ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP

CLEARWATCH SOLUTION BRIEF · MICROSOFT INTUNE

Microsoft Intune, from managed to monitored.

How ClearWatch reads a client's Intune tenant after one approval at Microsoft, imports the devices it manages and pushes the ClearWatch agent to them through Intune.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO MICROSOFT INTUNE

EXECUTIVE SUMMARY

Managed is not the same as watched.

Intune knows which devices a client owns, whether they meet policy and who uses them. It does not watch a filling disk, a stopped service or a failed backup, and getting a monitoring agent onto every device means packaging, uploading and assigning it by hand, tenant by tenant.

ClearWatch connects to a client's tenant after its own administrator approves ClearWatch at Microsoft, so no password is handed over. It reads the tenant every hour, imports the devices you choose or a rule picks, shows their compliance and health, and pushes the ClearWatch agent to them through Intune.

KEY TAKEAWAYS

- **No password, ever:** the tenant's administrator approves at Microsoft, and nothing of theirs is stored.
- **Import by rule:** by Entra group, platform, ownership, Autopilot tag or name, placed where the rule says.
- **The agent through Intune:** ClearWatch creates the group and assigns the agent.
- **Recovery keys on request:** read live from Intune, audited before they are shown.

IN THIS BRIEF

01 **The challenge** — What Intune leaves to you — 2
02 **How ClearWatch connects** — One approval at Microsoft — 2
03 **Devices into ClearWatch** — The device list, and import rules — 4
04 **The agent, and the device** — Deploying, the Intune card, recovery keys — 5
05 **Checks and alerts** — Compliance and device health — 6
06 **Good to know** — Requirements and limits — 6

WHO THIS IS FOR

MSPs whose clients manage their devices with Microsoft Intune, and IT teams with their own tenant, who want every managed device monitored and the agent deployed without packaging it by hand.

AT A GLANCE

CONNECTION	REFRESHED	LICENSING	AGENT
Admin consent	**Every hour**	**Per device**	**Through Intune**
Approved at Microsoft by the tenant's administrator.	Or read at once with Read from Intune now.	An imported device uses one device license.	A group, an assignment and status per device.

01 THE CHALLENGE

Intune manages devices. It does not monitor them.

Intune is where a client's devices are enrolled, configured and held to policy. It answers whether a device is compliant and when it last checked in. It does not tell an engineer that a disk is filling, a service has stopped or a patch failed, and the tools that do need an agent on every device, put there tenant by tenant.

THE QUESTION	INTUNE ADMIN CENTER ALONE	CLEARWATCH
Which client is this device?	Switch to that client's tenant	Each tenant **connected to a client**, its domains to their organizations
Is every managed device monitored?	Intune runs no monitoring	A **Not in ClearWatch** list, and **import rules**
How does our agent get there?	Package, upload and assign it by hand	**Deploy agent**: ClearWatch builds the group and the assignment
Why is it not compliant?	Open the device's policies one by one	The **failing settings named** on the device and in the alert
The recovery key, right now?	Sign in to the admin center as that tenant	**Revealed on the device page** to people allowed, audited first

A device in Intune is not a device being watched

Intune's view stops at policy and check-ins. ClearWatch brings each managed device in, with its compliance and health, and then puts the agent on it through Intune, so the full monitoring that runs on every other machine takes over: disks, services, patching, backups and remote control.

02 HOW CLEARWATCH CONNECTS

One approval at Microsoft, then Microsoft Graph

ClearWatch's own servers read the tenant through Microsoft Graph every hour, as an app the client's administrator approved. Nothing is installed to connect, and ClearWatch writes to the tenant only when you deploy the agent.

THE CLIENT'S TENANT
Microsoft Intune
Manages the devices exactly as it does today.

→

MICROSOFT CLOUD
Microsoft Graph
Answers for devices, compliance, profiles and apps; takes the agent's deployment.

→

CLEARWATCH'S SERVERS
Devices and checks
Imports and places devices, runs the checks, deploys the agent.

