

Modern Management of Windows Devices

Ron van Herk

rvherk@opentext.com

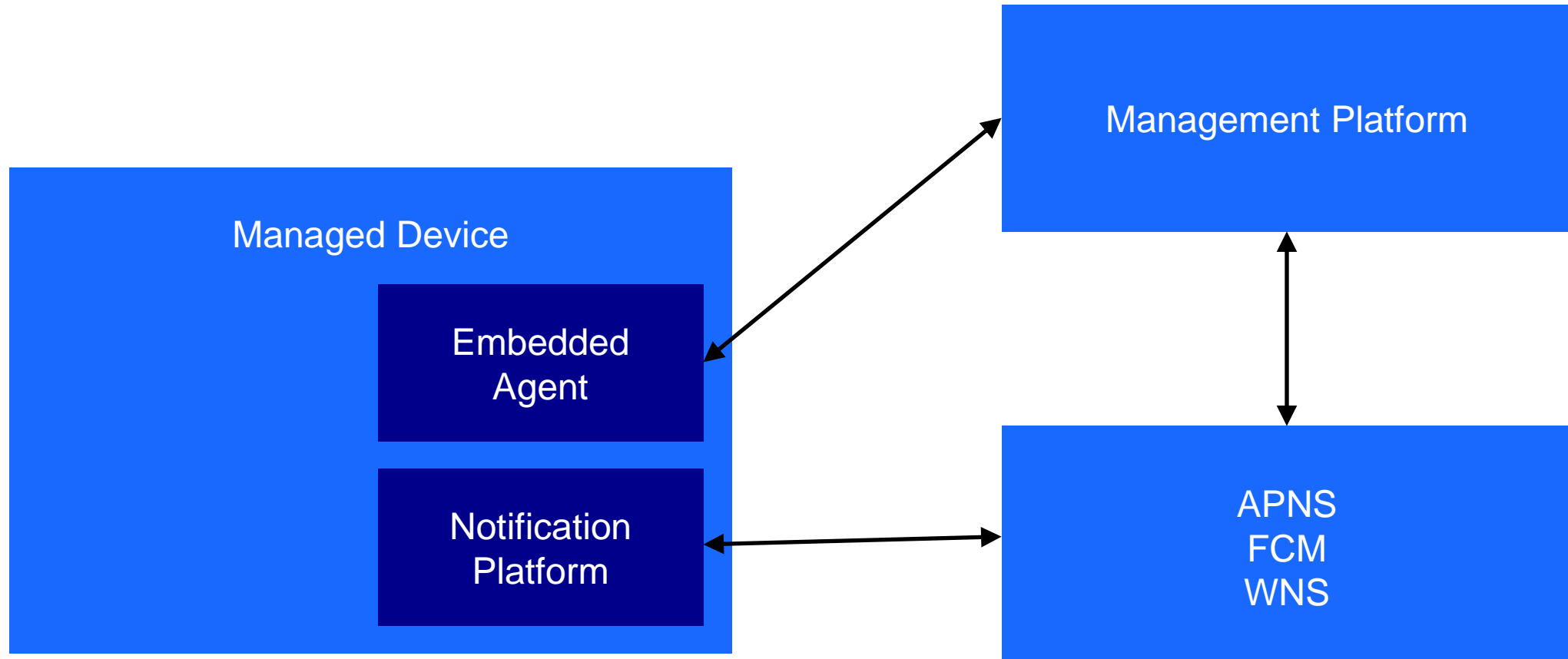
Agenda

- What is Modern Management ?
- Modern Management of Windows Devices
- ZENworks and Modern Management of Windows
- Windows Provisioning Package
- Windows Autopilot

