

MIGRATING ENDPOINTS

Create a Secure, Productive,
and Modern Environment



At last count, there were well over **1 billion users and 300,000 organizations** using Entra ID (formerly Azure Active Directory). And yet – while difficult to measure – on-premises Active Directory appears to remain alive and well in a majority of organizations that are either continuing to run a strictly on-premises environment, or a hybrid environment utilizing Entra ID.

Organizations that are not fully “cloud-first” should be (or, hopefully, are) taking a long hard look at the Microsoft environment they rely on today and are realizing the need to streamline and strengthen it from several perspectives:



Security: The years of forgotten permissions assigned, group memberships changed, and trusts established – along with the decades of configuration changes made to endpoint – all have resulted in an established and present cybersecurity risk that needs to be addressed through migration to a new environment (whether that be on-prem AD or Entra ID in the cloud) that is known to have a secure configuration.



Management: Take all those security reasons and then multiply them times the number of AD domains (commonly known as AD Sprawl), and then realize that none of it is being proactively managed; after all, IT is far too busy putting out the next fire, and then the next one, and the next one...



Simplicity: Depending on the history of your environment's evolution, you may have far too many domains and trusts that only complicate everything from DNS, to domain controller placement, to security configurations, to creating a singular global address list, and more.



Productivity: When you think about it, both IT and users are locked in a state of coexistence. Sure, everyone's getting their job done, but we all know there are plenty of workarounds in place on IT's part (often considered technical debt by IT) to keep users unaware and productive. Additionally, the reliance upon on-premises AD only stifles the heightened levels of innovation, collaboration, and productivity found with cloud-based applications, tools, and platforms.

The answer to addressing these aspects of your current environment that are less than optimal is a modernization exercise that is found practically in the form of a migration. And as part of that migration, endpoints, the source of much of the security and operational risk, need to come along for the ride.

The goal of this eBook is to provide you with some perspective on the need to migrate your endpoints, pointing out along the way some of the challenges you'll face using real-world use cases, and then provide some guidance on how to best address endpoint migration.

Migrating Endpoints Won't (Necessarily) Be Easy

Roll the clock back to when there was only AD on-premises and the concept of migrating an endpoint was pretty simple: on the “easiest” side of the spectrum, just change domains under Computer Properties, and on the more “advanced” side, use a tool like the User State Migration Tool (USMT) to migrate files, OS settings, user profiles and the like.

It was always historically pretty straightforward, but modern endpoint migrations are a bit more complex; today's organization needs to be concerned with much more than just what domain the endpoint belongs to. Modern endpoint migration is concerned with a number of factors:



The security of the endpoint: There are more security risks than you're aware of (even on your endpoints) that require locking down. A migration is the opportunity to refresh the configuration of affected endpoints to ensure they meet current security requirements.



The user's profile and personalization: Every user (you included) has customized the working environment within their endpoint (think desktop, icons, file locations, application settings, and more). This personalization equates to productivity. So it stands to reason that a migration need to keep as close to 100% of the user's environment intact as possible post-migration.



Having a working endpoint post-migration: When moving to a new environment, there will be configuration changes needed to ensure the security and productivity of the endpoint. Take something as simple as a new WiFi network endpoints will connect to post-migration – this (and every other configuration change like it) needs to be a part of the process. Remember, the perfect migration is one where the user simply logs on to their endpoint post-migration and just starts working.



The user experience during the migration: Historically, migration tools have required users to relinquish their endpoints for a period of time to allow the migration to occur. That's no longer entirely acceptable; the user experience is something the organization is concerned about, making it necessary to find ways to migrate endpoints without inconveniencing the user.



The endpoint management solution post-migration: Today, you may be using System Center or a third-party solution. But after a move to Entra ID, you may be thinking you'll use Intune. Ok, great. But how do you incorporate that change into the migration so that as soon as the endpoint migration is done, it's managed by the new solution? You'll need to figure that out.



Whether you're migrating to Entra ID or just another AD domain: Moving to Entra ID requires, in essence, completely starting over with a new endpoint, which contradicts your desire to “migrate” endpoints to Entra ID (more on this in a moment).

