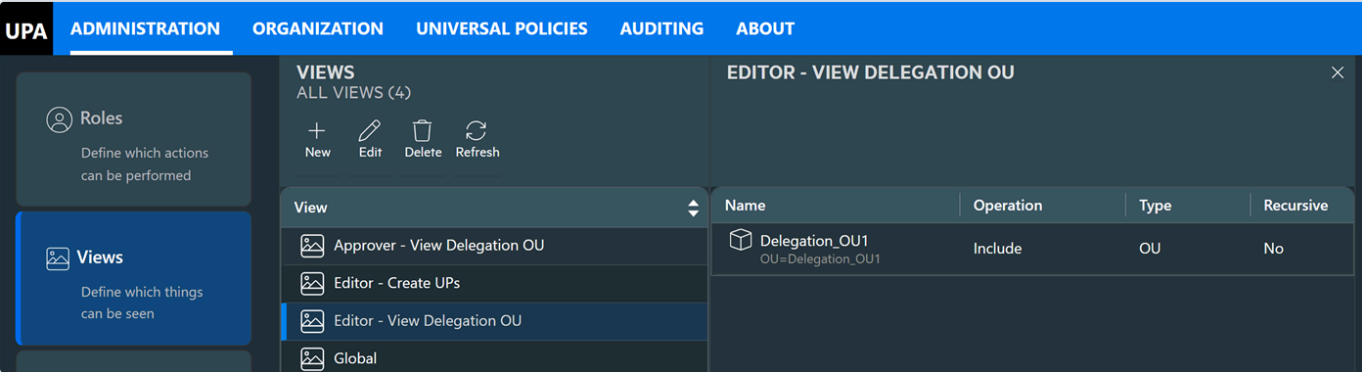
FULLARMOR

Permission	Set to	Gives the Editor
Approve UP	Clear	nothing — this is what stops them releasing their own work
Submit UP For Approval	Ticked	the ability to hand a policy to an Approver
Create UP	Ticked	the ability to create new policies
Modify UP	Ticked	the ability to change settings
Modify UP Links	Ticked	the ability to manage the policy's links
Undo Checkout	Ticked	the ability to abandon their own checkout
Rollback	Ticked	the ability to return to an earlier version
View UP	Ticked	the ability to see the policy
Delete UP	Clear	optional — leave clear to prevent removal
Rename UP	Clear	optional

Leave **Full AD Control**, **Full GPO Control**, **Full Agent Control** and **Full Delegation Control** entirely clear.

Step 3 — Editor: create the View

- 1. Go to **Administration** → **Views** and click **New**.
- 2. Name the view **Editor - View Delegation OU**.
- 3. Add one rule pointing at the Delegation OU you created in Step 1.
- 4. Click **Save**.

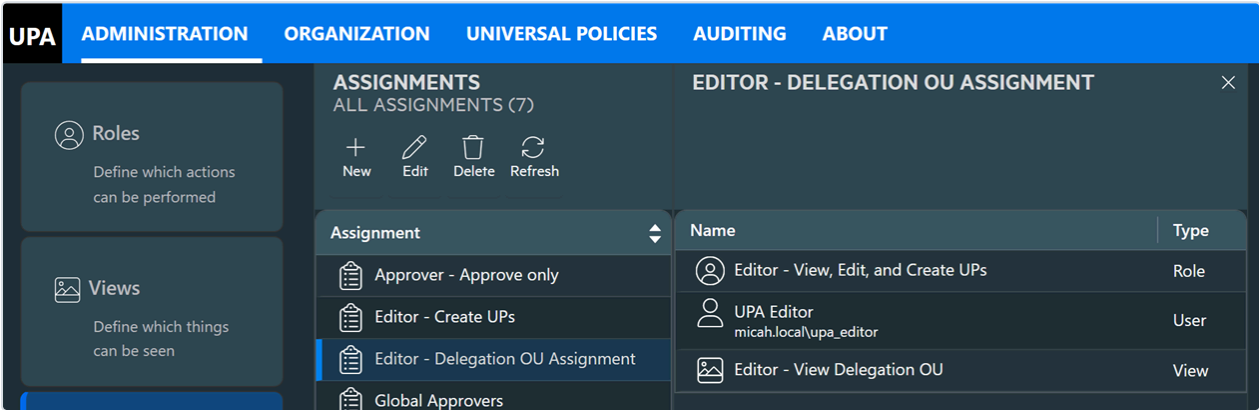


Field	Set to
Name	Delegation_OU1 (OU=Delegation_OU1)
Operation	Include
Type	OU
Recursive	No

Set **Recursive** to **Yes** only if the Editor should also see policies in OUs nested beneath this one.

