Windows 11 Transition Guide

Security, Performance & Compatibility in VDI

Windows 10 Support Ends in October 2025 – Plan Your Move Now

Windows 10 will reach its end-of-life on 14th October 2025, meaning there will be no further security updates or patches. Organisations using Windows 10 virtual desktops need to plan their transition to Windows 11 to ensure security, performance, and compliance.

Whether you're currently using Omnissa Horizon or Citrix Virtual Apps & Desktops, ebb3 are here help you navigate the transition.

Don't Get Caught Out by Performance Drops

Windows 11 introduces advanced security and system enhancements, increasing its compute overhead compared to Windows 10. This can impact performance, especially in GPU-accelerated workloads.

Planning your transition carefully ensures your VDI environment is optimised to handle the additional resource demand to maintain user experience and efficiency.

Plan your transition with ebb3 to prevent slowdowns and performance issues.

Contact Us

Security Considerations for Windows 11 in VDI

Security is at the core of Windows 11. Ensure your VDI environment aligns with modern security best practices:

Encryption and Compliance

- Align encryption policies with Windows 11's stronger security requirements, including BitLocker and VBS.
- Ensure compliance with industry standards such as ISO 27001, NIST, and GDPR.

Zero Trust Security Model

- Windows 11 embraces Zero Trust principles, requiring continuous verification of users and devices.
- Test your IAM policies, including Windows Hello for Business, Multi-Factor Authentication (MFA), and Conditional Access in a VDI environment.

Hypervisor Security Readiness

- Confirm your hypervisor supports vTPM, Secure Boot, and Hypervisor-Enforced Code Integrity (HVCI).
- These features prevent rootkit attacks, unauthorised firmware modifications, and malicious code execution.

Windows 11 introduces stricter security standards—we make sure your VDI stays compliant and secure.

Contact Us

Endpoint Security Compatibility

- Ensure antivirus, endpoint detection and response (EDR), and security monitoring tools are compatible with Windows 11.
- Key security features include Kernel Mode Hardware Enforced Stack Protection, Windows Defender Application Guard, and Smart App Control.

Security Logging & Monitoring

- Windows 11 enhances security logging and integrates with Microsoft Defender for Endpoint, Azure Sentinel, and third-party SIEM platforms.
- Verify that your monitoring tools capture Windows 11-specific security events to detect and mitigate threats proactively.

Understanding TPM 2.0 and Windows 11 Security Requirements

Windows 11 mandates TPM 2.0 as part of Microsoft's enhanced security framework. TPM (Trusted Platform Module) is a built-in security chip that protects against malware, unauthorised access, and data breaches.

In a VDI environment, your hypervisor must support Virtual TPM (vTPM) to enable these security features:

- **Secure Boot** – Prevents malicious software from loading during startup.
- **BitLocker Encryption** – Protects data at rest through disk encryption.
- **Windows Hello** – Enables passwordless authentication.
- **Virtualisation-Based Security** – Isolates sensitive data and processes.

Without TPM 2.0 or vTPM, Windows 11 won't be officially supported, and these critical security features will be unavailable.

ebb3 ensures your infrastructure is compliant, so you don't risk security gaps or unsupported deployments.

Contact Us

Ensuring Application Compatibility

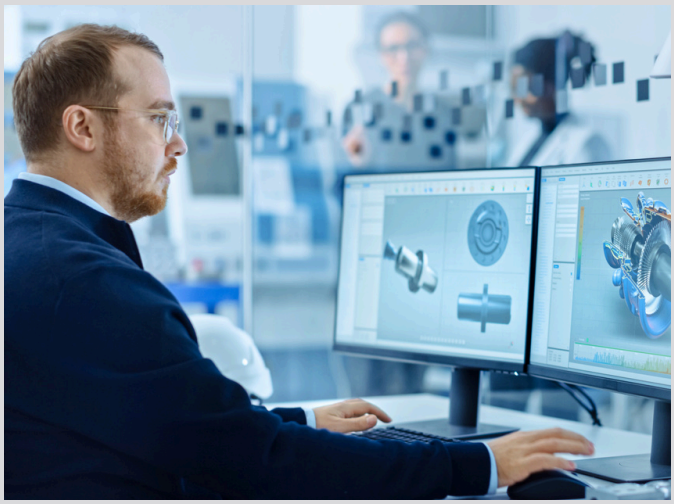
Before migrating, verify that your entire IT infrastructure, including servers, hypervisors, and VDI components, is updated and ready for Windows 11.

Key steps include:

- **Testing enterprise-critical applications** for compatibility.
- **Assessing graphics-heavy applications** like AutoCAD, Revit, Rhino, and SketchUp.
- **Running pilot migrations** to identify and resolve potential issues before full deployment.

ebb3 can help you testing and validate compatibility to avoid downtime and disruption.

Contact Us



Licensing & Activation

Windows 11 in a VDI environment requires proper licensing to ensure compliance and activation at scale.

Ensure:

- Your organisation has the correct KMS license server setup.
- You're using Volume Licensing to cover your virtual desktop infrastructure.

Optimising for a Fresh Start

Migrating to Windows 11 is an opportunity to streamline and enhance your VDI environment:

- Switch to FSLogix for improved profile management and faster logins.
- Optimise system performance by cleaning up legacy settings and configurations.

How ebb3 Can Help

At ebb3, we specialise in Windows 11 migrations for VDI environments. **Our expert team is already working with organisations to:**

- Identify and mitigate deployment challenges.
- Optimise infrastructure for performance and security.
- Ensure compliance with industry best practices.

A seamless migration minimises downtime, enhances security, and improves user experience.

Let's plan your Windows 11 migration together. Get in Touch to discuss your VDI migration strategy.

Contact Us