Each of these concerns equates to migration tasks that will need to be accomplished to ensure a secure and functional endpoint post-migration. We'll use the following three endpoint migration Use Cases to talk about some of the challenges you'll face, and then discuss what your options are to modernize your endpoints.



Endpoint Migration

Use Case #1: Moving to the Cloud

The Focus: Migrating the “Un-migratable” to Entra ID

So, your company has decided it’s time to take the plunge and move everything to the cloud—specifically, to Entra ID. This move is supposed to streamline operations, making it easier for everyone to work seamlessly whether they’re in the office or working remotely. But here’s the catch: natively, you can’t migrate an endpoint to Entra ID. Microsoft requires you to basically start with fresh endpoints (more on this in a moment) – obviously, not a great option.

Why Endpoints Matter Here

This isn’t just about copying over some files and calling it a day. If your organization is serious about staying productive, everything on a user’s current device – their settings, applications, and all those little tweaks they’ve made to make it feel like “theirs” – all needs to remain on the endpoint and be functional once the endpoint has “made the jump” to Entra ID. The last thing anyone wants is to lose precious time reconfiguring everything or, worse, starting over on a new machine that feels foreign.

What’s the Challenge?

In short, you can’t migrate endpoints to Entra ID. Microsoft’s “migration” recommendation is for you to wipe and reinstall each endpoint. That’s it – cut and dry. This means starting over, no migration of the user environment, and a terrible (and unproductive) user experience.

And If You *Don’t* Migrate the Endpoints?

Let’s be clear – skipping this step isn’t an option. If your endpoints (those laptops and desktops) don’t migrate, your team will be stuck in hybrid AD limbo, not truly able to utilize Entra ID. In other words: if you don’t, you aren’t truly moving to the cloud.

Endpoint Migration

Use Case #2: Mergers & Acquisitions

The Focus: Coexistence and Migration

Picture this: two companies have decided to tie the knot—whether it's through one acquiring the other or a full-blown merger. Naturally, the new, larger organization needs to bring everyone together under one roof, digitally speaking. But there's a tremendous amount of complexity here; each company has its own AD, hybrid, or fully-Entra ID environment and you've got to get endpoints moved (as part of a larger migration) and – at the same time – keep them working in this new super-complex coexisting environment until it's their turn to be migrated.

Why Endpoints Matter Here

In a merger or acquisition, the stakes are high. Teams from both companies need to keep working together without missing a beat. That means you need a way for employees to access and share the right data, applications, and tools both within the coexisting environment as well as whatever the new target environment will look like post-migration. It also means that at some point, you'll have to migrate everything—including user accounts and their devices—to the new, unified environment. And you've got to do it in a way that ensures the endpoint can be managed in both a coexistence and migrated state, adopts the security configurations necessary to be considered secure, and remains a productive tool for its user throughout the entire process.

What's The Challenge?

There are usually a lot of moving pieces with this kind of migration, making the managing of migration timelines, the maintaining of productivity during coexistence, the minimizing of migration errors, and the ensuring of a seamless user experience a difficult task – all things you'll need to address with whatever methodology and toolset you choose to utilize for the migration.

And If You *Don't* Migrate the Endpoints?

You're looking at a potential nightmare. Imagine trying to keep two different IT environments in sync *indefinitely*—policies start clashing, security holes start appearing, and before you know it, productivity is tanking because nothing works the way it should. Not to mention, keeping both environments alive for too long adds complexity and costs that no one wants. Simply put, staying in coexistence forever isn't sustainable. In reality, many of you are already there, having maintained multiple environments that have evolved somewhat uncontrollably into its current state – so you're feeling this pain already.

