



Microsoft meets Community: Windows Virtual Desktop

Sharing Tips and Tricks on how to Manage Windows Virtual Desktop via Intune in Microsoft Endpoint Manager

Anoop C Nair
Microsoft MVP - Solution Architect



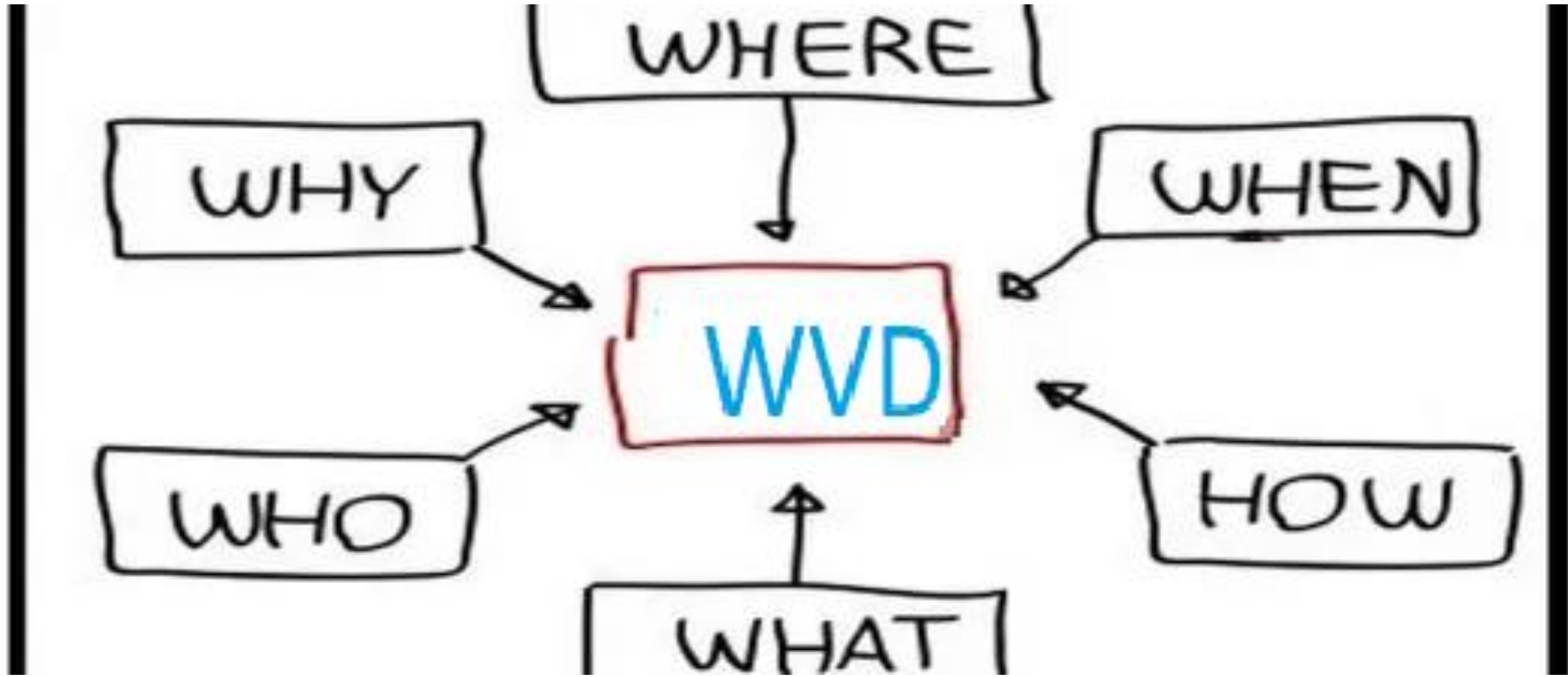
@anoopmannur

3rd edition

Content

- Context
- Hybrid AAD Join + Group Policy
- Conditional Access Policies + Dynamic Groups
- Enrolment Process
- Security Policies
- Application Deployment
- Patching & Updates
- Demo, Demo, and Demo