The client's administrator can withdraw the approval in Microsoft Entra at any time. ClearWatch keeps only the tenant's ID.

YOU PROVIDE	WHAT IT IS
The tenant's domain or ID	The client's Microsoft domain, or its tenant ID, typed into **Add tenant**.
An administrator's approval	A Global Administrator or Privileged Role Administrator of the tenant presses Accept at Microsoft, once. Their password never reaches ClearWatch.
Where devices go	Each of the tenant's domains mapped to one of your organizations, and a default for devices with no primary user.

02 HOW CLEARWATCH CONNECTS, CONTINUED

A domain, a link and an administrator's Accept

Under Manage, Integrations, Microsoft Intune, **Add tenant** opens a window. The tenant is connected to the organization chosen in the console's picker 1 .

Type the tenant's domain or tenant ID and press **Make link**. **Enable Intune** 2 takes an administrator of the tenant to Microsoft, where they sign in under their own MFA and press Accept. That creates the ClearWatch Enterprise App in their tenant.

Approving needs a Global Administrator or a Privileged Role Administrator. If that is somebody else, copy the link for them 3 . It works for seven days, connects only that tenant and finishes only in your own ClearWatch session.

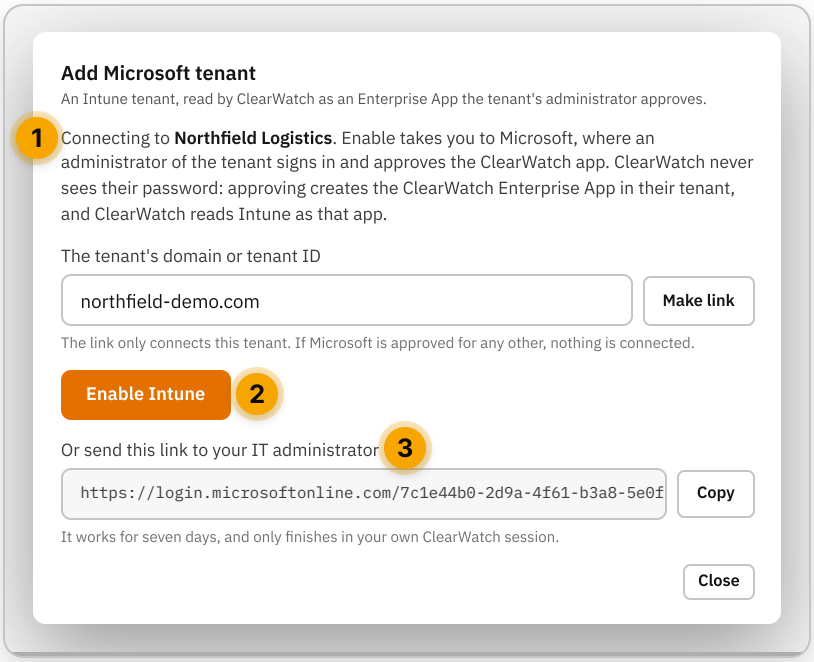


FIGURE 1 Add Microsoft tenant, rebuilt from the ClearWatch console with demo data.

What the approval grants

The ClearWatch app asks for Microsoft Graph application permissions in three groups. Most only read. The write permissions are used only when somebody deploys the agent, and the recovery key permissions only when somebody allowed to presses Reveal.

FOR	GRAPH PERMISSIONS	WHAT CLEARWATCH DOES WITH THEM
Reading the tenant	`DeviceManagementManagedDevices.Read.All`, `DeviceManagementConfiguration.Read.All`, `DeviceManagementApps.Read.All`, `DeviceManagementServiceConfig.Read.All`, `Device.Read.All`, `Domain.Read.All`	The managed devices, which compliance settings fail, profiles, assigned apps, Autopilot records and the tenant's domains
Deploying the agent	`DeviceManagementScripts.ReadWrite.All`, `DeviceManagementApps.ReadWrite.All`, `Group.ReadWrite.All`, `DeviceManagementManagedDevices.PrivilegedOperations.All`	Create the deployment group, add devices, assign the agent as a script or an Intune app, and ask devices to check in
Recovery keys	`BitlockerKey.Read.All`, `DeviceLocalCredential.Read.All`	BitLocker keys and local administrator passwords (LAPS), and FileVault keys, read live on request

A permission added to ClearWatch later must be approved again in each tenant. Until it is, the tenant reads **Needs re-consent**, names what is missing, and everything else keeps working.

