Microsoft

Windows Virtual Desktop on Modern Devices

Robert Henry & Craig Tellalian
Surface Sales and Strategy

April 2020

Contents

Authored by Robert Henry & Craig Tellalian. Edited by John Kaiser.

Introduction

Using Windows Virtual Desktop with modern devices like Microsoft Surface represents another milestone in the evolution of computing combining Microsoft 365 – virtualized in the Azure cloud – with the advanced security protections, enterprise-level manageability, and enhanced productivity tools of Windows 10.

With Windows Virtual Desktop (WVD), users get a virtualized Windows 10 experience that is always up to date and available on any device. It's the only virtual desktop infrastructure (VDI) that delivers simplified management, multi-session Windows 10, optimizations for Office 365 ProPlus, and support for Remote Desktop Services (RDS) environments. IT admins can deploy and scale Windows desktops and apps on Azure in minutes and get built-in security and compliance features.

Windows 10 Modern Devices

Although you can run Windows Virtual Desktop on Windows 7, Windows Server 2012 R2, or virtual machines, running WVD on modern devices provides unique advantages including support for:

- **Flexible form factors** – like 2-in-1 devices with pen and detachable keyboard.
- **Persistent, on-demand and just-in-time work scenarios** – with offline and on-device access for more productive experiences.
- **Windows 10 modern device security and manageability** – providing the flexibility to be productive anywhere.

Flexible form factors

Windows 10 modern devices comprise a diverse portfolio of form factors including traditional laptops, all-in-one machines, and 2-in-1 devices.

Transforming the Windows Virtual Desktop endpoint

Devices with a 2-in-1 form factor provide users with the ideal WVD endpoint bringing together the optimal balance of portability, versatility, power, and long battery life. From site engineers relying on Surface Go in tablet mode to financial advisors attaching Surface Pro 7 to a dock and multiple monitors, 2-in-1 devices deliver the versatility that has come to define the modern workplace.

Features designed to enhance productivity on 2-in-1 modern devices include:

- Vibrant, high resolution displays.
- Natural inking and multi-touch for more immersive experiences.
- Accessibility - With a robust set of built-in and third-party accessibility features, Windows 10 modern devices let you choose how to interact with your device, express ideas, and get work done.
- Far-field mics and high-performance speakers for crystal-clear Microsoft Teams meetings.
- Integrated experiences with Microsoft 365 apps and services.
- Biometric security.

- Long battery life and fast charging.
- LTE options, on modern devices like Surface Pro X and Surface Go, for always connected, secure network access without the inconvenience or risk of depending on public Wi-Fi hotspots.
- Windows 10 modern devices work with the widest range of peripherals such as printers (including 3D printers), cameras, credit card readers, barcode scanners, and many others.
- With a large ecosystem of built-in and third-party accessibility features, Windows 10 modern devices let you choose how to interact with your device, express ideas, and get work done.

VDI Device Redirection Support

When considering VDI on Azure it's also important to keep in mind that Windows 10 devices like Surface provide the broadest range of Device Redirection support compared to Android-, iOs/macOS- and Web-based access. The Windows Inbox (MSTSC) and Windows Desktop (MSRDC) clients provide the most Device Redirection capabilities including Input Redirection (keyboard, mouse, pen and touch), Port Redirection (serial and USB) and Other Redirections (cameras, clipboard, local drive/storage, location, microphones, printers, scanners, smart cards and speakers).

For a complete comparison of Device Redirection support visit: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-app-compare#redirection-support

Familiar Desktop Experience

Not only does running the Windows Desktop Client on Surface devices provide users with the broadest set of Device Redirection capabilities but it also provides the additional capability to use the apps in the way that is familiar to the end users – by launching an app directly from the Start Menu or launch the apps by searching it in the search bar.

Persistent, on-demand and just-in-time work scenarios

Windows Virtual Desktop on modern devices helps customers meet increasingly complex business and security requirements across industries, employee roles, and work environments. These include:

- Multi-layered security of access to data and organizational resources.
- Compliance with industry regulations.
- Support for an increasingly elastic workforce.
- Employee-specific needs across a variety of job functions.
- Ability to support specialized, processor-intensive workloads.
- Resilience for sustaining operations during disruptions.

Table 1. Windows Virtual Desktop ecosystem

Security & regulation	Elastic workforce	Work Roles	Special workloads	Business continuity
- Financial Services - Healthcare	- Merger & acquisition	- BYOD & mobile - Call centers	- Design & engineering	- On demand - Just-in-Time (JIT)

- Government	- Short term employees - Contractors & partners	- Branch workers	- Support for legacy apps - Software dev & test	- Work @ Home

Unlike traditional, fixed VDI "terminals", 2-in-1 modern devices allow users to work from anywhere and enable companies to remain viable and operational during unforeseen events -- from severe weather to public health emergencies. With support for persistent, on-demand and just-in-time scenarios, Windows 10 modern devices effectively help companies sustain ongoing operations and mitigate risk from disruptive events.

