Migrating from Windows 10 to Windows 11:

A Guide for IT Project Managers

Macrium Software
www.macrium.com

Migrating from Windows 10 to Windows 11: A Guide for IT Project Managers

Table of Contents

Understanding Windows 10 End of Life

After a decade of working with Windows 10, the operating system we've grown so accustomed to and have used on a daily basis will reach end-of-life in October 2025. Beyond this point, Microsoft will no longer offer technical support, software or security updates for those continuing to use Windows 10.

Why not remain on Windows 10?

There's technically nothing stopping you from clinging on to Windows 10. Just like there's nothing stopping you from driving an old car. But eventually, like all unsupported technology, it'll let you down. Here are just some of the obstacles your IT team and business will face if you continue to use Windows 10 beyond its sunset date.

- Unpatched security vulnerabilities will leave you exposed to malware attacks and data breaches. With ransomware more prevalent than ever and cyber criminals taking every opportunity to exploit vulnerabilities in your software and systems, this is a significant risk for any business to take.
- You'll experience compatibility issues with new hardware and software that either doesn't work, or partially works until something goes wrong.
- Because Windows is an operating system (OS), not just a piece of functional software, you may lose vendor support for other pieces of software.
- Governance could catch up with you. You may encounter compliance issues with industry regulations that mandate the use of supported software to protect sensitive data.
- When things don't work properly, it's not just IT that suffers. The whole business could become less productive and its people demotivated. This can also affect your appeal as an employer: the brightest talent expects, rather than hopes for, functioning software and hardware in their workplace as standard.
- Finally, fixing old software eats up IT resource, which could be better used on core business activities and innovation.

The Benefits of Migrating to Windows 11 Sooner, Rather than Later

Should you bite the bullet and commit to your Windows 11 migration sooner rather than later, there are plenty of good reasons to make the transition.

Performance: Windows 11 is designed with the modern workplace in mind. It offers features like improved multitasking, a more streamlined and user-friendly interface and enhanced compatibility with the latest hardware.

Currency: Microsoft's current focus is rolling out new features to Windows 11; and is winding down its work on Windows 10. As PC World notes, "The last two feature releases have basically passed over Windows 10, relegating the new features to Windows 11 only."

Security: From a security standpoint, Windows 11 introduces state-of-the-art security features and enhancements that continually improve your business' cyber resilience. These include Windows Hello identity protection, biometrics to eliminate the weakness of passwords, on-chip hardware defenses and more layers of application protection.

AI: No discussion around today's trends would be complete without a nod to AI. Microsoft Copilot is not only a powerful AI tool, it's also seamlessly embedded within Windows 11. If you don't upgrade, your business and employees risk being left behind by this integral technology of the future.

Migrating to Windows 11 is no overnight task, though - especially for organizations with a substantial number of machines or those spread across multiple locations. And you may think that October 2025 is way out on the horizon; but the larger your organization, the more important it is to make a start now.

The migration process requires thorough planning, preparation and testing to ensure a smooth transition for your teams and business. This will include preparing your IT infrastructure and developing a comprehensive migration strategy that minimizes downtime, mitigates operational disruption and keeps your people productive throughout.

Start Your Engines: How to Prepare for Migration

As the old adage goes, “fail to plan, plan to fail”. The effort your business will need to put into pre-migration planning will be significantly more than what’s required to execute the migration itself.

Appoint your Windows 11 Migration Team

An effective migration cannot be left to the last minute. Your timeline for migration planning will depend on the size of your estate, number of users and application complexity. Larger organizations should bring together a team with multiple appropriate skills and responsibility for the migration 9-12 months ahead of time. Smaller businesses may have a little less work to do, but they are also likely to be less well-resourced in-house, which will put pressure on day-to-day delivery and may require that you get outside help from an agency or consultancy. Therefore, whatever the size of your business, a longer planning horizon can only be a good thing.

You’ll want to begin with a kick-off meeting which brings internal and external resources together, assigns roles and responsibilities and establishes the scope of the project. The team also cannot work in isolation: it must put effort into recognizing the effect of the migration on BAU and understand the needs of departments and key stakeholders across the business. For the duration of the project, it will also be up to this team to maintain a consistent drumbeat of communication, making users aware of what they will have to do, any inconvenience they can expect and the good news of progress made.