Step 4 — Editor: create the Assignment

- 1. Go to **Administration** → **Assignments** and click **New**.
- 2. Name it **Editor - Delegation OU Assignment**.
- 3. Add the Role, the user, and the View, so the assignment holds all three.
- 4. Click **Save**.



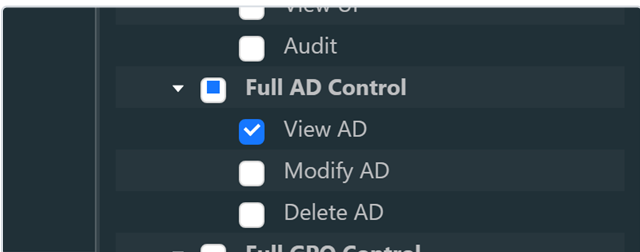
Add	Type
Editor - View, Edit, and Create UPs	Role
micah.local\upa_editor	User
Editor - View Delegation OU	View

To add more Editors later, add them to this same assignment rather than creating a new one.

Step 5 — Editor: allow new policies

An Editor scoped to only the Delegation OU cannot create a policy, because creating one requires being able to see the directory it is created against. Grant that — and nothing else — with a second, deliberately tiny set.

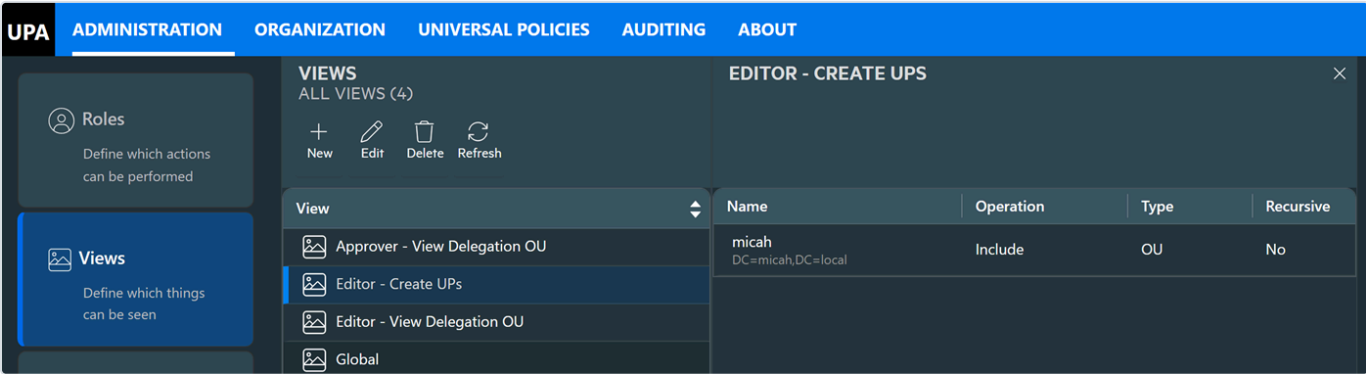
- 1. Go to **Administration** → **Roles** and click **New**.
- 2. Name the role **Editor - Create UPs**.
- 3. Under **Full AD Control**, tick **View AD**. Tick nothing else anywhere in the role.
- 4. Click **Save**.



This grants visibility of Active Directory only — no ability to modify, delete or export anything.

Step 6 — Editor: the View for that Role

- 1. Go to **Administration** → **Views** and click **New**.
- 2. Name the view **Editor - Create UPs**.
- 3. Add one rule pointing at the domain.
- 4. Click **Save**.



Field	Set to
Name	micah (DC=micah,DC=local)
Operation	Include
Type	OU
Recursive	No

Step 7 — Editor: the second Assignment

- 1. Go to **Administration** → **Assignments** and click **New**.
- 2. Name it **Editor - Create UPs**.
- 3. Add the Role, the same user, and the View.
- 4. Click **Save**.

UPA

ADMINISTRATION

ORGANIZATION

UNIVERSAL POLICIES

AUDITING

ABOUT

Roles

Define which actions can be performed

Views

Define which things can be seen

ASSIGNMENTS

ALL ASSIGNMENTS (7)

New

Edit

Delete

Refresh

Assignment

Approver - Approve only

Editor - Create UPs

Editor - Delegation OU Assignment

Global Approvers

EDITOR - CREATE UPS

Name	Type
Editor - Create UPs	Role
UPA Editor micah.local\upa_editor	User
Editor - Create UPs	View

Add	Type
Editor - Create UPs	Role
micah.local\upa_editor	User
Editor - Create UPs	View

Step 8 — Link Universal Policies into the Delegation OU

Existing policies do not move into the Delegation OU on their own. Link the ones this Editor should work on.

