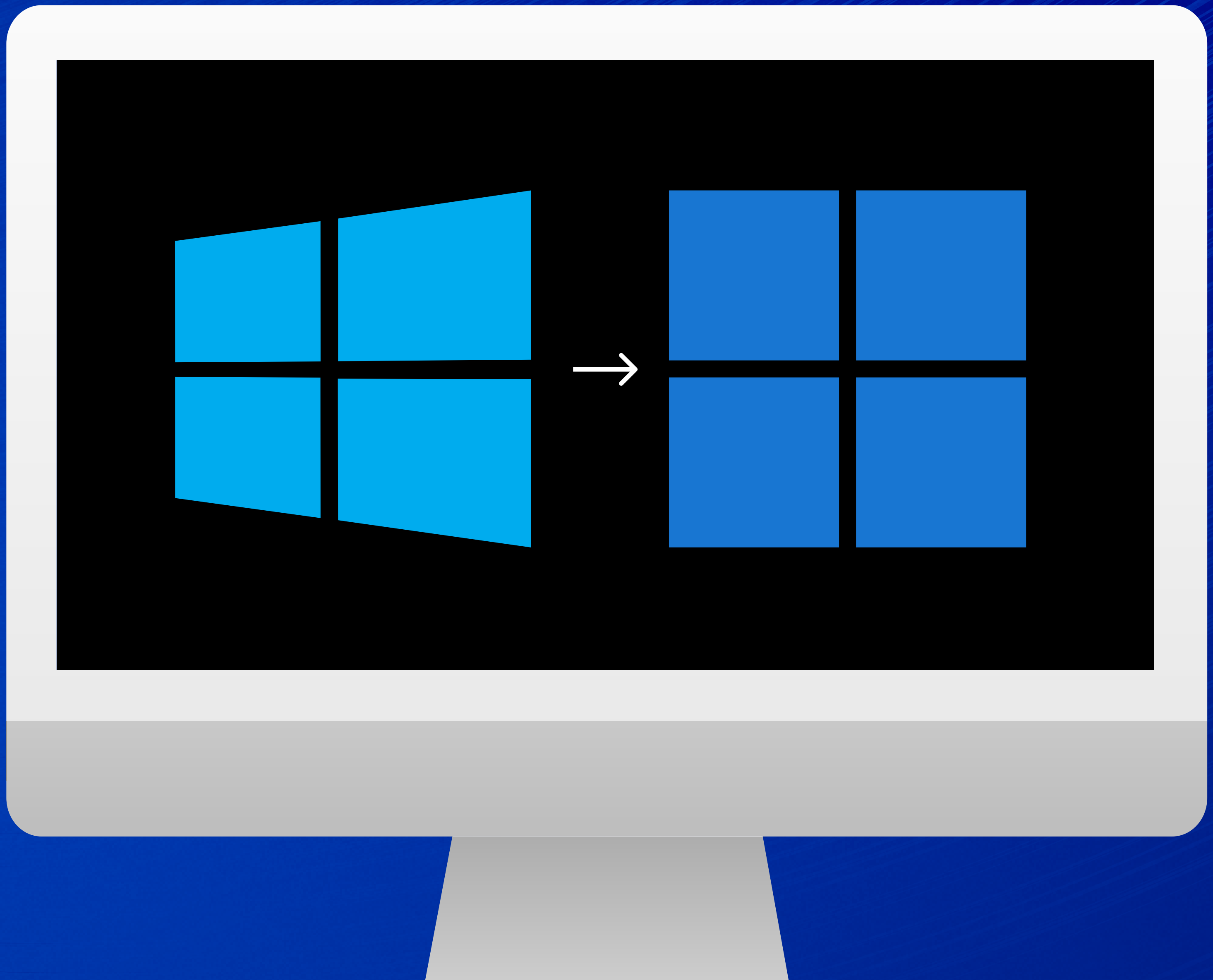
From Windows 10 to 11

A comprehensive guide to seamless migration with Endpoint Central.