Your team should therefore include a mix of IT experts - who will do the work - and broader stakeholders who will keep the business aligned with the project's progress:

- **Sponsoring Stakeholders:** your link with business leadership.
- **Programme Management:** leading the migration team.
- **Infrastructure:** whatever specialists you need to understand your cloud, hybrid and local network infrastructure.
- **Deployment Engineers:** your dedicated deployment team, with the skills to manage the heavy-lifting of Windows and application migration across a large number of devices.
- **Application Experts:** to deal with testing and any ongoing compatibility work required to keep your applications running – particularly if you have in-house-developed tools.
- **Communications:** for two-way dialogue with users across the business.
- **Security / CISO:** the guardian of data and business protection throughout the process.

Conduct a Readiness Assessment

A readiness assessment is the natural first step to planning your Windows 11 migration. It involves evaluating the current state of your organization's IT environment from both a technology and user perspective, in order to prepare for the migration.

The assessment will ensure that your hardware and software are compatible with the new operating system. It will identify any potential challenges and solutions early in the process. According to Computacenter, around 5% of business-critical applications will need some sort of remediation to operate under Windows 11.

The Anatomy of a Readiness Assessment

Here's the structure of a typical readiness assessment.

- **Inventory your Current IT Assets:** Begin with a comprehensive inventory of your IT assets. This includes all hardware devices, installed software applications and network infrastructure components.
- **Check Hardware Compatibility:** Compare the hardware specifications of all devices in your environment against Windows 11's minimum system requirements. There was a time when this was easy because your hardware view was end-to-end. But now that many users bring their own devices into the work environment, things might be trickier. Most of all, recognize that Windows 11 requires 64-bit machines. The days of support for older x86 processor units are over.

HARDWARE REQUIREMENTS FOR WINDOWS 11

Processor	Minimum 1GHz with two or more cores on a compatible 64-bit processor.
Memory	Minimum 4GB.
Storage	Minimum 64GB available disk space (more will be required for updates).
Graphics card	Compatible with DirectX12 or later, with a WDDM 2.0 driver.
System firmware	UEFI, Secure Boot capable.
TPM	Version 2.0.
Display	Minimum 720p HD display, on a screen 9" or greater monitor.
Internet	Connection required for updates and to use some features.
Installed Software	Unit must be running Windows 10, v2004 or later, with a minimum security update currency of September 14 2021.

A complete list of requirements can be found here.

- **Check Software Compatibility:** Work with your key software vendors to get their Windows 11 compatibility statements and their plans for any updates of non-compatible applications. Old tools which are not going to be updated will need to be replaced and that can be painful for users. For in-house developed applications, testing will be required to ensure they function correctly on the new OS.

TESTING... TESTING...

With millions of pieces of software on the market, it's impossible to offer assurance as to which will work on Windows 11 and which won't. All major software providers will have long established their Windows 11 compatibility, so most firms will have nothing to worry about.

If you do encounter incompatibility, all is not lost. This is the sort of work that you should be doing on testbed machines prior to any upgrade process. There are two useful options to consider:

1. If an application installs but is incompatible with Windows 11, there's a compatibility checker which should identify (if not fix) the problem. Right-click the app's shortcut, select 'Properties', then the 'Compatibility' tab and select 'Run Compatibility Troubleshooter'. The Troubleshooter should present you with fixes for software incompatibilities.
2. In developer mode (Settings > System > For Developers), you can run software from outside the Microsoft Store environment without the usual protective guiderails. This developer environment may solve your issue, or at least find a way forward.