Open the dialog

1. Go to the **Organization** tab.
2. Under **Delegation**, select your Delegation OU. The toolbar shows **New**, **Rename**, **Delete** and **UPs**.
3. Click **UPs**.

UPA

ADMINISTRATION

ORGANIZATION

UNIVERSAL POLICIES

AUDITING

ABOUT

ORGANIZATIONAL UNITS

REPOSITORY AND DELEGATION

Refresh

Search Repository

Repository

micah.local

Delegation

Delegation_OU1

DELEGATION_OU1

RESTORED BY IMPORT-UPA-ADMIN...

New

Rename

Delete

UPs

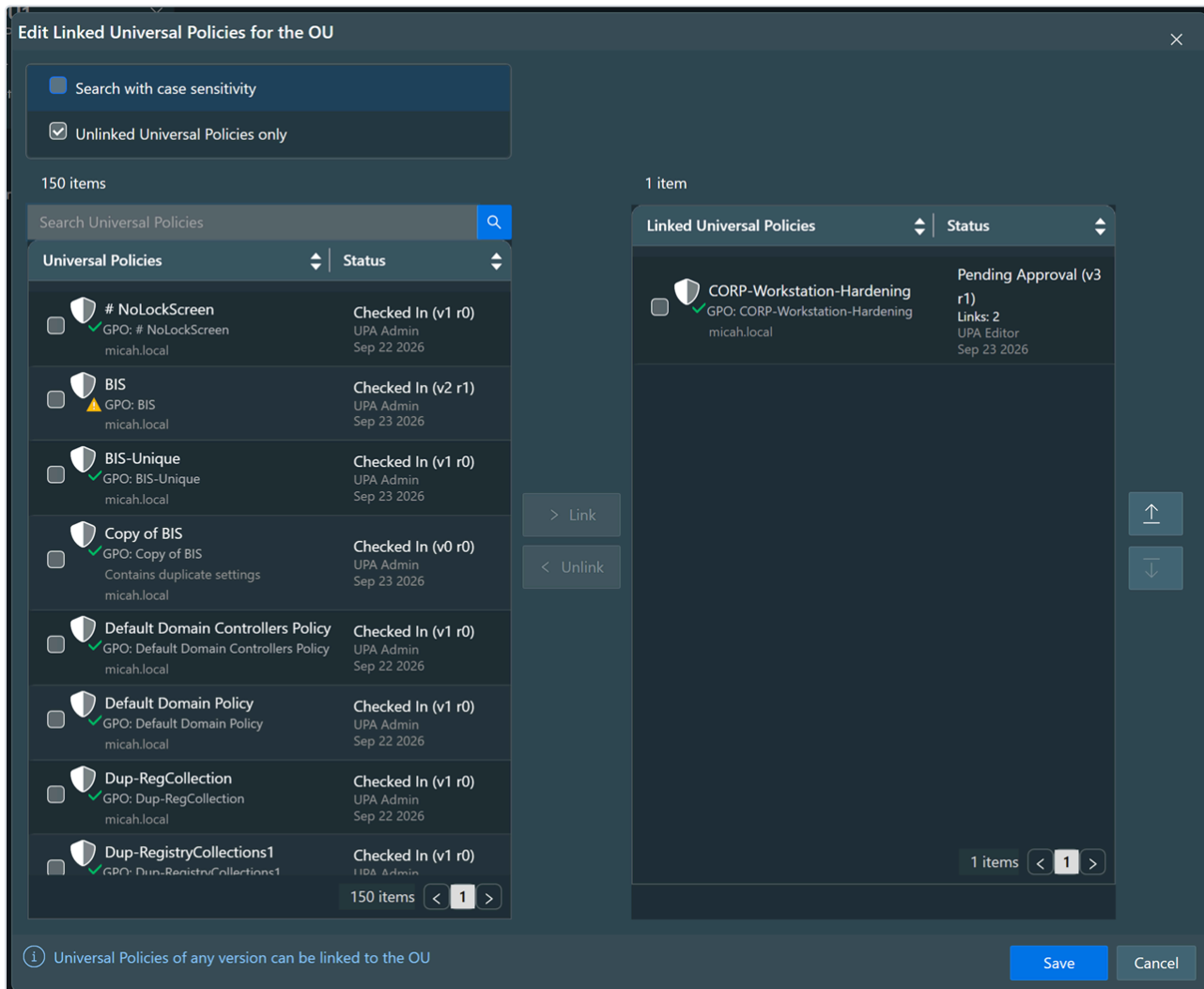
POLICIES

Linked Universal Policies (1)

Link the policies

The **Edit Linked Universal Policies for the OU** dialog lists every policy on the left and the ones already linked on the right.