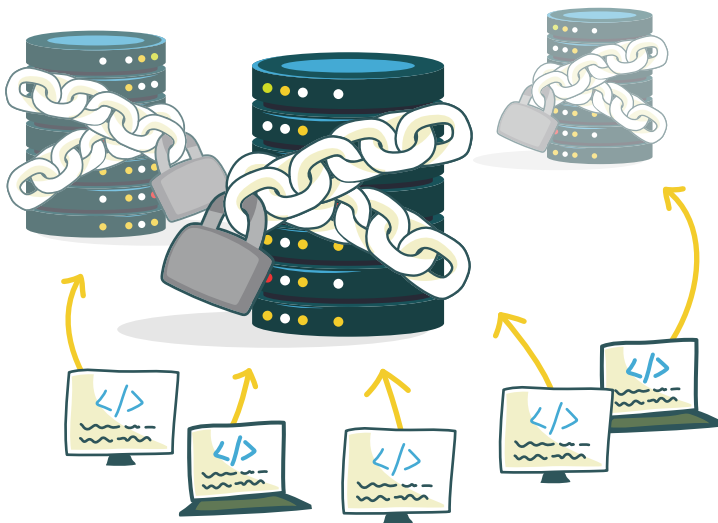
Endpoint Migration

Use Case 3: AD Modernization and Consolidation

The Focus: Endpoint Security

Let's say your organization has been around for a while, and over the years, you've collected a number of AD environments—maybe from old acquisitions, maybe just from teams doing their own thing. These environments have become a tangled mess of trusts, security, and management. Now, you've decided it's time to clean things up. The goal? Consolidate everything into a single, streamlined Active Directory (AD) or Entra ID environment. But it's not just about moving systems and permissions around; it's about making sure the new environment has a modern security stance while still keeping people productive.

The more environments you have, the messier things get. Each one comes with its own security settings, policies, and access controls, which can easily become outdated, misconfigured, or just plain insecure. Consolidating all these environments isn't just a nice-to-have—it's a must to reduce risks, simplify management, and ensure consistent security practices.



Why Endpoints Matter Here

As part of the effort to shore up your security through modernizing the environment, you've got to migrate everything – which includes your endpoints, as they likely pose a security risk as well that provide threat actors with initial access, persistence and control over the endpoint, and potentially access to privileged credentials that will facilitate lateral movement. So, the security of your endpoints equally needs to be assessed and addressed as part of the modernization efforts through migration.

What's The Challenge?

The assumption here is that you have years and years of security complexity build-up that needs to be unwound. Take Group Policy as an example: it's likely that no one in IT even knows what policies impact a given endpoint, requiring quite a bit of discovery. Now add in local admin group members, permissions that grant system-level access, and a myriad of other OS security configuration settings that somehow need to be all addressed using a singular means to turn that endpoint into one that meets the current security requirements of the organization via the modernization process.

And If You Don't Migrate the Endpoints?

It's really not an option – assuming you've already come to the conclusion you need to de-risk your Microsoft environment through modernization and consolidation, endpoints are along for the ride. And *not* migrating them means you're keeping the old environment in play – and that's a non-starter for the organization looking to improve its security stance.

Navigating to Seamless Endpoint Migration: What Are Your Options?

Whether in the context of moving to the cloud, merging organizations, or consolidating AD environments—migrating endpoints presents a complex challenge for IT teams. Regardless of the specific use case, the objective remains the same: to move devices from one computing environment to another while ensuring minimal disruption, maximum security, and operational efficiency. To achieve this, IT departments have a few different options at their disposal. Below, we explore these options, along with the pros and cons of each, so you can make informed decisions tailored to your organization's needs.

1

Manual Migration: The Traditional Approach

This involves IT teams physically or remotely touching each endpoint device to perform the necessary steps to migrate it to the new environment (keeping in mind that you can't do this in the case of migrating to Entra ID). This can include backing up user data, wiping and reinstalling the operating system, reinstalling applications, and reconfiguring settings to fit the new environment.

Pros	Cons
• Full control over every aspect of the migration process. • Highly customizable to specific needs, allowing for tailored configurations per endpoint. • Immediate troubleshooting capability during the migration process.	• Extremely time-consuming and labor-intensive, especially for organizations with hundreds or thousands of devices. • A complete lack of visibility into the migration's progress. • High risk of human error, which can lead to missed configurations, lost data, or other issues. • Significant disruption to end users as they may be without their devices for extended periods. • Inefficient use of IT resources and increased costs due to the time and labor involved.

Who Is This Best For?