- **Network Readiness and Security:** Assess your network infrastructure and security policies to ensure they can support Windows 11. This will include compatibility with new security features and support for new authentication protocols. Microsoft advises, "Before you deploy Windows 11, assess your deployment infrastructure (that is, tools such as Configuration Manager, Microsoft Intune, or similar) and current configurations (such as security baselines, administrative templates and policies that affect updates). Do the tools themselves need to be updated? Do you have the right settings and policies defined to support devices once Windows 11 is installed?" Your network should not be challenging in this respect. It's more important that it's ready to support new features in Windows 11 so your systems are as secure as possible.
- **User and Device Control:** Determine how Windows 11 will integrate with your existing policies and controls. This includes the group policy objects (GPOs) by which you define permissions and use cases for multiple users and mobile devices.

The result of this effort should be a clear understanding of the devices and applications that are ready for migration. It should also expose those that require updates or replacements and any potential risks or issues (operational, mission-critical, security etc.) identified during the assessment. This will, in turn, feed discussions on timelines, process and, of course, budgets, ultimately leading to:

- **Pilot Deployment:** A proof-of-concept deployment to a small subset of devices – more than one (to test rollout at scale), across more than one department, location or configuration (to test multiple environments). But a small enough number of units not to compromise the operation in the event of total failure. Microsoft offers the following advice for a pilot:

INGREDIENTS OF A PILOT ROLLOUT OF WINDOWS 11

- Assign a group of users or devices to receive the upgrade.
- Implement baseline updates.
- Implement operational updates.
- Validate the deployment process.
- Deploy the upgrade to devices.
- Test and support the pilot devices.
- Determine broad deployment readiness based on the results of the pilot.

Microsoft, "Prepare for Windows 11"

Back up for a Moment…

Your readiness assessment will generate a workable migration plan. From this you can work towards October 2025 (or sooner) with confidence. It should also be economical – with expenditure based on the specific needs of the business.

But one-off change presents one-off risks. Not least because no major software migration goes so seamlessly that every device, laptop and data source carries on working without a hiccup.

Develop a Backup and Recovery Plan

It's therefore essential that you have an effective backup and disaster recovery plan in place. Ideally, this is part of your BAU. The thought you put into your Windows migration can be leveraged to become part of the fabric of your everyday IT management. Failing that, it will give you confidence that you're following best practice when it comes to backup and disaster recovery for the duration of this one-off activity. Here's how:

- **Dust off the IT Asset Inventory:** This time, we're not just looking at hardware and software/applications, but also data. What are your classes of data (customer, financial, intellectual property…), how and where are they kept and how rapidly would you need access to them in the event of a migration problem? Your corporate data systems will likely be irrelevant for a Windows end-user migration, but the question remains: who uses what data on which devices?

- **Develop your Risk Approach:** Create a clear disaster recovery strategy based on recovery point objectives (RPOs) and recovery time objectives (RTOs). Your RPO is the maximum amount of data – measured by elapsed time – that can be lost to full recovery from a failure before data lost exceeds what is operationally acceptable. Your RTO is the maximum acceptable amount of time for restoring your data after an unplanned disruption.

- **Determine Your Backup Requirements:** Understand the frequency at which data changes to determine your ideal backup intervals (see RPO and RTO above). Laptops will be unlikely to need real-time backups. But your backup regime should recognize that it may take a few days to fully execute the migration and daily incremental backups will probably be needed. Ensure that your solution of choice offers appropriate encryption and complies with regulations and standards. Plus, ensure your solution is compatible with both Windows 10 and Windows 11 to facilitate a smooth migration. Macrium Reflect is not only effective and fully compatible from Windows XP through to 11, it can be deployed from one dashboard across multiple sites and devices.

WHY BACKUP ON-SITE?

- **Compliance:** In many regulated industries, on-site backups are essential for compliance purposes.
- **Speed:** Backup and restoration of large amounts of data (like hundreds of users' work) will always be faster on-premise than to and from the cloud.
- **Security:** Data in transit is always more at risk than data at rest, and the further it travels across systems over which you have no control, the higher the risk.
- **Cost:** Data transit fees are the basis of cloud billing, whereas local storage has zero transit fees. A major migration to and from the cloud could be exceptionally expensive.
- **Reliability:** Onsite backups files are less prone to errors in images as cloud backups are prone to data drops which ultimately affect whether an image can be recovered from.