1. Find the policy in the left-hand list — use the search box, and tick **Unlinked Universal Policies only** to hide everything already linked.
2. Tick the policy, then click **Link >**. It moves to the **Linked Universal Policies** list on the right.
3. Repeat for any other policies.
4. Click **Save**.



To remove a policy from the OU later, select it on the right and click **< Unlink**. That only removes it from this Delegation OU — the policy itself is untouched.

Once saved, the OU's **Policies** panel shows **Linked Universal Policies (n)**, and those are exactly the policies your scoped Editor will see.

A policy of **any version** can be linked, including one that is checked out or pending approval.

Step 9 — The Approver

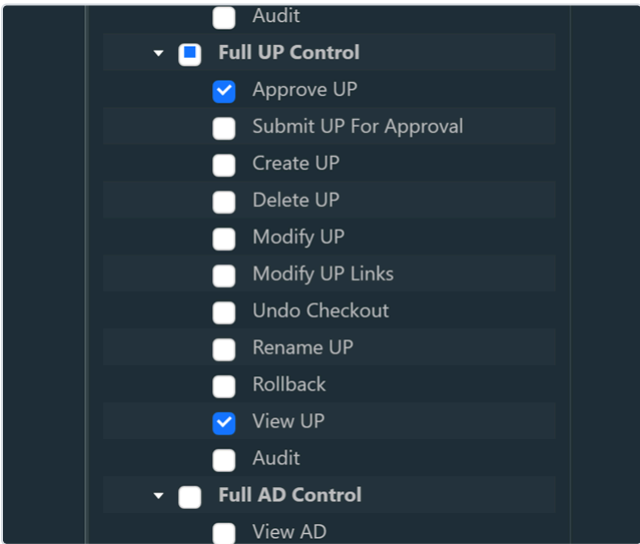
The Approver decides whether the Editor's work is released. They deliberately cannot write policy content, so approval is a genuine second pair of eyes rather than a formality.

Create the Role

- 1. **Administration** → **Roles** → **New**, named **Approver - Approve only**.
- 2. Tick exactly two permissions:

Permission	Where in the tree
Approve UP	Full UP Control
View UP	Full UP Control (also shown under Full Domain Control)

- 1. Click **Save**.



Note what is **clear**: **Submit UP For Approval**. The Approver cannot submit work and then approve it themselves. **Export To AD** is clear too — approving is not publishing.

Create the View

- 1. **Administration** → **Views** → **New**, named **Approver - View Delegation OU**.
- 2. Add one rule: `Delegation_OU1` , **Include**, **OU**, **Recursive No** — the same scope as the Editor's view.
- 3. Click **Save**.

UPA
UNIVERSAL POLICIES
ABOUT

UNIVERSAL POLICIES (1)
WINDOWS

Refresh

CORP-Workstation-Hardening

Universal Policy

Status

CORP-Workstation-Hardening
GPO: CORP-Workstation-Hardening
micah.local

Pending Approval (v1 r0)
Links: 2
UPA Editor
Sep 24 2026

CORP-WORKSTATION-HARD...
RELEASE 0, VERSION 1 PENDING A...

✓

Approve

✗

Reject

PLATFORMS

Windows Group Policy

Policies (7)

Preferences

DETAILS

Linked OUs (0)

Synchronization

Events

Exports

Security Filtering (1)

REPORTS

Conflicts

Differences

Settings

Create the Assignment

1. **Administration** → **Assignments** → **New**, named **Approver - Approve only**.
2. Add the Role, `micah.local\upa_approver`, and the View.
3. Click **Save**.

UPA

ADMINISTRATIONORGANIZATIONUNIVERSAL POLICIESAUDITINGABOUT

Roles

Define which actions can be performed

Views

Define which things can be seen

ASSIGNMENTS

ALL ASSIGNMENTS (9)

New

Edit

Delete

Refresh

Assignment

Approvers - Approve only

Deployer - Export only

Editor - Create UPs

Editor - Delegation OU Assignment

APPROVER - APPROVE ONLY

Name

Type

Approvers - Approve only

Role

UPA Approver

User

Approvers - View Delegation OU

View

The Approver sees the same policies as the Editor and nothing else. Scoping both to the same Delegation OU is what keeps the pair working on one agreed set.

Step 10 — The Deployer

The Deployer publishes an approved policy into Active Directory. This is the only role here that writes to AD.

