nerdio | manager for enterprise

EDITION 2026

MICROLEARNING

Intune Policy Studio

and the rollback Intune never had

By **Bas van Kaam**

PRINCIPAL LEARNER ARCHITECT

STEP 1 · WHY THIS LESSON

In Intune, you can *push* a policy. You cannot pull it back.

01 70% of incidents start with a misconfig

Up to 70% of major production incidents stem from misconfigurations (ECI Research). Intune is no exception. One typo in a Conditional Access policy can lock every signed-in user out.

02 No rollback button anywhere

Native Intune has no rollback button. When a policy goes wrong, there is no instant way back to the previous known-good state. The fix becomes a manual scramble.

03 Policy Studio adds the safety net

Intune Policy Studio in Nerdio Manager for Enterprise 8.0 adds versioning, approval workflow, drift detection, and full audit history on top of the same Intune you already use.

STEP 2 · WHAT IT IS

One console for the full Intune policy lifecycle.

Centralized in Nerdio Manager for Enterprise 8.0. Handles create, edit, version, assign, publish, monitor, and roll back. Public Preview was announced at NerdioCon 2026 in Palm Springs and rolls out late May.

POLICY STUDIO AT A GLANCE

Launch	Announced at NerdioCon 2026 (May 5, 2026). Public Preview in Nerdio Manager for Enterprise 8.0, rolling out late May 2026.
Foundation	Built on the existing Intune integration in Nerdio Manager. No separate license required.
Coverage	All Intune policy types: compliance, configuration profiles, security baselines, conditional access, app policies, and update rings.
Coexistence	Native Intune admin center keeps working. Edits made directly there are detected and reported with the admin's UPN.
Audience	Endpoint security admins, EUC engineers, compliance and audit officers managing Intune at scale.

STEP 3 · THE FOUR PILLARS

What Policy Studio adds on top of native Intune

VERSIONING & ROLLBACK

Auto-backup on every change

Snapshot taken whenever a policy is edited, in Nerdio Manager or directly in the Intune admin center. Up to 50 versions per policy, retained up to 156 weeks.

Side-by-side diff

Visual comparison of any two versions in the JSON editor. Shows exactly which setting moved, which assignment changed, who did it.

One-click restore

Revert a policy and its assignments together, or just one of them. The "undo button" Intune does not have natively.

APPROVAL WORKFLOW

Submitter / Approver RBAC

Two custom roles: `Read Approvals` and `Manage Approvals`. Submitters draft, approvers review, approve, or reject before anything reaches Intune.

Diff review with notes

Approver sees the JSON diff, the assignment changes, and the requester's message. Send back for rework if needed.

No self-approval

Approvers cannot approve their own changes. Forces a true four-eye review and removes the "I'll just push it quickly" failure mode.

DRIFT DETECTION

Out-of-band edit tracking

Detects when a policy was changed directly in the Intune admin center, not Nerdio Manager. Catches the "someone fixed it manually at 11 PM" scenario.

UPN of who changed what

External policy change tracking captures the UPN of the admin who made the change. No more "no idea who edited the CA policy".

Realign to desired state

One click to push the Nerdio Manager version of the policy back into Intune, overwriting the drifted settings.

AUDIT & CHANGE HISTORY

Full change log

Every edit, with the requester's description, the approver's notes, and the resulting JSON diff. Searchable per policy or per admin.

Recoverable submissions

Rejected change requests preserve the proposed content, so the requester can adjust and resubmit without retyping the whole policy.

Compliance-ready trail

Exportable evidence for HIPAA, PCI-DSS, ISO 27001, and SOC 2 audits: who requested what, who approved, when it published.

STEP 4 · HOW IT WORKS

From "I need to change a policy" to "published, audited, reversible" in five moves

0

Enable Intune integration and approval workflow ONE-OFF

In Nerdio Manager: `Settings > Environment > Intune`. Enable in Application context mode. Then turn on Policy approval requests and assign the `Read Approvals` and `Manage Approvals` roles to your reviewers.

1

Open Policy Studio and edit the policy

`Endpoints > Policy Management`. Pick the tab for the policy type (compliance, configuration, conditional access, etc.) and select Edit. The JSON editor opens with field suggestions, autocomplete, and type validation.

2

Submit for approval (auto-backup is taken)

Save the change. A backup of the previous version is taken automatically before anything moves. Add a change-log message explaining the why. Approvers receive an in-app notification and email.

3

Approver reviews the diff and assignments

Approver opens `Endpoints > Approvals`. Sees the JSON diff side-by-side with the live policy, the assignment changes, and the requester's note. Approve, reject with feedback, or send back for rework. Self-approval is blocked.

4

Approved policy publishes to Intune (audit entry written)

Approved changes publish to Intune via Microsoft Graph. Change log records who requested, who approved, when published, and the JSON diff. Drift detection takes over from there.

STEP 5 · THE INSIGHT TO REMEMBER

Policy Studio is not a different Intune.

*It is **the same Intune**, with versioning, four-eye approval, drift detection, and full audit history baked in between you and production.*

STEP 6 · IN PRACTICE

The accounting-firm CA scenario

TODAY

A 280-person regional accounting firm runs four IT admins on a single Microsoft 365 tenant, all endpoints managed through Intune. With tax season approaching, a junior admin needs to update the Conditional Access policy that gates the financial reporting tool, to allow newly hired contractors temporary access. The firm has had to roll back three CA policy changes in the last 18 months, each one painful.

280	4	3	0
EMPLOYEES	IT ADMINS	PAINFUL ROLLBACKS	NATIVE UNDO

WITH POLICY STUDIO

The junior opens the CA policy in Policy Studio, edits the Excluded Groups, adds a change-log message, and submits. A senior admin opens the Approvals dashboard, spots in the diff viewer that the new exclusion accidentally removes the firm's partners, rejects with feedback. Junior corrects, resubmits, gets approved.

✓ **Auto-backup**
Snapshot of the live policy before anything moves

✓ **Diff viewer**
Senior spots the partner exclusion error visually

✓ **4-eye review**
Self-approval blocked, junior cannot push it alone

25 min total elapsed · partners impact zero · audit trail ready for the firm's annual security review

STEP 7 · NOW YOU TRY

Three questions to lock the lesson in

Q · 01

In your own words, why is "no native rollback" in Intune such an underrated risk?

Hint: *One bad CA policy locks every user out. Manual fix, no audit trail.*

Q · 02

Which two Policy Studio pillars would have caught your last bad policy push?

Hint: *Approval workflow (four-eye review) and versioning (one-click rollback).*

Q · 03

Who in your team or customer base should be Submitter, and who should be Approver?

Hint: *Submitter drafts. Approver reviews. No self-approval. Need enough approvers for timely review.*

TAKE-AWAY

Same Intune. Same Microsoft Graph.
Now with **the brakes you didn't know were missing.**

Found this useful? Share it with one colleague who'd benefit from a four-eye review on Intune.

BAS VAN KAAM · PRINCIPAL LEARNER ARCHITECT AT NERDIO