Context



Hybrid AAD Join & Group Policy

- Make sure the VMs are Hybrid AAD Join
- MDM Group Policy for All WVD VMs

The image shows two screenshots side-by-side. The left screenshot is the Microsoft Azure Active Directory Connect console. In the left-hand navigation pane, 'Device systems' is selected, and 'Hybrid Azure AD join' is highlighted. A blue arrow points from this menu item to the 'Device operating systems' section in the main pane. In this section, the checkbox for 'Windows 10 or later domain-joined devices' is checked and highlighted in yellow, with a blue circle containing the number '1' next to it. The right screenshot is the Windows Group Policy Editor. The 'MDM' folder is expanded, and the policy 'Enable automatic MDM enrollment using default Azure AD credentials' is selected. The policy state is 'Not configured'. A table below shows the policy settings:




Setting	State	Comment
Enable automatic MDM enrollment using default Azure AD credentials	Not configured	No
Disable MDM Enrollment	Not configured	No

The 'Enable automatic MDM enrollment...' policy is shown in a detailed view. The 'Enabled' radio button is selected and highlighted in yellow, with a blue circle containing the number '2' next to it. The 'Supported on' field is set to 'At least Windows 10'. The 'Device Credential' type is selected in the 'Select Credential Type to Use' dropdown.

Azure AD Conditional Access & Groups

- Modern Security Parameters with Azure AD CA
- Dynamic Azure AD user/device groups

Selected items 1

	Windows Virtual Desktop 9cdead84-a844-4324-93f2-b2e6bb768d07	Remove
	Windows Virtual Desktop AME 5a0aa725-4958-4b0c-80a9-34562e23f3b7	Remove
	Windows Virtual Desktop Client fa4345a4-a730-4230-84a8-7d9651b86739	Remove

Grant 2 ✕

Control user access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ


Require Hybrid Azure AD joined device ⓘ

Microsoft Azure Search resources, services, and docs (G+)

Home > **Conditional Access | Policies** 3
Azure Active Directory

[+ New policy](#)
[What If](#)
[Refresh](#)
[Got feedback?](#)

Policy Name

WVD 

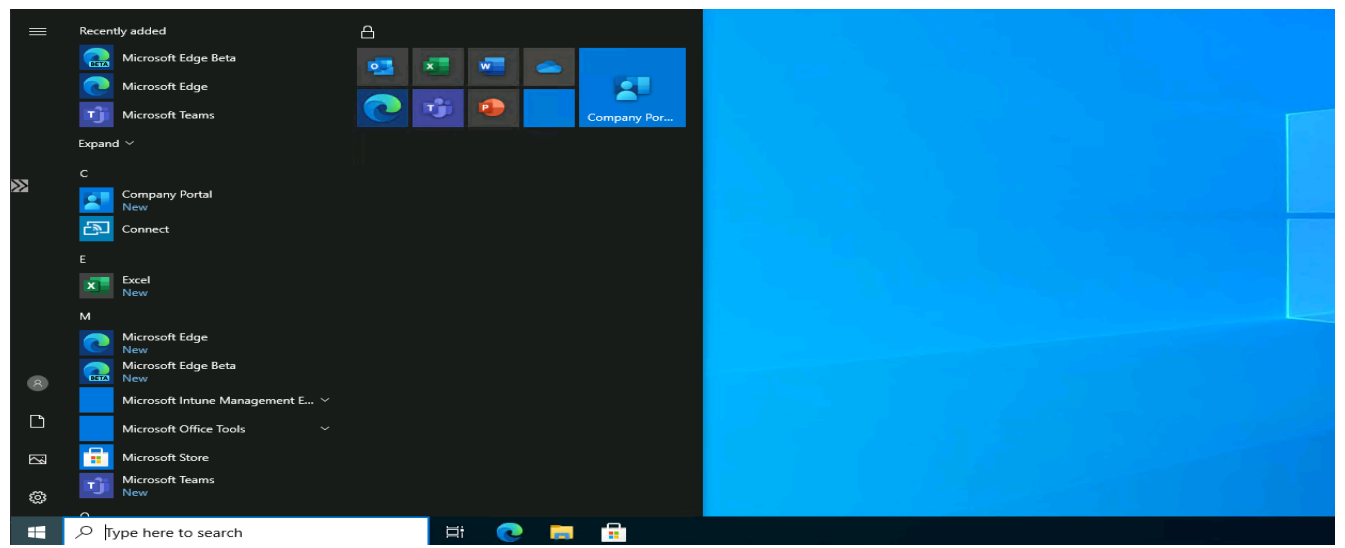
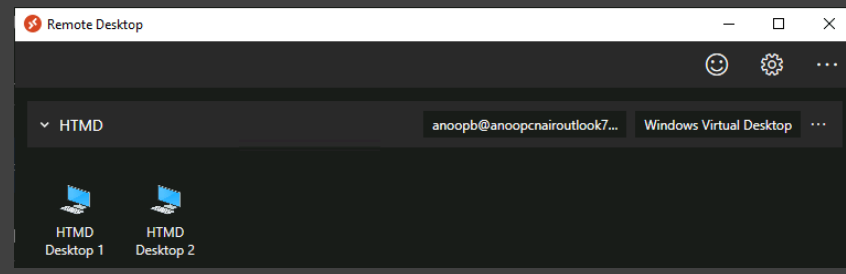
End User Experience