Create the Role

- 1. Administration → Roles → New, named **Deployer**.
- 2. Tick these permissions:

Permission	Gives the Deployer
Export To AD	the ability to publish an approved policy
Create GPO	the ability to create the backing GPO when one does not exist
Modify UP Links	the ability to link the policy where it must apply
View AD	sight of the directory to publish into
View GPO	sight of the resulting GPOs
View OU	sight of the OU structure
View UP	sight of the policy being published

- 1. Click **Save**.

UPA

ADMINISTRATION

ORGANIZATION

UNIVERSAL POLICIES

AUDITING

ABOUT

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 (9)

+

✎

🗑

↻

New

Edit

Delete

Refresh

Role

Approver

Approver - Approve only

Deployer

Editor

Editor - Create UPs

Editor - View, Edit, and Create UPs

Full Administrator

Reviewer

Reviewer - audit only

DEPLOYER

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

Note what is **clear**: **Modify UP**, **Create UP**, **Approve UP** and **Submit UP For Approval**. The Deployer publishes what was approved — they cannot alter it on the way out, and they cannot approve it themselves.

Use the Global view

This role is assigned the **Global** view rather than a scoped one. That is deliberate: publishing writes into Active Directory, and the GPO or OU it must reach can be anywhere in the policy environment. A view scoped to one Delegation OU would block the very thing the role exists to do.

Create the Assignment

1. **Administration** → **Assignments** → **New**, named **Deployer - Export only**.
2. Add the Role, `micah.local\upa_deployer`, and the **Global** view.
3. Click **Save**.

Universal Policy Administrator

14 of 23

FULLARMOR

UPA

ADMINISTRATIONORGANIZATIONUNIVERSAL POLICIESAUDITINGABOUT

Roles

Define which actions can be performed

Views

Define which things can be seen

ASSIGNMENTS

ALL ASSIGNMENTS (9)

New

Edit

Delete

Refresh

Assignment

Approvers - Approve only

Deployer - Export only

Editors - Create UPs

Editors - Delegation OU Assignment

DEPLOYER - EXPORT ONLY

Name

Type

Deployer

Role

UPA Deployer

User

Global

View

Step 11 — The Reviewer

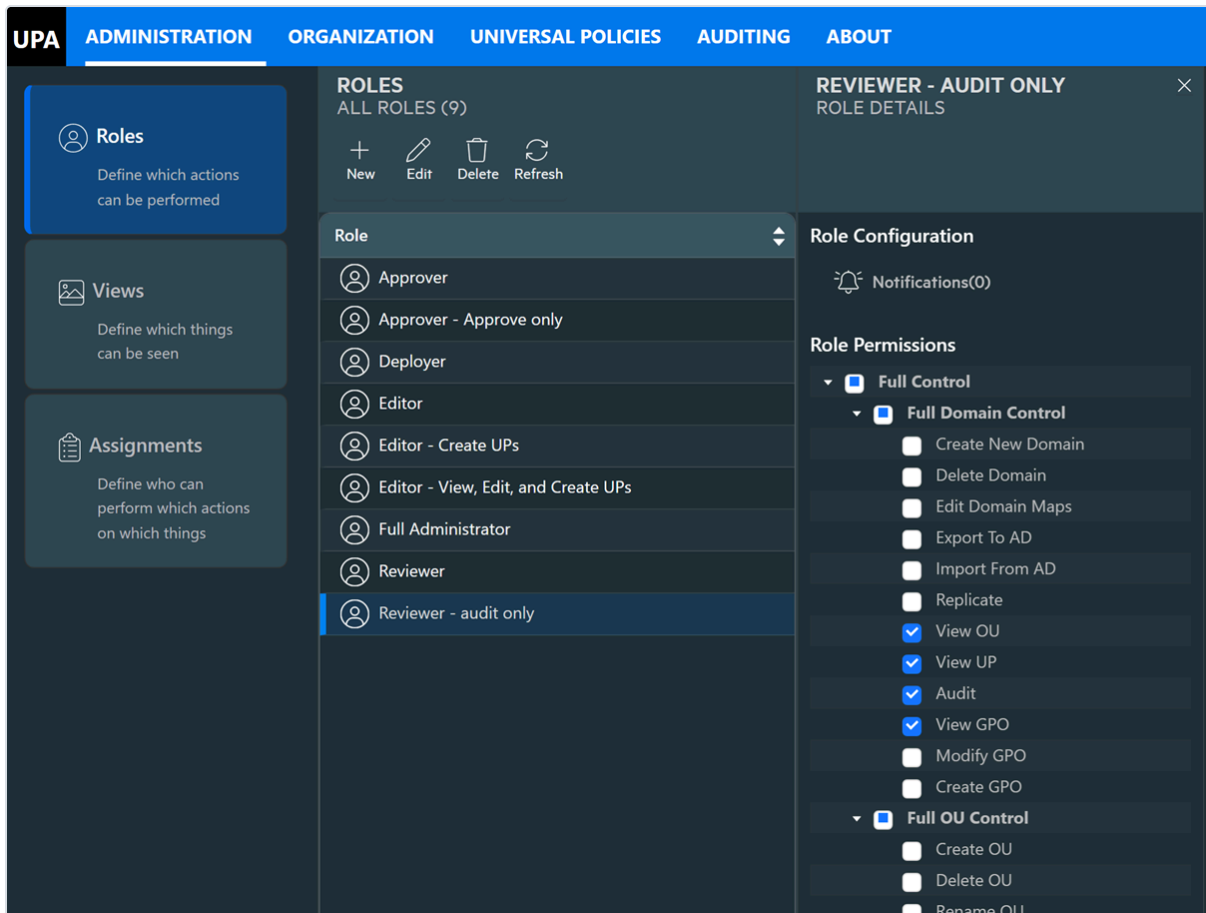
The Reviewer answers "who changed what, and when". They can read everything and change nothing.