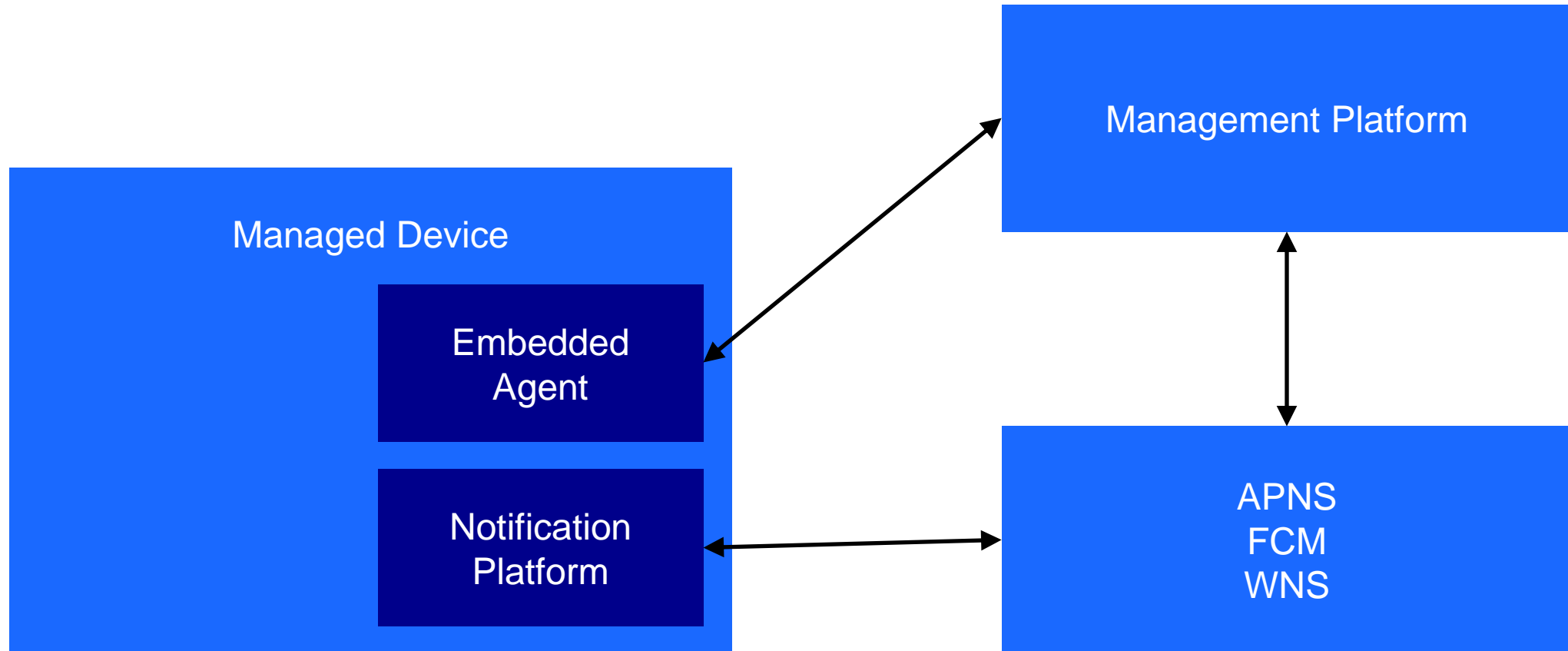
What is Modern Management ?

- Use of native OS built-in management agents or OS provided management API's
 - Supports 'agent less' management
- Requires internet connectivity for enrolment and subsequent management
 - Management servers reside either in Cloud or in a DMZ environment
 - Need Push notification services offered by OS vendors
- Lesser emphasis on custom OS images and more on customizing the built-in OS through applying settings and provisioning applications
 - Supports 'ZERO Touch by IT' scenarios
 - More focus on Self-Service / Self-deployment
- Wide variance between capabilities available across platforms
- OS supporting Modern Management
 - Windows 10/11 (Built-in Management Agent)
 - macOS (Built-in Management Agent)
 - Android (Uses OS provided management API's)
 - iOS / iPadOS (Built-in Management Agent)