ManageEngine
Endpoint Central

Table Of Content

01

Introduction

- The move from Windows 10 to Windows 11 is a significant upgrade, offering improved user experiences, performance, and security, making it crucial for organizations to stay current in the digital transformation era. It’s estimated that around 62% of the 1.6 billion Windows PCs globally are running Windows 10. This translates to approximately 992 million devices that are eligible for an upgrade to Windows 11.

- Windows 11 features a streamlined interface, better multitasking, and enhanced security, but the transition to it can be challenging due to hardware and software compatibility concerns. This white paper serves as a comprehensive guide for organizations considering the upgrade, outlining its benefits, its challenges, and the best practices for a smooth transition. After October 14, 2025, Microsoft will no longer provide free software updates from Windows Update, technical assistance, or security fixes for Windows 10. IT administrators face the urgent task of migrating systems to Windows 11, navigating various scenarios to ensure a successful migration.

02

An overview of Windows 11

Windows 11, released in October 2021, is Microsoft's newest OS. It has a revamped Start menu and taskbar, modern design elements, improved performance and gaming capabilities, virtual desktops, Microsoft Teams built in, a widgets panel, enhanced inputs, stricter hardware requirements, and advanced security. It aims to create a seamless, efficient user experience across devices.

Advantages

- **A revamped UI:** A centered taskbar, a new Start menu, and improved window management with Snap layouts and groups
- **Performance boosts:** Faster boot times and enhanced memory and resource usage
- **Advanced security:** Hardware-based isolation and Trusted Platform Module (TPM) 2.0 for protection against threats
- **Virtual desktops:** Better management for different tasks
- **Gaming upgrades:** DirectStorage and Auto HDR for a superior experience
- **An improved user experience:** A redesigned interface and features for better organization and productivity
- **Enhanced security:** Advanced measures to prevent vulnerabilities
- **Access to new tools:** New applications for collaboration and productivity
- **Better hardware support:** Optimized for the latest technologies for better compatibility and performance

Disadvantages

- **Stricter hardware requirements:** Windows 11 has stricter specifications, like TPM 2.0 and Secure Boot, making it incompatible with older devices.
- **A difficult learning curve:** The redesigned Start menu and taskbar may confuse users familiar with previous versions.
- **Software incompatibility:** Older applications may not work properly, causing issues for businesses or users.
- **Lower performance on older hardware:** Windows 11 may run slowly on older hardware due to new features.
- **Limited customization options:** Compared to previous versions, there are fewer customization options for the taskbar and Start menu.
- **Bloatware and preinstalled apps:** Windows 11 comes with preinstalled apps that can clutter and use up system resources.
- **Updates and changes:** Frequent updates can disrupt workflows and introduce new issues.
- **Gaming limitations:** Some gaming features require an internet connection or online activation, which is a disadvantage for users with limited connectivity

03

Steps to check devices' compatibility with Windows 11 using Endpoint Central

To assess devices' compatibility with Windows 11 using Endpoint Central, you can follow these steps to evaluate the hardware and software setups of your devices. Using Endpoint Central, you can gather the necessary information through the inventory and reporting features.

Here’s how:

- Go to **Inventory > Computers** to view the list of managed devices.
- Go to **Inventory > Inventory Reports > Hardware Reports > Windows 11 Readiness** to view the list of Compatible Devices along with their OS version, OS license status, free space, firmware type, etc.

In the case of devices that are found incompatible with Windows 11, refer to the section outlining strategies that can be followed to resolve hardware and software limitations to make them upgrade-ready.