Create the Role

- 1. **Administration** → **Roles** → **New**, named **Reviewer - audit only**.
- 2. Tick these permissions:

Permission	Gives the Reviewer
Audit	the audit trail — who did what, and when
View UP	sight of every policy
View OU	sight of the OU structure
View GPO	sight of the GPOs in Active Directory
View AD	sight of the directory
View Delegation	sight of the Roles, Views and Assignments themselves

- 1. Click **Save**.



Every **Create**, **Modify**, **Delete**, **Rename**, **Approve**, **Submit** and **Export To AD** permission stays clear, in every branch. The role cannot change anything.

View Delegation is worth calling out: it lets the Reviewer inspect the delegation setup itself — so an auditor can confirm the Editor really does lack Approve and Export, rather than taking it on trust.

Use the Global view

Assign the **Global** view. An auditor scoped to one Delegation OU could not answer a question about anywhere else, which defeats the purpose of the role.

Create the Assignment

1. **Administration** → **Assignments** → **New**, named **Reviewer - Audit/View only**.
2. Add the Role, `micah.local\upa_reviewer`, and the **Global** view.
3. Click **Save**.

UPA

ADMINISTRATION

ORGANIZATION

UNIVERSAL POLICIES

AUDITING

ABOUT

Roles

Define which actions can be performed

Views

Define which things can be seen

ASSIGNMENTS

ALL ASSIGNMENTS (9)

+

✎

🗑

↻

New

Edit

Delete

Refresh

Assignment

📋

Approver - Approve only

📋

Deployer - Export only

📋

Editor - Create UPs

📋

Editor - Delegation OU Assignment

REVIEWER - AUDIT/VIEW ONLY

×

Name

Type

👤

Reviewer - audit only

Role

👤

UPA Reviewer
micah.local\upa_reviewer

User

🖼

Global

View

Step 12 — How a change now flows

1. **The Editor** opens a policy in the Delegation OU — or creates a new one — then **Check Out**, makes the changes, and **Check In with a comment** recording what changed and why.
2. **The Editor** clicks **Submit for Approval, with a comment**. This hands the policy on and notifies the Approver. The Editor can do no more.
3. **The Approver** reviews it and **approves or rejects** it. They see the Editor's comments, and the same set of policies. They cannot edit it — if it is wrong, it goes back.
4. **The Deployer** takes the approved policy and **exports it to Active Directory**, creating or updating the backing GPO and linking it where it must apply.
5. **The Reviewer** can, at any point, read the policy, the GPO, and the audit trail of every step above — without being able to alter any of it.

Capability by role

Every row has exactly one owner, or is read-only. No column holds both **edit** and **approve**, or both **approve** and **export**.

CAPABILITY	EDITOR	APPROVER	DEPLOYER	REVIEWER
See policies in the Delegation OU	✓	✓	✓	✓
Create a Universal Policy	✓	—	—	—
Edit a Universal Policy	✓	—	—	—
Submit for approval	✓	—	—	—
Approve or reject	—	✓	—	—
Export to Active Directory	—	—	✓	—
Create the backing GPO	—	—	✓	—
Read the audit trail	—	—	—	✓
Inspect the delegation setup	—	—	—	✓
SCOPE OF THE VIEW	Delegation OU	Delegation OU	Global	Global

WHY TWO ARE GLOBAL

The **Deployer** writes into Active Directory, and the GPO it must reach can sit anywhere — a scoped view would block the one thing the role exists to do. The **Reviewer** scoped to one OU could not answer “who changed what, anywhere”.