Seamless experience for the end users



Applications + Policies are deployed immediately after the Intune enrolment process



Security Policies

- National Cyber Security Center NCSC.gov.uk Guideline for MDM **security baseline** using CSPs
 - <https://www.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/windows-10-1803-with-mobile-device-management>
- Security Policies should be deployed either using
 - Intune Administrative Templates (Preferred for WVD)
 - Security Baselines

Home > Devices > Windows

Windows | Configuration profiles

Search (Ctrl+/) << + Create profile Columns Refresh Export Filter

Windows devices
Windows enrollment

Windows policies

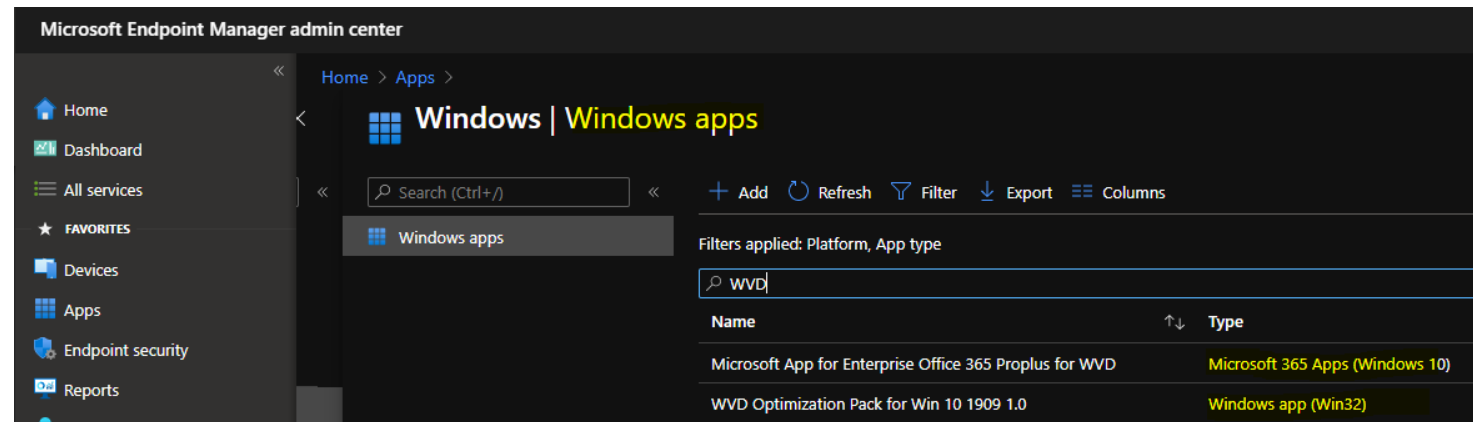
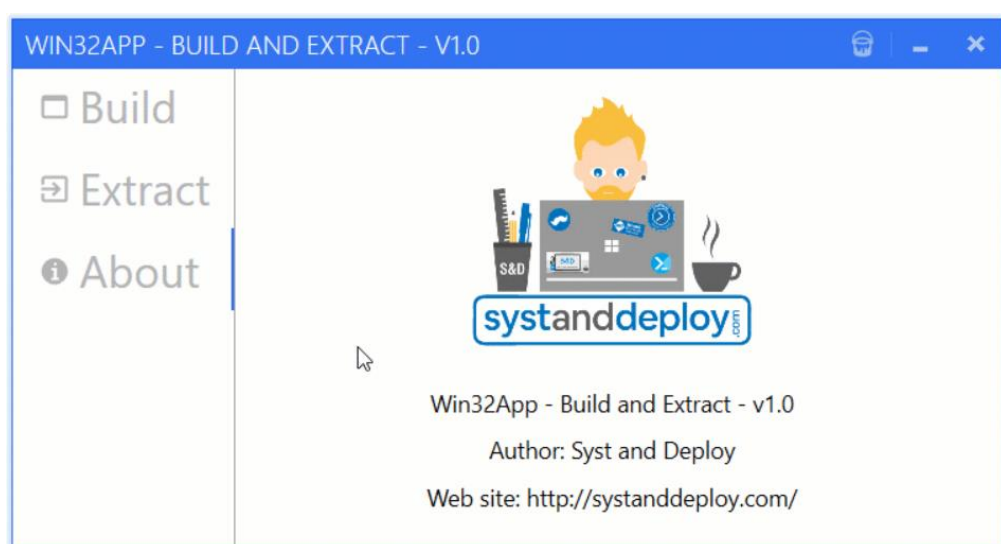
- Compliance policies
- Configuration profiles**
- PowerShell scripts
- Windows 10 update rings