It's also worth investing in more than one backup, particularly at points of weakness, for redundancy if one type of backup is inaccessible. A popular approach is the "3-2-1 backup strategy":

- **Three Copies of Your Data:** the original data plus two backups. This ensures that if one backup fails, you have another to fall back on.
- **Two Different Types of Storage:** to protect against device failure from the same type of hardware malfunction.
- **One Backup stored Off-site:** to protect against the risk of physical damage (like fire, theft, or natural disaster) which could affect all local copies.

> *"Macrium Reflect allows our business to focus more effectively, reducing the risks associated with data loss and downtime. This gives our clients peace of mind that their systems and data are available to them when they need them most."*
>
> **Martin Paul, IT Works**

- **Implement your Backup Solution:** Install and configure backup software on all systems and devices, and make sure users know what's happening and anything they need to do. This should require as minimal changes to their existing processes as possible. Automate and schedule wherever you can, so that backups need no manual intervention.
- **Testing and Verification:** Conduct regular tests – especially in the months leading up to your migration point – to ensure that schedules work and backups can be restored successfully. Regularly check the integrity of backup files to ensure they're not corrupted and can be restored when needed.
- **Write Everything Down:** Document your backup and disaster recovery procedures, including step-by-step restoration processes.
- **T-Minus-Zero:** At the point of migration, conduct a full backup of all systems before starting the move to Windows 11. Because you've installed, tested and used your migration process for several weeks, this should be a simple process rather than a surprise for everyone!

Your Trusted Partner in Windows 11 Deployment

Looking for a stress-free way to migrate to Windows 11?
Macrium SiteDeploy makes deploying at scale a breeze! Book a demo of our powerful SiteDeploy software, and let our experts show you how we can help you with a quick and stress-free migration to Windows 11.

BOOK A DEMO

The Migration Process

We haven't talked much about the migration process itself so far. That's because it will differ according to the scope and scale of your IT estate.

Some businesses will be able to execute an in-situ upgrade – effectively following prompts within Windows 10. This will only really be applicable for smaller businesses, and only available to those where all devices meet a fairly strict set of criteria for modernity of hardware and software. After all, upgrading from Windows 10 to Windows 11 is relatively simple; the idea of an in-situ upgrade from Windows 7 to Windows 11 is non-sensical.

But if you're running just 20 machines rather than 200; and all of them were set up in the past couple of years, then an in-situ upgrade may be possible and desirable for simplicity. Access it via Settings > System Update.

If not, you'll need a Golden Image – the base configuration which you intend to replicate across your other machines.

Preparing Your Golden Image

Your golden image should be an optimally functional copy of the operating system, apps, software and settings that your corporate devices need to function effectively. As well as the OS, it will include applications, drivers, standardized configurations, a set of default security measures and policy settings. Any customizations users need can be made after the migration – tools like Microsoft Autopilot can further automate this if you're working on a large number of devices.

The key benefit of a Golden Image is that it can be configured to adhere by default to your in-house governance, compliance and security standards. We find that most businesses running in-house IT for governance reasons have more stringent operational standards; and those can be embedded in your Golden Image. Similarly, while nobody wants to admit that rules get bent, your Golden Image is also an opportunity to return to enforcement of your standards where some employees might have pushed the boundaries.

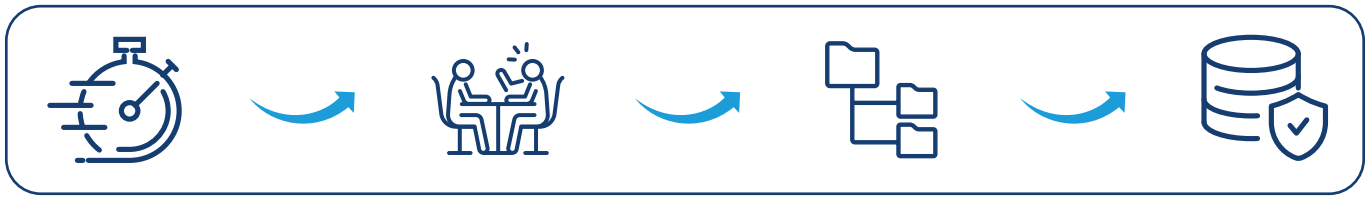
To create your Golden Image:

- On a typical machine running Windows 11, set it up with all the applications you want to include in the Golden Image, plus any configurations, current updates etc.
- Run Sysprep (Win-R > "SysPrep") and select OOBE > Generalize. Sysprep prepares the system for imaging by removing all elements of Windows specific to the donor machine, effectively creating a "blank" version of your ideal configuration.
- After shutdown, reboot this donor machine using Macrium Reflect to create an image of the entire reference machine – this is your Golden Image.