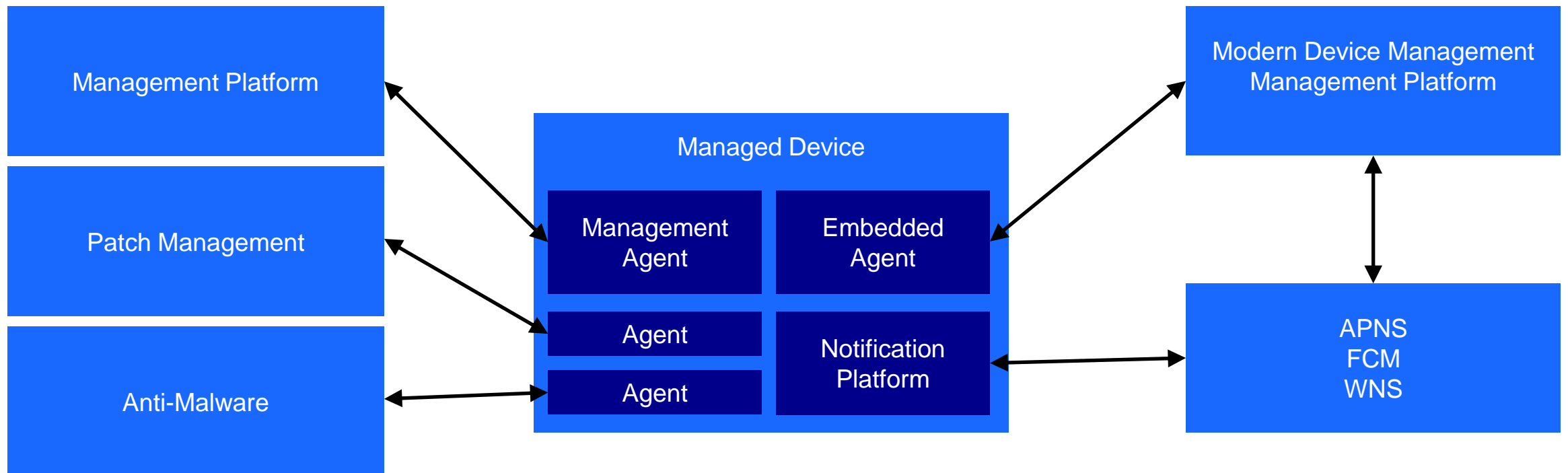
Modern Management



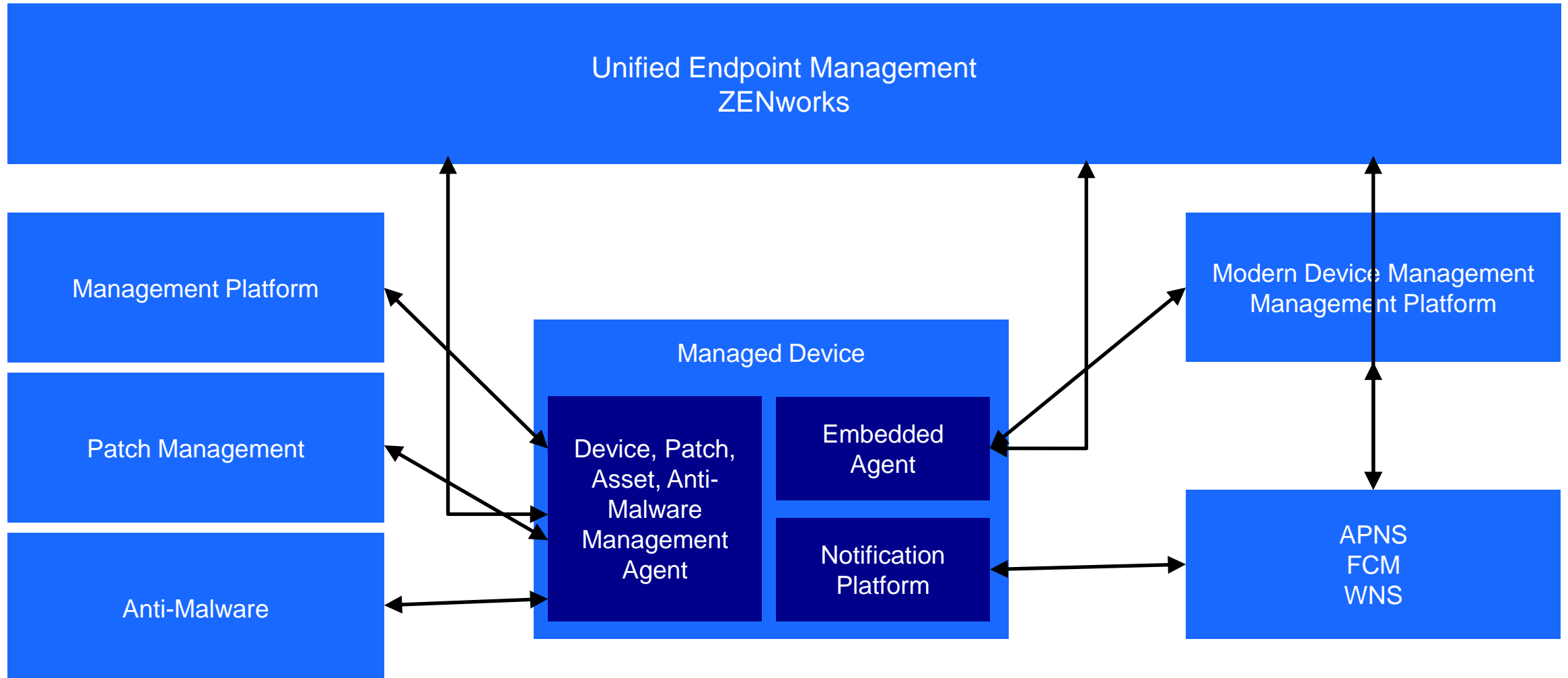
Modern Management



Managing Windows



Managing with ZENworks



ZENworks & Modern Management of Windows 10 & 11

- Enrolment of Corporate Devices –
 - Through deployment of Provisioning Package (for AD environments)
 - Through AutoPilot / OOBE Experience (for Azure AD environments)
- Support for following modes of enrolment
 - Devices managed through both ZEN Agent & Win 10/11 Modern Management
 - Device Managed through Win 10/11 Modern Management alone (without a need for 'Agent' on device)



Enrollment of Devices


Getting Started to Manage Windows 10 & 11 Devices

[Managing Windows 10 Devices](#) [Managing Android Devices](#) [Managing iOS/iPadOS Devices](#)

Getting started to managing Windows 10 Devices

Configure ZENworks Servers for Communication with Windows Services


ZENworks servers need to be configured for access to internet and also to enable devices to reach out to ZENworks server over internet



MDM Servers
Configured


Designate one or more primary servers in the DMZ as an MDM Server. Mobile devices can enroll to MDM Servers. Also, all push notifications necessary to manage mobile devices will be sent by MDM Servers.

[Add MDM Server](#)



Check Certificates

Check if certificates being used by MDM server conform to requirements. Also, check if required ports are open on the designated MDM server(s).




Configure Push Notification Service
Configured

Configure Windows Notification Services to allow ZENworks to send push notifications to Windows Devices.

[Configure WHS](#)

Setup and Enroll Device via AutoPilot


Windows 10 Devices which are not linked to Azure AD can be enrolled through MDM for management with ZENworks.



Create Azure MDM Application
Not Configured

Create Azure AD MDM Application to link ZENworks with Azure AD.


[Create Azure MDM Application](#)



Create Terms of Use
Not Configured


Create Terms of Use Policy to be shown to end users during Autopilot enrolment.

[Create Terms of Use Policy](#)



Configure Windows Business Store


Manage your Autopilot devices and assign them Enrolment Profiles.



Enrolment Workflow for AutoPilot

You can enrol devices into AutoPilot.