03 DEVICES INTO CLEARWATCH

Every managed device, and where it belongs

The tenant's page lists every device Intune manages, with its primary user, compliance and last check-in, and whether it is in ClearWatch yet (1). A device is placed by its primary user's email domain: each of the tenant's domains maps to one of your organizations.

Choose which devices become ClearWatch devices: only the ones you import, those matching your import rules, or every managed device on each sync. Each imported device uses one device license (2), checked before anything is imported.

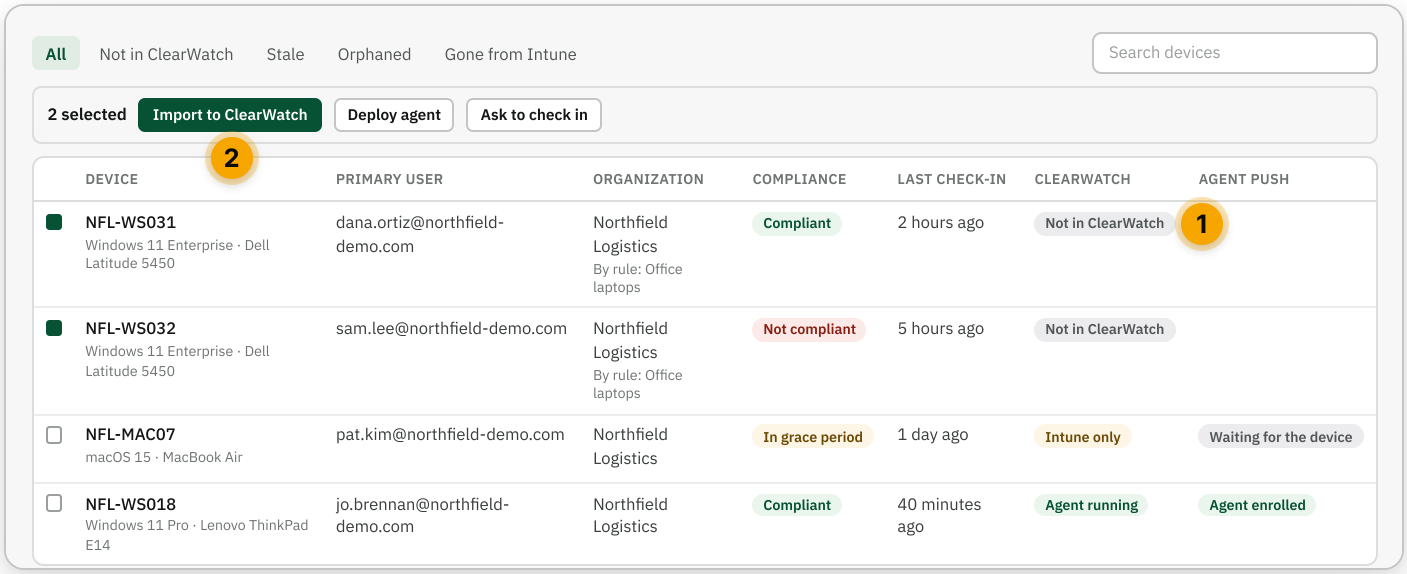


FIGURE 2 A tenant's devices, with the two selected about to be imported (cropped).

Import rules do it for you

A rule imports matching devices on every sync and places them in an organization and location (3). Conditions are Entra groups, operating system, ownership, join type, last check-in, device category, Autopilot tag or profile, and device name. Every condition must match; within one, any value does.

The live preview counts the devices a rule will import before you save it (4). A rule can also push the agent through Intune (5). The first rule a device matches wins, and a device somebody removed by hand is never imported again.