It's vital to conduct exhaustive testing of the Golden Image and its settings against your infrastructure to verify that everything works in a real-world scenario. Deploy it on a collection of varied QA machines before the wider rollout.

On the day…

Always perform major upgrades out-of-hours. If you have a large IT estate, run the upgrade over a weekend. Ideally, have some hot-swappable machines available for home-working or in case of overrun on the Monday morning.



Your upgrade day also needs to have been well communicated to all employees – there's nothing worse than your whole upgrade team working a weekend at great expense, only to find that half of your employees have taken their laptops home…

When you're ready to execute, Macrium SiteDeploy will be your new best friend. Once devices have been rebooted into the deployment environment, SiteDeploy makes restoring your golden image to multiple machines fast and simple. Even when deploying across multiple locations, disparate networks and to a wide range of devices, from laptops and PCs to servers.

It ensures that when you deploy Windows 11, the process is smooth. Sector level Golden Images ensure that the target endpoint devices are an exact copy of the reference machine where the Golden Image was created, regardless of discrepancies and variables in each device's hardware setup. Macrium SiteDeploy scales that uniformity across your estate, making deployment as fast, reliable and uncomplicated as possible.

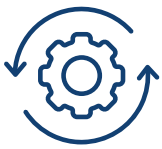
Tips for Success

OS migrations are among the most complex and lengthy projects an IT professional can face. Instead of looking for perfection, think about risk mitigation. Anything you can do to reduce risk and complexity is a good thing. Here are some key points to consider.

Plan, Plan and Plan Some More: The foundation of any successful migration is meticulous planning. Understand the compatibility between your current and future environments. Establish a detailed project timeline, complete with milestones and deadlines, to ensure that all stakeholders are on the same page. This will mitigate risks associated with time and scope creep.

Work Across Departments to Prepare, Train and Onboard Users: An OS update will affect everyone in your organization - from the top table to the shop floor. To successfully prepare, train and onboard users across the business, work collaboratively with key stakeholders to ensure the changeover and subsequent weeks go as smoothly as possible.

…And Keep Talking: Effective, well-timed communication is crucial throughout the migration process and beyond. Keep all stakeholders informed about progress, potential impact and scheduled downtime. A well-informed team will accept change more readily and adapt more quickly, reducing the risk of disruption. Digital Information World says, “Windows 11 introduces new features and a different user interface compared to previous versions. Provide end-user training and documentation to help employees familiarize themselves with the changes and maximize productivity.”



Automate Everything You Can: Not just because it makes life easier, but because manual processes during an intricate upgrade path are a recipe for human error. Use migration tools that automate repetitive tasks, such as data transfer and application deployment. Automation also facilitates continuous integration and delivery (CI/CD) processes, enabling faster deployment cycles and more efficient use of resources.

Dotting the ‘i’s: After Migration

Migrating from Windows 10 to Windows 11 in businesses with complex user communities doesn’t stop with the migration process itself. Post-migration diligence ensures that the transition won’t disrupt operations, compromise security or hinder productivity. Here are some of the considerations you should prioritize.

Basic Post-Migration Audit:

Conduct a thorough audit of all migrated systems to ensure applications have been accurately transferred and that there are no discrepancies or losses. Spiceworks advises, “While Microsoft states that Windows 11 will support any application currently supported by Windows 10, it’s best to trust but verify. It would be best if you were extra diligent about running Windows updates to fix the undiscovered bugs that could appear once large-scale rollouts begin.”