04

Pre-migration checklist for Windows 11 with Endpoint Central

- Ensure critical data is backed up using Endpoint Central's backup solutions or third-party tools. Use a Folder Backup configuration to back up a machine's files and folders.
- Update all devices to the latest Windows 10 version and apply critical updates. Check out the document for Windows 10 deployment.
- Use the patch management features to update any incompatible patches.
- Use the Software Deployment module to install or uninstall any incompatible software.
- Export BitLocker details by going to **Reports > Inventory Reports > Security Reports > BitLocker Details.**
- Inform users about the upcoming migration, including timelines and new features, by going to **Tools > Announcement.**
- Upgrade the firmware of transitioning devices from the legacy BIOS to the UEFI for Windows 11 migration by verifying and installing specific updates provided by the device manufacturers according to their instructions. Ensure hardware compatibility, UEFI support, and proper hardware initialization and update the BIOS and drivers using the patch deployment features.
- Ensure your Windows 10 edition and product key are compatible with Windows 11. Link your digital license to your Microsoft account and stay updated on licensing and activation for Windows 11. Ensure your current edition (Home or Pro) is compatible and consider upgrading or obtaining a new license if you're using the Enterprise or Education edition.

05

How to upgrade to Windows 11 using Endpoint Central

Upgrading to Windows 11 using Endpoint Central involves a series of steps to configure and deploy the upgrade across your organization's devices. Here are several methods to help you through the process:

Software deployment

- Endpoint Central supports deploying Windows 11 upgrade executables (e.g., ISO files or the Windows Update Assistant) through its Software Deployment features. The upgrade can be scheduled, and progress can be tracked on all devices.

Patch management

- Endpoint Central allows you to deploy Windows 11 patches (including feature updates) to endpoints automatically through its patch management features. You can configure schedules for patch installations or apply patches in bulk to ensure all devices are upgraded to the latest Windows 11 version.

OS deployment (upgrade)

- Using OS Deployer, you can deploy Windows 11 upgrade packages to multiple machines from a central location. Endpoint Central allows you to create upgrade packages based on the specific Windows 11 version you wish to deploy.

- Additionally, Endpoint Central enables you to create bootable USB drives for offline Windows 11 upgrades when remote upgrades are not feasible or a fresh installation is needed.

Remote installation

- If needed, administrators can manually initiate Windows 11 upgrades on remote machines using the remote control feature of Endpoint Central, which allows administrators to initiate OS upgrades across machines remotely.

Post-upgrade verification

a. Check the migrated devices listed under **Reports > Inventory Reports > Hardware Reports > Computers by OS** once the successive asset scan is completed.

b. Check for and install any available updates for Windows 11 under **Threats & Patches > Patches > Missing Patches.**

c. Ensure that all critical applications are functioning properly. Use Software Metering to monitor the software usage.

d. Use the reports under **Reports > Inventory Reports > Security Reports** to confirm that Windows Security features (like Windows Defender and Firewall) are enabled and properly configured.

e. Continue to monitor devices for performance, compliance, and security issues using Endpoint Central's reporting tools.

f. Verify that all devices are functioning correctly after the upgrade is complete.

g. Check for any application compatibility issues and ensure user settings are preserved.

Compliance and reporting

- Use the reporting features in Endpoint Central to monitor upgrade compliance. Generate reports to track the status of the upgrade across your organization.

Optional practices to consider for the upgrade process

- **Testing:** Before deploying widely, consider testing the upgrade on a small group of devices to identify potential issues.
- **User training**: Provide resources or training to help users acclimate to the new Windows 11 features and interface.
- **Backups:** Ensure critical data is backed up before the upgrade to prevent data loss.

By following these steps, you can efficiently manage the upgrade to Windows 11 using Endpoint Central, ensuring a streamlined, organized deployment process across your organization.

06

Troubleshooting steps and how to fix Windows 11 migration failures

Some common issues that users may encounter when upgrading to Windows 11 include failing to meet system requirements, experiencing installation difficulties, having performance issues, needing driver updates, managing storage space, dealing with the Start menu search bar, addressing File Explorer memory leaks, and resolving gaming issues. If you encounter migration failures when upgrading to Windows 11, here are some troubleshooting steps and solutions to resolve common issues:

1. **Check for compatibility issues**

- **Check the system requirements:** Verify that the device meets the minimum hardware requirements for Windows 11 (e.g., TPM 2.0 and Secure Boot).
- **Use the PC Health Check app:** Run the PC Health Check app to identify specific compatibility issues.
- For more information, please refer to this Microsoft document.