Deploy ZENworks Agent and Applications



Deploy ZENworks Agent
Not Configured

ZENworks agent can be deployed onto Win 10 MDM enrolled devices to augment management capabilities

[Create Agent Deployment Policy](#)



Deploy Applications

Applications with an MSI installer can be deployed onto Win 10 MDM devices

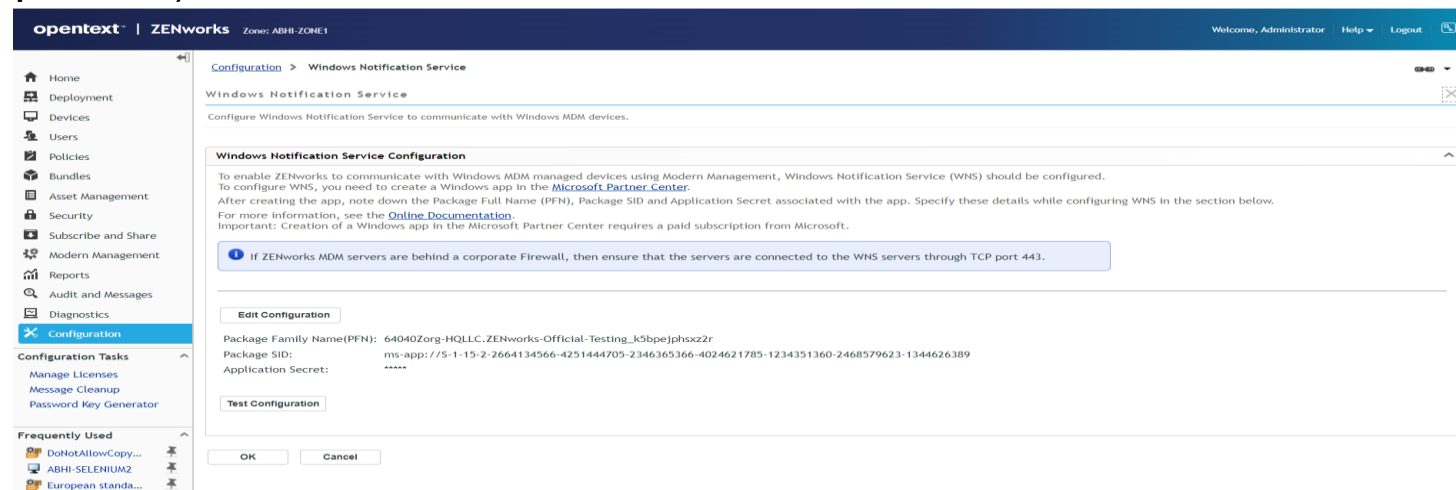
[Create Bundles](#)

Deployment of Windows Provisioning Package

A cosmic background featuring a view of Earth from space, with the horizon line and a thin blue atmosphere. A large, detailed Moon is visible in the upper left, showing its cratered surface. The sky transitions from deep blue to a bright yellow-orange glow on the right side, suggesting a sunrise or sunset. The overall scene is serene and futuristic.

Windows Provisioning Package Pre-requisites

- Requires Configuration of Windows Notification Service (WNS). Requires a MS developer Account (at present)



- Doesn't require user to be there on device. Is independent of logged in user and its directory source

Windows Provisioning Package Pre-requisites

[Configuration](#) > Enrollment using Provisioning Package

Enrollment using Provisioning Package

Prerequisites to create a provisioning package to enroll Windows MDM devices.

Prerequisites for Provisioning Package Creation

The Provisioning Package is created using the Windows Configuration Designer tool on a Windows MDM device. The following prerequisites are required. For information on enrolling Windows MDM devices to ZENworks, see the [Online Documentation](#).

Registration Key

Create a new registration key or use an existing key to set rules for enrolling Windows MDM devices to ZENworks.

[Create or View Registration Key](#)

Authorization Key

Create a new authorization key or use an existing key to validate the devices that will be registered to the zone.

[Create or View Authorization Key](#)

MDM Server

Select a MDM Server to which the Windows MDM devices should be enrolled.