Security Baseline Review:

Immediately after migration, establish a new security baseline for your Windows 11 systems. Make sure all security software is working and updated. Apply the latest security patches from Microsoft and configure all relevant Windows 11 security features (e.g. BitLocker for disk encryption, Windows Defender for malware protection and Windows Hello for secure authentication).

Re-evaluate Access Control:

Review your user access controls to ensure that only authorized personnel have access to sensitive data. This may involve setting up new group policies or adjusting existing ones to align with Windows 11's security framework s. Similarly, remember that your backups are sensitive data too – make sure network backups are appropriately secured. Offline physical backups should be locked away (e.g. in a safe) and ideally in a different location.

Regular System Monitoring and Auditing Program:

Implement regular system monitoring to ensure ongoing compliance with security policies and to identify any issues before they become serious problems.

Automated Updates:

Activate automated update policies for Windows 11. These will keep your systems up to date with the latest features and security patches with minimal effort. This can be achieved via Windows Update for Business or management tools like Microsoft Endpoint Configuration Manager. They'll also allow you to schedule updates during off-peak hours to minimize disruption.

Revisit your Disaster Recovery Plan:

Update your business continuity and disaster recovery plans to include Windows 11-specific advancements. Consider the use of offline backups and system imaging via Macrium Reflect (which is well supported within Windows 11) to provide additional layers of redundancy and protection.

> ***"Data is priceless, you can't recreate it. I can tell you that Macrium Reflect pays for itself compared to other products. It's been a great solution for us."***
>
> **Damon Dawson, Senior Network Engineer**

Those are the technical considerations, but your users may also need some assistance in the weeks post-migration. Offer them training and enhanced support tailored to their varying levels of tech proficiency. This should comfortably pay for itself in reduced support calls.

Establish a temporary helpdesk or support code for post-migration issues and questions. Implement a feedback loop with users to identify challenges they face in the new environment. This feedback will be invaluable for refining training materials and support services. More importantly, it's how you'll identify deficiencies which have slipped through the net and which prevent employees from working.

It Has to Happen – So Make it Stress-Free...

Migrating from Windows 10 to Windows 11 is not negotiable. It's an essential step forward to keep your organization efficient and secure. It will keep you compliant with current technological best practice and will improve employee experience in the long-term.

Windows 11 not only offers enhanced performance, security features and compatibility with modern hardware. It also integrates innovative tools like Microsoft Copilot, designed to keep your corporate technology updated and your teams as productive as possible.

Out With the Old, In With the New

As Windows 10 approaches its end of life, the vulnerabilities and lack of support pose significant risks that can hinder business operations and expose sensitive data.

The question is: do you want to upgrade on your terms – planned, efficient, pain-free – or at the last minute?

The Windows 10 to 11 migration process requires thorough planning, assessment and testing to ensure a smooth transition. Starting early means you'll be able to give this work the meticulous attention it deserves, minimizing operational disruptions and complexity for you and your end users.

How Macrium SiteDeploy can ensure a smooth migration

At Macrium Software, we have been helping our customers safeguard their data for almost two decades. That means both protecting the everyday flow of work and supporting complex mission-critical projects like OS migrations.

- **Macrium SiteDeploy** is one of the fastest and most easy-to-use imaging and deployment solutions available, cutting the need for extra operational training and budget. Through SiteDeploy and its central console, you can view, manage and deploy Windows 11 to all your devices in just a few minutes, making migration painless and stress-free.
- **Macrium Image Guardian (MIG)** adds a new layer of protection to your migration process. OS changeovers can add new risk to your systems and leave them exposed to threat actors. MIG is a feature of Macrium Reflect, Site Manager and SiteDeploy. Granting write access only to Macrium tools, MIG blocks unauthorized modifications to your backup files, making it virtually impossible for malware, such as ransomware, to access your backups.

Your Trusted Partner in Windows 11 Deployment

Looking for a stress-free way to migrate to Windows 11? Macrium SiteDeploy makes deploying at scale a breeze! Book a demo of our powerful SiteDeploy software, and let our experts show you how we can help you with a quick and stress-free migration to Windows 11.

BOOK A DEMO