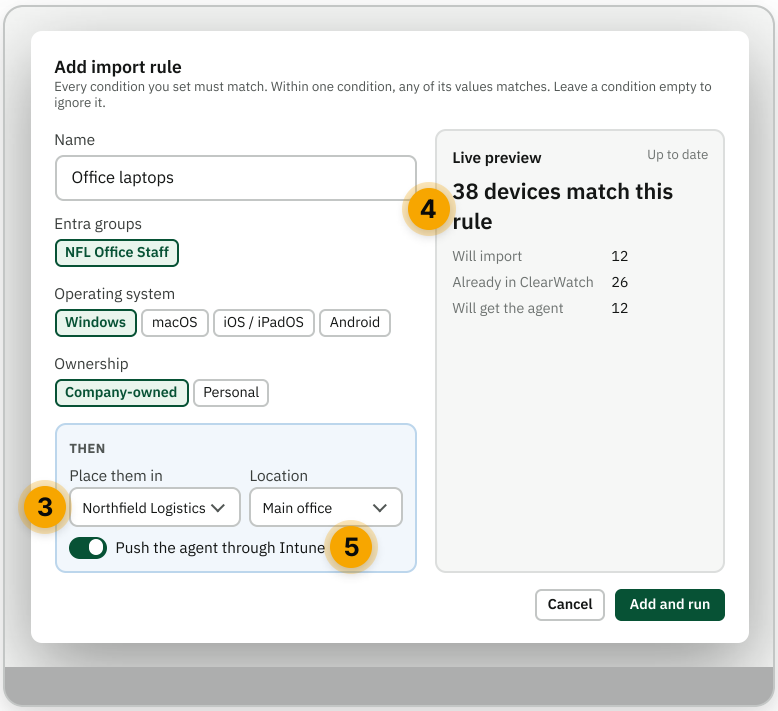
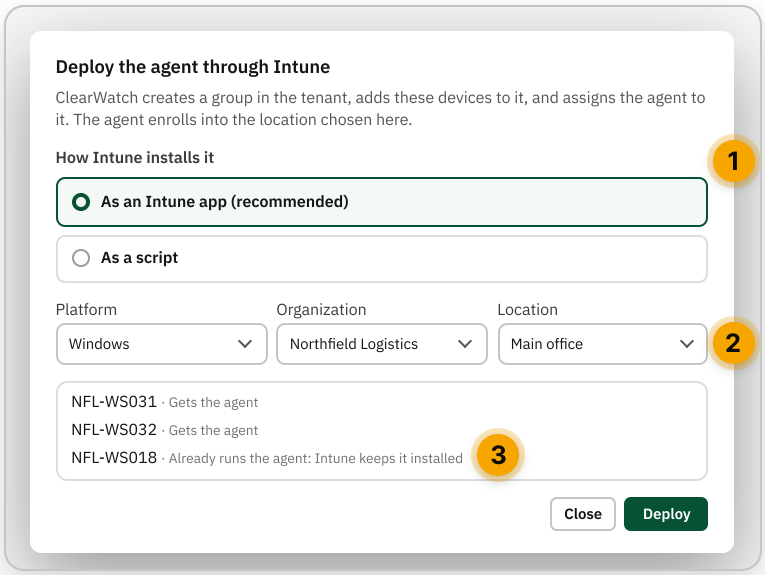


FIGURE 3 Add import rule, with its live preview.

04 THE AGENT, AND THE DEVICE

The ClearWatch agent, deployed through Intune



Deploy agent, on selected devices or from an import rule, creates one Entra group per client, location and platform, adds the devices and assigns the agent to it. Choose how Intune installs it 1 : as an Intune app, or as a script, which puts the agent on once.

The agent enrolls into the location chosen here 2 , and lands on the device row already imported from Intune, matched by its Entra device ID. A device that already runs the agent is listed and left alone 3 .

Each device's progress shows in the Agent push column. Intune installs on its own check-in cycle, so a device can take up to eight hours.