KEY

- ✓ granted by the role
- permission left clear

Step 13 — Verify the setup

Sign in as each account in turn. Most of the answer is visible before you click anything — the tab strip along the top differs for every role, and so does the policy count.

As the Editor

UPA
ORGANIZATION
UNIVERSAL POLICIES
ABOUT

UNIVERSAL POLICIES (1)
WINDOWS

+
Refresh

CORP-Workstation-Hardening

✕

🔍

Universal Policy

Status

CORP-Workstation-Hardening

GPO: CORP-Workstation-Hardening
micah.local

Checked In (v1 r0)

Links: 2
UPA Admin
Sep 24 2026

CORP-WORKSTATION-HARD... ✕
RELEASE 0, VERSION 1 CHECKED IN

Checkout

Submit for Approval

Merge

PLATFORMS

Windows Group Policy

Policies (7)

Preferences

DETAILS

Linked OUs (2)

Synchronization

Events

Exports

Security Filtering (1)

REPORTS

Conflicts

Differences

Settings

No **Administration** tab, so the Editor cannot alter the delegation that constrains them, and no **Auditing** tab. One policy — the one linked into the Delegation OU — sitting **Checked In**. The second blade offers **Checkout** and **Submit for Approval**, and neither Approve nor Export.

- ❑ Only the policies linked to the Delegation OU are listed
- ❑ A new policy can be created, and appears in the Delegation OU
- ❑ A policy can be checked out, changed, and checked in with a comment
- ❑ **Submit for Approval** is available
- ❑ **Approve** and **Export to Active Directory** are not available

As the Approver

Universal Policy Administrator

19 of 23

FULLARMOR

UPA
UNIVERSAL POLICIES
ABOUT

UNIVERSAL POLICIES (1)
WINDOWS

Refresh

CORP-Workstation-Hardening

Universal Policy

Status

CORP-Workstation-Hardening
GPO: CORP-Workstation-Hardening
micah.local

Pending Approval (v1 r0)
Links: 2
UPA Editor
Sep 24 2026

CORP-WORKSTATION-HARD...
RELEASE 0, VERSION 1 PENDING A...

✓

Approve

✗

Reject

PLATFORMS

Windows Group Policy

Policies (7)

Preferences

DETAILS

Linked OUs (0)

Synchronization

Events

Exports

Security Filtering (1)

REPORTS

Conflicts

Differences

Settings

The same scope as the Editor, with the **Organization** tab gone too — this account cannot link or create policies. The policy is now **Pending Approval**, and the second blade offers exactly two actions: **Approve** and **Reject**. There is no **Checkout**, so the Approver cannot edit what they are reviewing.

- ❑ The same policies are listed, and no others
- ❑ A submitted policy can be approved or rejected
- ❑ **Check Out** and **Export to Active Directory** are not available

As the Deployer

UPA
ORGANIZATION
UNIVERSAL POLICIES
ABOUT

UNIVERSAL POLICIES (1)
WINDOWS

Refresh

CORP-Workstation-Hardening

Universal Policy
Status

CORP-Workstation-Hardening
GPO: CORP-Workstation-Hardening
micah.local

Approved (v1 r1)
Links: 2
UPA Approver
Sep 24 2026

CORP-WORKSTATION-HARD...
RELEASE 1, VERSION 1 APPROVED

PLATFORMS

Windows Group Policy

Policies (7)

Preferences

ACTIONS

Export to Active Directory

DETAILS

Linked OUs (2)

Synchronization

Events

Exports

Security Filtering (1)

REPORTS

Conflicts

Differences

Settings

CONFIGURATION

Enabled

Global scope, because the GPO it must reach can be anywhere. The policy now reads **Approved**, and **Export to Active Directory** has appeared on the second blade — the one action this role exists for. There is still no **Checkout** and no **Approve**.

Universal Policy Administrator

21 of 23

FULLARMOR

- ☐ An approved policy can be exported to Active Directory
- ☐ **Check Out** and **Approve** are not available