2. **Make sure there is sufficient disk space**

- **Free up space:** Ensure there is sufficient free space on the system's drive (at least 64GB). Delete unnecessary files or use Disk Cleanup to remove temporary files using Endpoint Central's File Folder Operation configuration.

3. Check for corrupted Windows update components

- **Run the Windows Update Troubleshooter:** Go to **Settings > Update & Security > Troubleshoot > Additional troubleshooters**. Select Windows Update and run the troubleshooter.
- For more information, please refer to the Windows Update Troubleshooter document.

4. Check for driver issues

- **Update drivers:** Ensure all drivers are up to date, especially for graphics and network components. Use Device Manager or manufacturer websites to download the latest drivers.
- **Uninstall incompatible drivers:** Remove any known incompatible drivers that might cause issues during the migration.

5. Upgrade the firmware

- Update the low-level software controlling a device's hardware, such as its BIOS or UEFI, ensuring proper initialization during booting. Unlike OSs, firmware manages hardware directly.
- **Ensure compatibility:** Enable hardware features like Secure Boot and TPM 2.0, as required by Windows 11.
- **Enable UEFI support:** Transition devices from the legacy BIOS to the UEFI for Windows 11.
- **Optimize hardware initialization:** Optimize boot processes for Windows 11 compatibility.
- **Enable security enhancements:** Enable features like Secure Boot and firmware-based encryption.
- For more information, please refer to the firmware upgrade troubleshooting document.

6. Uninstall unnecessary applications

- Remove any applications that are not essential, especially older software that might conflict with Windows 11.

7. Check for Windows update error codes

- **Check for error codes:** If you receive specific error codes during the migration, search for them on Microsoft's support site for tailored troubleshooting steps.
- **Use the Windows 11 Installation Assistant:** If Windows Update fails, use the Installation Assistant from Microsoft's website to perform an upgrade

8. Use the Media Creation Tool

- **Create installation media:** Download the Windows 11 Media Creation Tool from the Microsoft website and create a bootable USB drive. Use this drive to upgrade your system directly.

9. Review the logs for errors

- **Check the logs:** Review the setup logs located in C:\$WINDOWS.~BT\Sources\Panther for any specific error messages that can help you diagnose the problem

10. **Restore systems to the previous version**

    - If the upgrade fails and you encounter booting issues, revert to your previous version of Windows using the recovery options available during startup.

11. **Contact support**

    - If all else fails, consider reaching out to Microsoft Support or your IT department (if applicable) for assistance..

To minimize issues during the upgrade process, it is recommended to:

- Ensure your hardware meets the system requirements.
- Back up your data and perform a clean installation if possible.
- Update drivers before and after the upgrade.
- Monitor for system updates and apply them as needed.

For more information, please refer to this Microsoft document.

07

Securing Windows 11 devices using Endpoint Central

Securing Windows 11 devices using Endpoint Central involves leveraging the software's features for device management, patch management, and security enforcement. Here’s a comprehensive guide on how to use Endpoint Central to secure your Windows 11 environment:

1. **Device inventorying and monitoring**
    - **Asset management:** Use Endpoint Central to maintain an up-to-date inventory of all devices. Regularly monitor the status of devices, including OS versions and installed software.
    - **Compliance checks:** Regularly check compliance with organizational policies and security configurations.

2. Patch management

- **Automated updates:** Configure Endpoint Central to deploy critical updates and patches automatically for Windows 11 and installed applications.
- **Scheduled patch deployment:** Set up a schedule for patch deployment during non-peak hours to minimize disruptions.
- **An approval workflow:** Implement an approval workflow for updates to ensure critical patches are tested before deployment.

3. Endpoint protection

- **Antivirus software management:** Integrate and manage endpoint protection solutions, ensuring that Windows Defender or third-party antivirus software is properly configured and up to date.
- **Malware protection policies:** Create and enforce policies for real-time protection, scheduled scans, and automatic updates.