FIGURE 4 Deploy the agent through Intune, for the devices selected.

Intune's view on the device page

An imported device carries an Intune card 4 : compliance with the failing policy and settings named, last check-in, primary user, ownership, encryption and what Intune reports about Microsoft Defender. Configuration profiles, apps and Autopilot follow below it.

Before the agent is on, that is all the device page shows. Once it enrolls, the full device page takes over and the Intune card stays.

Recovery keys, on request

A BitLocker or FileVault recovery key, or a LAPS password, is read live from Intune when somebody holding the Recovery keys permission presses **Reveal** 5 . Nothing is stored. The audit row is written before the read, and the value hides itself after a minute.

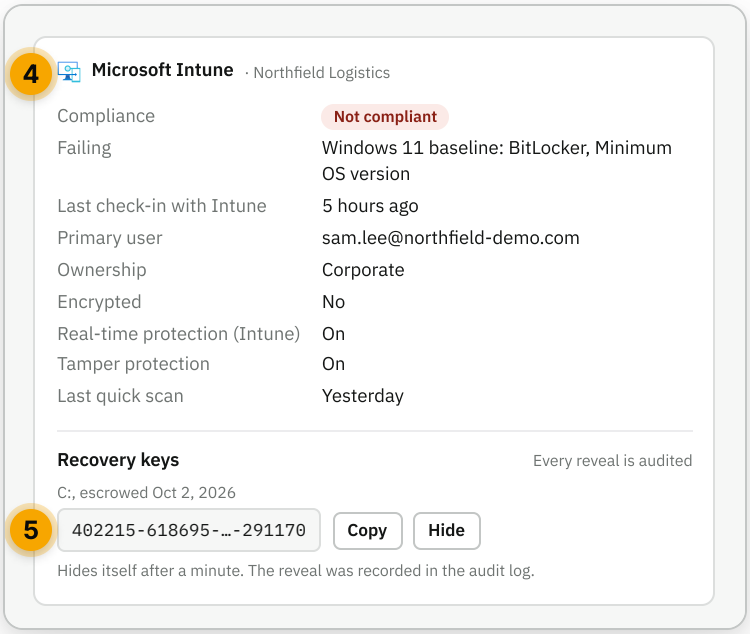


FIGURE 5 The Intune card on a device page (shortened), with a recovery key revealed.

05 CHECKS AND ALERTS

Compliance and device health, as checks

Two built-in monitors read what Intune reports: **Device compliance** and **Intune device health**. Apply them to the clients that use Intune. A Warning goes to Needs attention, a Failed is an Alert, and every level is a default you can change, for everyone or for one device.

CHECK	WARNING	FAILED
Intune compliance	In its grace period, or a state ClearWatch cannot read	Not compliant, in conflict or in error, naming up to six failing settings
Days since Intune check-in	7 days	14 days
Intune configuration profiles	A profile in conflict	A profile in error
Encryption (Intune)	None	The device is not encrypted
Intune app installs	An assigned app failed to install	None

Windows build and macOS, iOS or Android version checks read from Intune are also available, with the levels you set. Alerts follow your notification policies like any other check.

06 GOOD TO KNOW

Requirements

- Microsoft Intune in the client's tenant.
- A Global Administrator or Privileged Role Administrator of the tenant, to approve ClearWatch once.
- The tenant's domains mapped to your organizations, so devices land with the right client.
- The Intune permission in ClearWatch for whoever connects it, and the Recovery keys permission for whoever reveals keys.

Limits

- Each imported device uses a ClearWatch device license, with or without the agent.
- Intune installs on its own check-in cycle: up to eight hours per device.
- A script deployment installs the agent once; it does not put it back if removed.
- No remote wipe or restart from ClearWatch; those stay in Intune.

Every Intune device, monitored like the rest.

Start a free trial, or ask us to connect your Intune tenant with you.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. Microsoft, Intune, Microsoft Entra, BitLocker and Windows are trademarks of the Microsoft group of companies; FileVault and macOS are trademarks of Apple Inc. Screens show demo data.