Small organizations with limited endpoints or scenarios where very specific, customized configurations are required that cannot be automated.

2

Using Microsoft's Native Tools: Partial Automation with Limitations

Microsoft provides several native tools (e.g., the User State Migration Tool) designed to help automate parts of the migration process. These tools can handle tasks like moving user accounts, synchronizing settings, or deploying new applications across devices.

Pros

- Reduces the manual effort required from IT teams by automating specific tasks.
- Familiar tools that integrate well within Microsoft-centric environments.
- Cost-effective for organizations already using Microsoft 365 and related services.

Cons

- Not an option for moving to Entra ID.
- Limited in scope; may not cover all aspects of a complex migration (e.g., third-party application settings, specific user configurations).
- Can require significant setup, scripting, and customization to work effectively for each environment.
- Lacks flexibility when dealing with non-Microsoft applications or specific organizational needs.
- Still may require a manual or semi-manual effort to handle tasks that the tools don't support.

Who Is This Best For?

Organizations heavily invested in Microsoft environments looking for partial automation to reduce manual effort, particularly for simpler migrations between AD environments.

3

Wipe and Reinstall: A Clean Slate Approach

This method, recommended by Microsoft for organizations moving to Entra ID, involves wiping the entire device clean—removing all data, settings, and applications—and reinstalling the operating system from scratch in the new environment. After the reinstall, user data and settings can be manually restored, either from a backup or by reconfiguring the system.

Pros

- Ensures a fresh start, eliminating any legacy configurations, potential malware, or corrupted files from the old environment.
- Can be relatively straightforward for experienced IT teams with strong scripting capabilities.

Cons

- Users lose their personalized environment (custom settings, apps, files not backed up), leading to potential productivity loss and frustration.
- Time-consuming and disruptive for both IT and users, especially when personalizing configurations must be redone.
- Not practical for large-scale migrations due to the high volume of effort required for each endpoint.

Who Is This Best For?

Scenarios where security is paramount, and a completely clean start is needed to prevent any issues from carrying over from the old environment.

4

Third-Party Migration Tools: Comprehensive Automation Solutions

Third-party solutions, such as Quest On Demand Migration (ODM), provide comprehensive, end-to-end migration capabilities that go beyond what native tools can offer. These solutions focus on automating the migration process while ensuring minimal user disruption and preserving the integrity of user settings, profiles, and applications.

Pros	Cons
• Full automation of the migration process, drastically reducing manual effort and human error. • Preserves user profiles, applications, configurations, and settings, minimizing disruption and maintaining productivity. • Provides centralized management and visibility for large-scale migrations, handling thousands of endpoints efficiently. • Enhanced security and compliance features that address vulnerabilities during and after migration.	• Requires investment in third-party software, though it can save time and costs in the long run by reducing IT overhead. • Learning curve for IT teams to fully leverage the tool's capabilities.

Who Is This Best For?

Medium to large organizations with complex environments or a high volume of endpoints to migrate. Particularly effective for scenarios where maintaining user productivity and security during migration is critical.



CHOOSING THE RIGHT MIGRATION PATH



For IT teams, the decision on how to migrate endpoints involves weighing the trade-offs between time, cost, control, and user experience. While manual methods and native tools may suffice for smaller environments or less complex needs, most organizations will benefit from the comprehensive, automated approach offered by third-party solutions like Quest On Demand Migration. By choosing the right strategy, IT can ensure a smooth, secure, and efficient migration that meets both organizational goals and user expectations.



Quest On Demand Solutions

Platform changes and merger and acquisition (M&A) activity are occurring more frequently than ever before. If you have Microsoft 365 and you see M&A activity in your future, you will need to consolidate tenants. On top of that, like many companies, you're likely on course to move more of your systems and processes to the cloud to support your increasingly mobile workforce. Only with Quest can you take advantage of more than 20 years of expertise migrating, managing and securing Microsoft platforms — all through an Azure-hosted Software as a Service (SaaS) portfolio. We can help accelerate your quest to Entra ID and Microsoft 365.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

For more information, visit: www.quest.com/products/on-demand-migration