

Simplify Microsoft management

A practical five-step checklist



Manage Microsoft with confidence

As organizations expand their Microsoft footprint, each new user, device, application and policy adds another layer of operational complexity, making centralized management more difficult. Without a unified approach, IT teams spend more time navigating disconnected tools and fragmented environments than delivering strategic value. The result is slower IT operations and increased administrative overhead.

This complexity doesn't go away on its own, but it becomes far easier to control when you approach it systematically. We've put together a five-step checklist to help you build a more connected, standardized and manageable Microsoft environment — from your first complete inventory through ongoing upkeep.

1

Build a complete inventory

Create a complete inventory of your Microsoft environment by documenting and maintaining visibility into:

Users, identities, security groups and administrative accounts

Microsoft 365 licenses, applications and permissions

Workstations, laptops, servers, mobile devices and Cloud PCs

On-premises infrastructure, virtual machines, network devices and printers

2

Connect your Microsoft environment

Map ownership and relationships across your environment so you can quickly identify:

- Which users are assigned to which devices
- Which security groups and permissions each user has
- Which Microsoft and on-premises assets belong to each location or site
- Which licenses, applications and policies are assigned to users
- Which devices, applications and assets are connected to each other

3

Standardize Microsoft operations

Document repeatable processes for recurring operational work, including:

- User onboarding and provisioning (licenses, groups, MFA, devices, applications)
- Employee offboarding (disable access, revoke sessions, recover licenses, archive historical data)
- Password reset and account recovery (identity verification, MFA recovery, secure access restoration)
- Device provisioning and lifecycle management (Intune/Autopilot enrollment, replacement, retirement)
- Microsoft 365 troubleshooting and recovery (login issues, email, Teams, OneDrive, SharePoint and recovery procedures)

4

Automate Microsoft administration

Automate Microsoft user and device management by ensuring:

- Centralized Microsoft 365 user management (creation, deletion and editing)
- Unified monitoring and automation for Intune devices, Cloud PCs and endpoints from a centralized console
- Standardized user roles and license assignments, plus endpoint monitoring, patching and security policies
- Automated user onboarding and offboarding, including licenses, mailboxes, roles and device access
- Automated agent deployment and maintenance on Windows 365 Cloud PCs and new devices
- Secure remote monitoring, remediation and support without requiring users to be on-site increase admin stress, frustrate users and damage both revenue and trust.

5

Continuously maintain your environment

Ensure complete asset management and eliminate visibility, security and performance gaps by regularly reviewing:

Inactive users, stale accounts and unused Microsoft licenses

Privileged accounts and administrative access

Password health, including passwords that are stale or out of compliance

Unauthorized devices, configuration drift and policy changes

OS versions and systems missing patches or monitoring policies

Hardware standardization across the fleet

Disk health and available storage to prevent Windows crashes

Memory and CPU utilization trends to ensure system performance



Simplify Microsoft management with Kaseya

Kaseya brings Microsoft 365 users, Intune devices, Cloud PCs and on-premises infrastructure into a single console, so your team can automate onboarding and offboarding, standardize policies across the fleet and close the visibility, security and performance gaps this checklist is designed to catch.

[Request your demo today](#)

Kaseya®