Search: wvd

Profile Name	Platform	Profile Type
WVD Device Security Account Hardening	Windows 10 and later	Administrative Tem
WVD Edge Chromium Device Security	Windows 10 and later	Administrative Tem
WVD Edge Chromium User Based Security	Windows 10 and later	Administrative Tem
WVD Office Device Security Policies	Windows 10 and later	Administrative Tem
WVD Office User Based Security Policies	Windows 10 and later	Administrative Tem

Application Deployment

- Deploy Apps using Intune
- Complex Apps need to be converted (zipped) to **Intune win32 format**
 - Conversion Tool created by Damien Van Robaeys [MVP]
<http://www.systanddeploy.com/2020/11/intune-win32app-tool-create-and-extract.html>



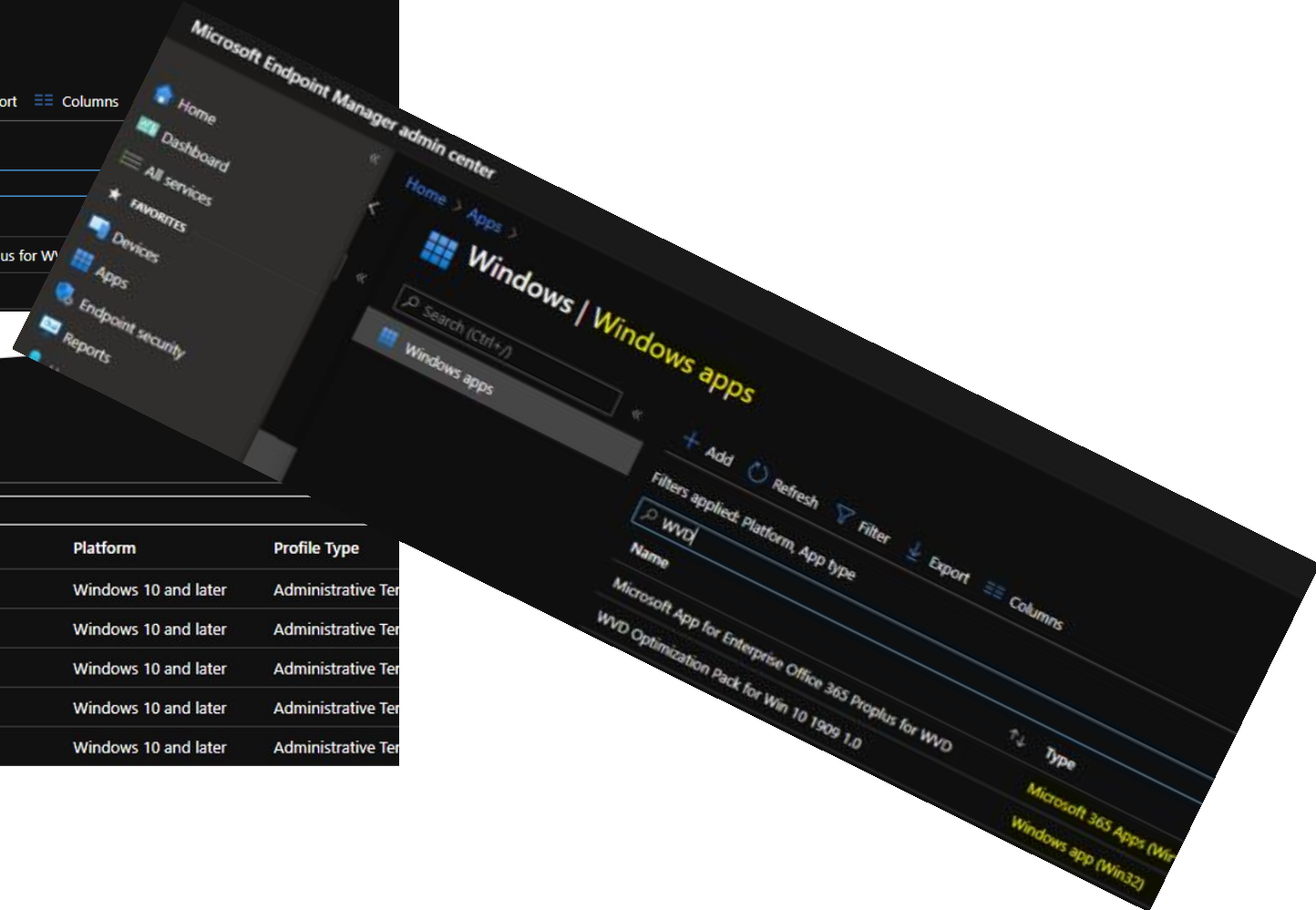
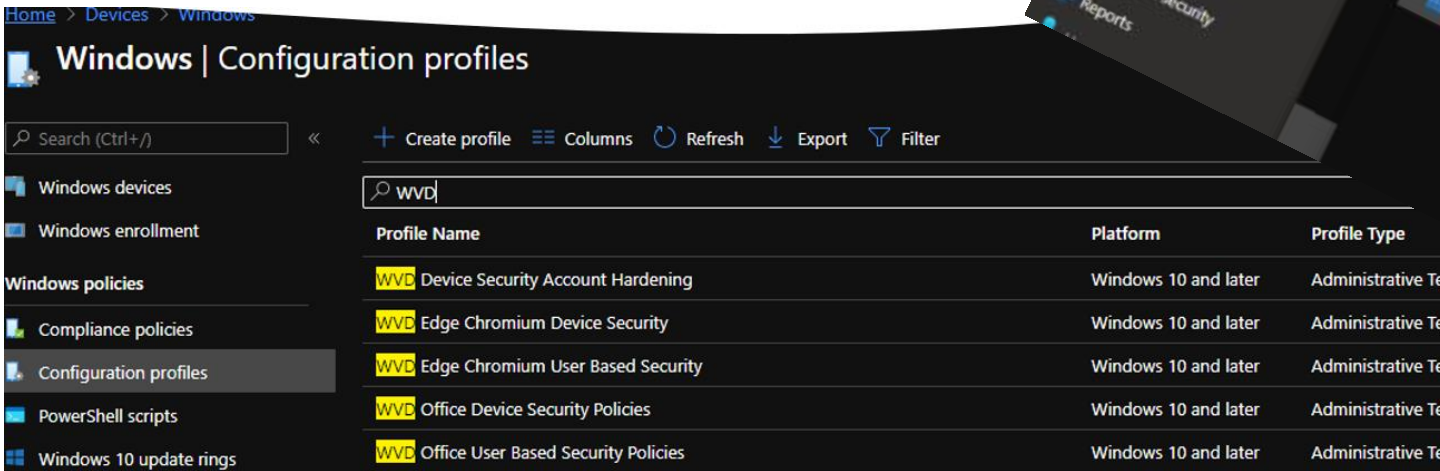
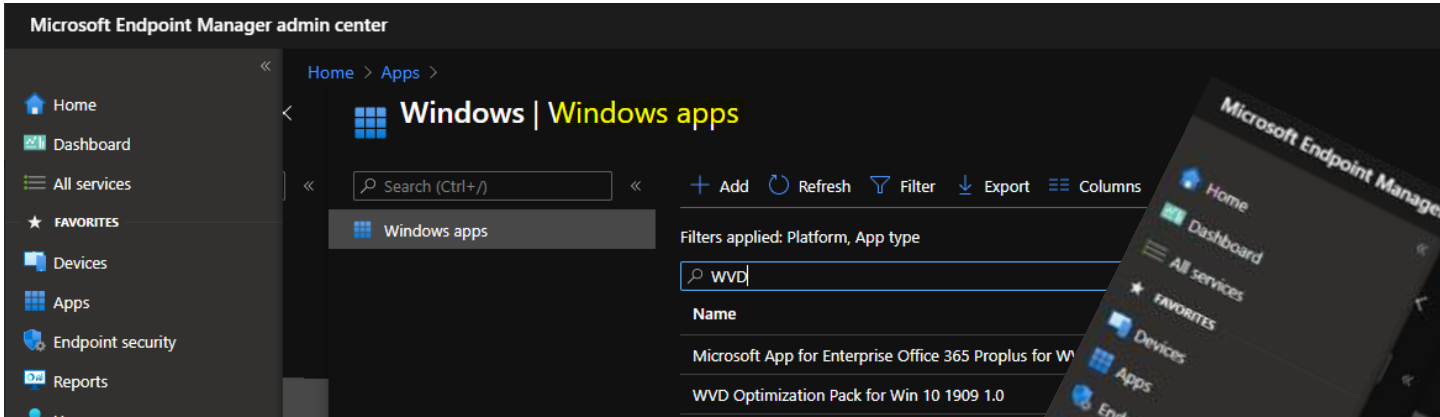
Patching & Windows 10 Upgrade

- Monthly **Patching** is managed via Windows Update for Business (**WUfB**) policies
- Windows 10 **Upgrade** policies are configured through WUfB **feature update** policies

The screenshot shows the Microsoft Intune console interface. The left-hand navigation pane includes options like Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Windows | Windows 10 update rings'. Below the title, there are search and action buttons: 'Search (Ctrl+ /)', 'Create profile', 'Refresh', 'Columns', 'Filter', and 'Export'. A list of 'Windows policies' is shown, including 'Windows devices', 'Windows enrollment', 'Compliance policies', 'Configuration profiles', 'PowerShell scripts', 'Windows 10 update rings' (which is highlighted), and 'Windows 10 feature updates (Pre...'. A table below the list displays the configuration for 'Windows 10 Monthly Patches':

Name	Feature Deferral	Quality Deferral	Feature
Windows 10 Monthly Patches	365	7	Running

Demo Time



Resources

- [Using Windows Virtual Desktop with Microsoft Intune | Microsoft Docs](#)
- [Windows Virtual Desktop documentation](#)
- [WVD - How To Manage Devices \(anoopcnaair.com\)](#)