As the Reviewer

PING ABOUT		Tr UPA REVIEW							
CORP-WORKSTATION-HARD... RELEASE 1, VERSION 1 APPROVED		EVENTS (10) CORP-WORKSTATION-HARDENING							
		Refresh Share Report							
PLATFORMS									
Windows Group Policy									
Policies (7)									
Preferences									
DETAILS									
Linked OUs (2)									
Synchronization									
Events									
Exports									
Security Filtering (1)									
REPORTS									
Conflicts									
Differences									
Settings									
CONFIGURATION									
Enabled									
VERSION: 1									
RELEASE: release-1									
		Event	Source Type	Source	Target Type	Target	User	Time	Comment
		Approve	CCM	CORP-Workstation-Hardening	Universal Policy	UPA Approver	UPA Approver	Sep 24 2026 11:16:08 AM	Reviewed against CR-2041. Approved.
		Submit for Approval	CCM	CORP-Workstation-Hardening	Universal Policy	CORP-Workstation-Hardening	UPA Editor	Sep 24 2026 11:15:39 AM	Hardening baseline ready for review. CR-2041.
		Revert	CCM	CORP-Workstation-Hardening	Universal Policy	UPA Editor	UPA Editor	Sep 24 2026 11:12:38 AM	
		Check Out	CCM	CORP-Workstation-Hardening	Universal Policy	UPA Editor	UPA Editor	Sep 24 2026 10:53:41 AM	
		Link Universal Policy to OU	Universal Policy	CORP-Workstation-Hardening	Universal Policy	OU=Delegation_OU1	UPA Admin	Sep 24 2026 10:52:41 AM	
		Repository OU Link Added	Universal Policy	CORP-Workstation-Hardening	Universal Policy	OU=Corp-Workstations,OU=Corp,DC=micalh,DC=local	UPA Admin	Sep 24 2026 8:52:21 AM	
		Check In	CCM	CORP-Workstation-Hardening	Universal Policy	Special Import Branch	UPA Admin	Sep 24 2026 8:49:00 AM	Imported in mass
		Update	CCM	CORP-Workstation-Hardening	Universal Policy	Special Import Branch	UPA Admin	Sep 24 2026 8:49:00 AM	
		Check Out	CCM	CORP-Workstation-Hardening	Universal Policy	Special Import Branch	UPA Admin	Sep 24 2026 8:49:00 AM	
		Create	CCM	CORP-Workstation-Hardening	Universal Policy	GPO=CORP-Workstation-Hardening	UPA Admin	Sep 24 2026 8:49:00 AM	

Events on the second blade opens the policy's full history: the approval by UPA Approver, the submission by UPA Editor, the link into the Delegation OU by UPA Admin — each with the comment its author left. The Reviewer is also the only role with an **Auditing** tab, and its toolbar offers **Refresh** and nothing else — no **New**.

- ☐ Policies, OUs and GPOs are all visible
- ☐ The audit trail is available
- ☐ Nothing can be created, changed or deleted

If somebody sees more than expected, check two things: the **Recursive** setting on their View, and whether their account is also a member of a broader assignment such as **Global Editors**.

If the Editor sees nothing at all, check that policies were actually linked in Step 8 — the Delegation OU's **Linked Universal Policies** count should be greater than zero.

What you built

Purpose	Role	View	Assignment
Work on policies in the OU	Editor - View, Edit, and Create UPs	Editor - View Delegation OU	Editor - Delegation OU Assignment
Create new policies	Editor - Create UPs	Editor - Create UPs	Editor - Create UPs
Approve or reject	Approver - Approve only	Approver - View Delegation OU	Approver - Approve only

Purpose	Role	View	Assignment
Publish to Active Directory	Deployer	Global	Deployer - Export only
Read and audit	Reviewer - audit only	Global	Reviewer - Audit/View only

Plus, in the **Organization** tab: the Delegation OU `Delegation_OU1`, and the Universal Policies linked into it.

The permissions behind it

The same five Roles as a single reference, for checking a setup rather than building one. Open each Role in **Administration** → **Roles** and compare. The right-hand column is the one that matters — a permission that has crept back in there is what quietly dissolves the separation.

Role	Ticked	Deliberately clear
Editor - View, Edit, and Create UPs	View OU, View UP, Create UP, Modify UP, Modify UP Links, Submit UP For Approval, Undo Checkout, Rollback	Approve UP, Export To AD , Delete UP, Rename UP
Editor - Create UPs	View AD — and nothing else, anywhere	everything else in every branch
Approver - Approve only	Approve UP, View UP	Submit UP For Approval, Export To AD , Modify UP, Create UP
Deployer	Export To AD, Create GPO, Modify UP Links, View AD, View GPO, View OU, View UP	Modify UP, Create UP, Approve UP , Submit UP For Approval
Reviewer - audit only	Audit, View UP, View OU, View GPO, View AD, View Delegation	every Create, Modify, Delete, Rename, Approve, Submit and Export To AD

Three checks settle whether the separation still holds:

- No role has both **Modify UP** and **Approve UP**.
- No role has both **Approve UP** and **Export To AD**.
- **Export To AD** is ticked in exactly one role — the Deployer.

Full AD Control, Full GPO Control, Full Agent Control and Full Delegation Control stay entirely clear for the Editor's main role; the second Editor role exists only to hold **View AD**, because a scoped Editor cannot otherwise create a policy.