4. Configuration management

- **Security baselines:** Implement security baselines based on industry standards (e.g., CIS Benchmarks) to ensure devices comply with security best practices.
- **Group Policies:** Utilize Endpoint Central to manage and enforce Group Policy settings across Windows 11 devices, controlling settings related to security, user permissions, and more.

5. Device encryption

- **BitLocker management:** Deploy and manage BitLocker encryption on Windows 11 devices to protect data at rest. Ensure that recovery keys are securely stored.
- **Encryption status monitoring:** Regularly monitor the encryption statuses of devices and ensure compliance.

6. Application management

- **Software deployment:** Control and manage the installation of applications under Inventory > Prohibit Software, ensuring only approved applications are installed on Windows 11 devices.
- **Uninstallation of unauthorized software:** Create policies to uninstall unauthorized applications automatically.

7. Network security

- **VPN configuration:** If your organization uses a VPN, configure Endpoint Central to enforce VPN settings for remote devices to ensure secure connections.
- **Network configuration policies:** Manage network settings and policies to enforce secure configurations on devices.

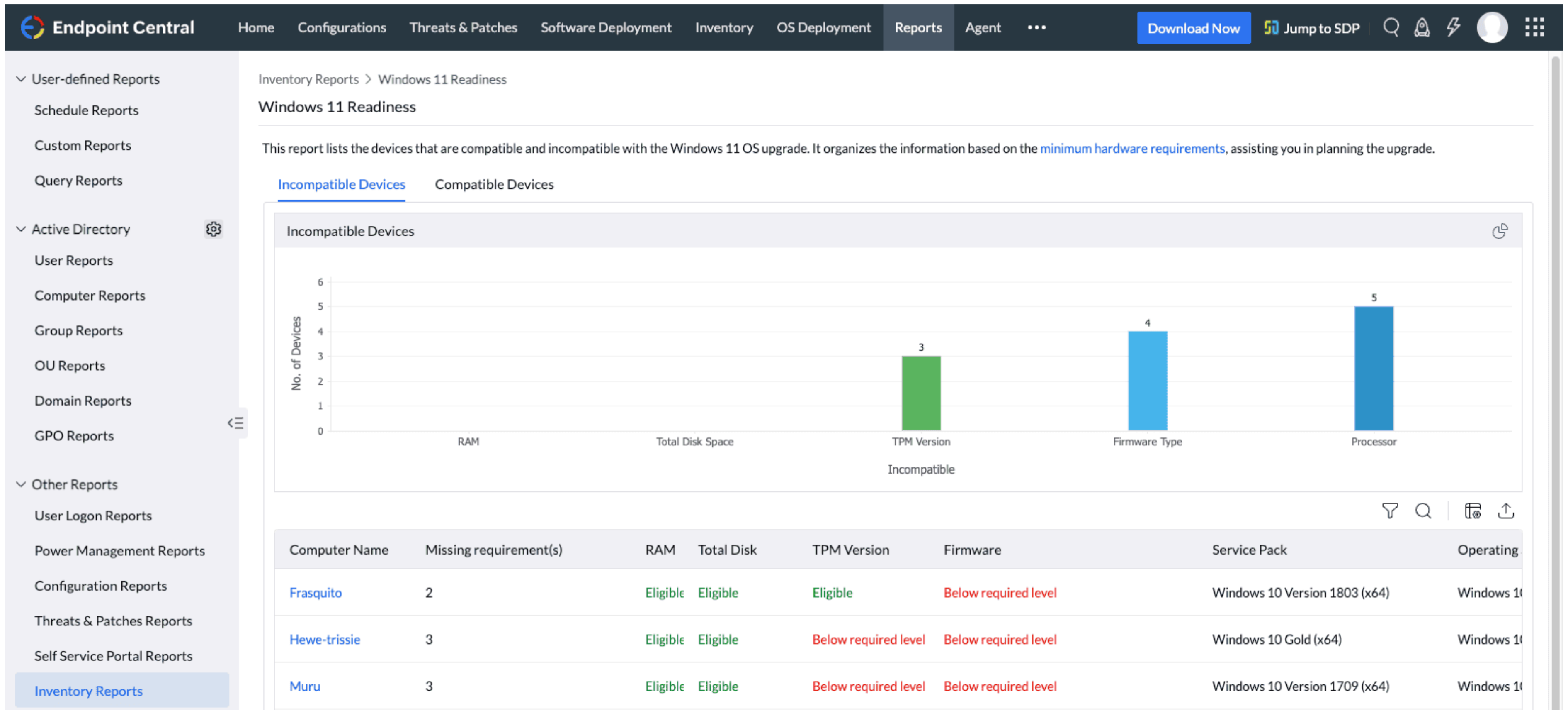
8. Security auditing and reporting

- **Audit logs:** Use Endpoint Central to monitor and audit user activities, software installations, and configuration changes.
- **Compliance reporting:** Generate compliance reports to track adherence to security policies and identify areas for improvement.

Steps to check devices' incompatibility with Windows 11 using Endpoint Central

To assess devices' incompatibility with Windows 11 using Endpoint Central, you can follow these steps to evaluate the hardware and software setups of your devices. Using Endpoint Central, you can gather the necessary information through the inventory and reporting features. Here’s how:

- Go to **Inventory > Computers** to view the list of managed devices.
- Go to **Inventory > Inventory Reports > Hardware Reports → Windows 11 Readiness** to view the list of **Incompatible Devices.**



Windows 11 Readiness

This report lists the devices that are compatible and incompatible with the Windows 11 OS upgrade. It organizes the information based on the minimum hardware requirements, assisting you in planning the upgrade.

Incompatible Devices

Computer Name	Missing requirement(s)	RAM	Total Disk	TPM Version	Firmware	Service Pack	Operating