Offline and on-device access for more productive experiences

Traditional VDI solutions only work when the endpoint is connected to the internet. But what happens when the internet or power is unavailable for any reason (due to mobility, being on a plane, or power outages, and so on)?

Modern devices can easily augment online productivity (based in Windows Virtual Desktop) with offline access to files and Microsoft 365 and third-party applications. Traditional desktop apps like Microsoft Office can provide users the ability to stay productive in "offline mode". Files from the cloud can be synced locally on the modern device using OneDrive for Business for offline access as well. You can have the confidence that all that locally "cached" information is up-to-date and secure.

In addition to adding support for offline access to apps and files, Windows 10 modern devices support the ability to run collaborative experiences like Microsoft Teams "On-Device". Although VDI solutions support the use of Teams through a virtual session, users may opt for an optimized experience by using an on-device instance of Teams for multimedia channels like voice, video, live captioning and emerging AI-on-device capabilities.

An alternative to locally installing traditional applications is to take advantage of the Chromium version of Microsoft Edge, which comes with Progressive Web Apps (PWA) support. Microsoft Edge makes it possible to install a website as a native app on a Windows 10 modern device enabling additional features, such as push notifications, background data refresh, offline support, and more.

Windows 10 modern device security and manageability

- **Enterprise-grade Security** - Windows Hello and Microsoft Passport provide secure and easy-to-deploy multi-factor credentials. Credential Guard protects the network while Advanced Threat Protection detects attacks that have made it past all other defenses. Only Windows has a comprehensive approach which secures critical business identities, data, devices and connections using industry standards such as TPM for device data encryption, all manageable by the enterprise.
- **Network Protection -** With Windows 10 and the Microsoft Enterprise Mobility Suite (EMS), you can defend your organization from growing online security threats to users, devices, data, and apps. Additionally, EMS allows you to use health data to build conditional access policies providing greater security when accessing corporate resources.
- **Backward and forward compatibility** - Windows 10 devices provide backward and forward compatibility across hardware, software and services. Microsoft has a strong history of maintaining legacy support of hardware, peripherals, software and services while incorporating the latest technologies. Businesses can

plan IT investments to have a long useful life.

- **Bridge for legacy Windows 7 workloads -** For solution scenarios dependent on legacy Windows OS environments, enterprises can use VDI instances of Windows 7 running in Azure. This enables support on modern devices like Surface without the risk of relying on older Windows 7 machines that no longer receive the latest security updates. In addition to these "future proofing" benefits, migration of any legacy workloads becomes greatly simplified when modern Windows 10 hardware is already deployed.
- **Simplified Device Management** - Intune is the tool of choice for configuring your Surface. It provides a platform that you can use to manage Surface and many other modern devices, including those running Windows, Android, iOS, and Mac operating systems. Intune lets you manage employee-owned devices as well as corporate-owned devices, which makes it the perfect tool for transitioning to modern management.
- **Modern management** – By maximizing efficiencies from cloud computing, modern management enables IT to better serve the needs of users, stakeholders and customers in an increasingly competitive business environment. For example, you can get user devices up-and-running with minimal interaction from your team. Setup is automatic and self-serviced. Updates are quick and painless for both your team and your users. You can manage devices regardless of their physical location. By adopting cloud technologies wherever possible, you can simplify management, improve security, and provide better user experiences while lowering TCO.
- **Zero-Touch Deployment** - Autopilot is the recommended modern management deployment option for Windows 10 modern devices, including Surface. Windows Autopilot is a cloud-based deployment technology in Windows 10. You can use Windows Autopilot to remotely deploy and configure devices in a zero-touch process right out of the box. Windows Autopilot-registered devices are identified over the Internet at first startup through a unique device signature that's called a hardware hash. They're automatically enrolled and configured by using modern management solutions such as Azure Active Directory (Azure AD) and mobile device management.

Summary

Windows Virtual Desktop on modern devices provides organizations with greater flexibility and resilience in meeting the diverse needs of users, stakeholders, and customers. Running WVD on modern devices provides unique advantages over continued reliance on legacy devices. Flexible form factors like 2-in-1 devices connected to the cloud, enable users to be productive from anywhere. Whether employees work in persistent, on-demand, or just-in-time scenarios, WVD affords businesses with the versatility to sustain productivity throughout disruptions from public health emergencies or other unforeseen events. Using the built in, multi-layered security and modern manageability of Windows 10, companies can take advantage of an expanding ecosystem of cloud-based services to rapidly deploy and scale Windows desktops and apps. Simply put, Windows Virtual Desktop on modern devices delivers critically needed technology to organizations and businesses of all sizes

Learn more

For more information, see the following resources:

- Windows Virtual Desktop