Frasquito	2	Eligible	Eligible	Eligible	Below required level	Windows 10 Version 1803 (x64)	Windows 1(
Hewe-trissie	3	Eligible	Eligible	Below required level	Below required level	Windows 10 Gold (x64)	Windows 1(
Muru	3	Eligible	Eligible	Below required level	Below required level	Windows 10 Version 1709 (x64)	Windows 1(

08

How to make incompatible devices compatible with Windows 11

To make incompatible devices compatible with Windows 11 using Endpoint Central, you can implement several strategies to address hardware and software limitations. The minimum requirements for installing Windows 11 on your corporate devices and the steps to make the devices compatible are given below:

Component	Description
RAM	4 GB
Processor	1 GHz or faster with 2 or more cores on a compatible 64-bit processor or system on a chip
Storage	A 64 GB or larger storage device—refer to this link for more information
System firmware	UEFI- and Secure-Boot-capable—check here for information on how your PC might be able to meet this requirement
TPM	TPM 2.0—check here for instructions on how your PC might be enabled to meet this requirement

For more information, check out the Windows support document .

Alternative methods to check if the devices in your organization are compatible with Windows 11

If you are looking to upgrade to Windows 11 but are not sure if the devices in your organization meet the minimum requirements, you can run the detection logic script or PC Health Check app. This helps you determine if the devices are compatible with Windows 11.

Endpoint Central incorporates the detection logic script to check if the processors are compatible with Windows 11. If the necessary requirements are not met, the detection logic provides an output that highlights the checks that failed. For more in-depth insights into this, check out the Windows community tech page.

09

Conclusion

Migrating from Windows 10 to Windows 11 presents a valuable opportunity to enhance your computing experience with improved features, a refreshed UI, and increased security measures. However, a successful migration requires careful planning, thorough compatibility checks, and effective management of the transition process. By utilizing Endpoint Central, organizations can leverage the benefits of Windows 11 while minimizing disruptions and ensuring a smooth transition for all users. Embracing the new features and enhancements of Windows 11 will not only improve productivity but also enhance overall security and user satisfaction.