MDM Enrollment URL

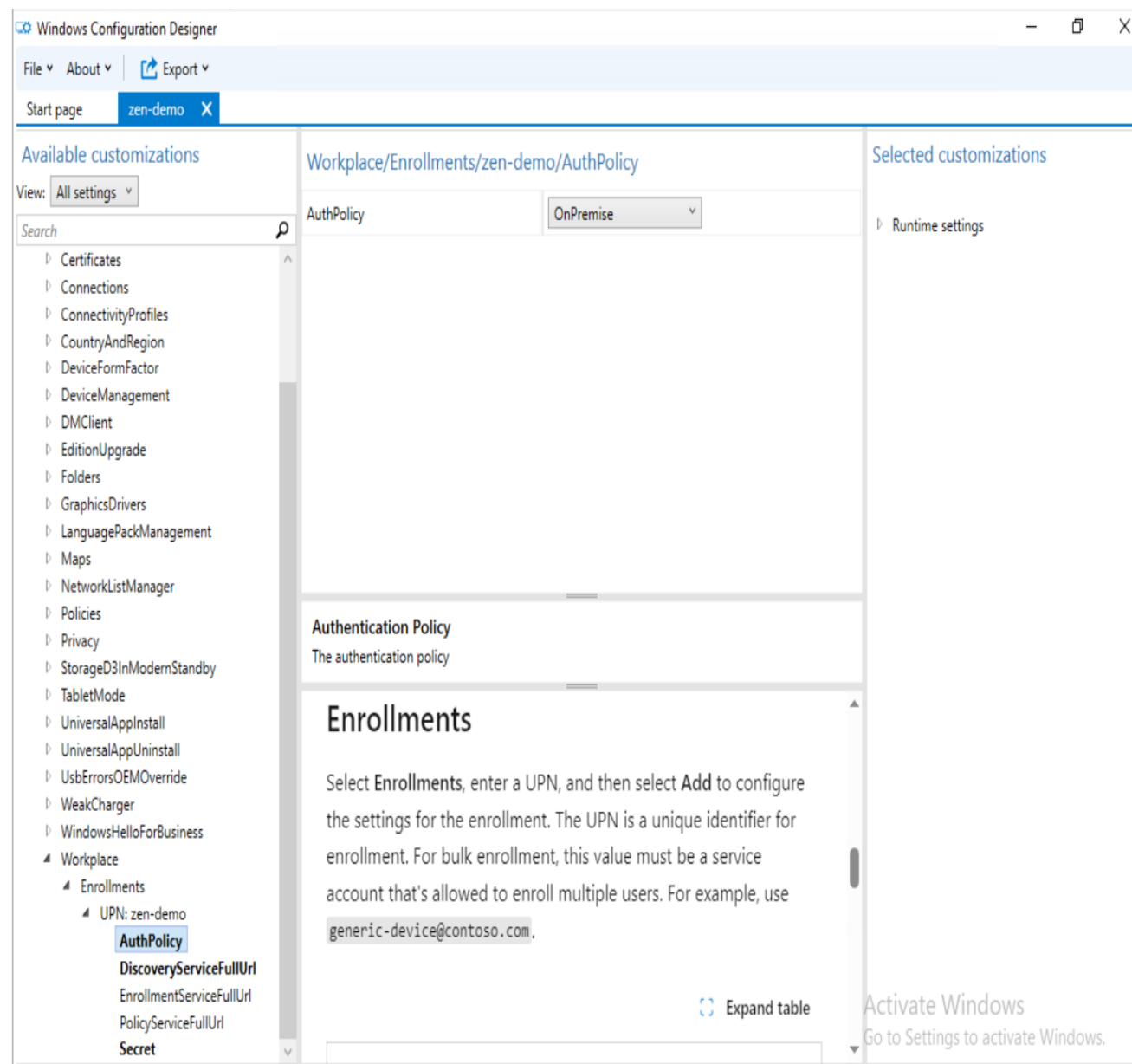
Copy the following URL, which is required while creating the provisioning package.

[Copy URL](#)

Zone Certificate

Download the zone certificate to secure the communication between Windows MDM devices and ZENworks during enrollment.

[Download](#)



Enrolment of Windows Devices as MDM Device

Deployment of Windows Provisioning Package

Devices can be enrolled just by executing Provisioning Package

- As part of Imaging
- Through ZENworks Agent (`Install-ProvisioningPackage -PackagePath C:\<packagename>.ppkg -QuietInstall`)
- Through Group Policies
- Manually

Suitable for scenarios, where bulk enrolment of devices is required

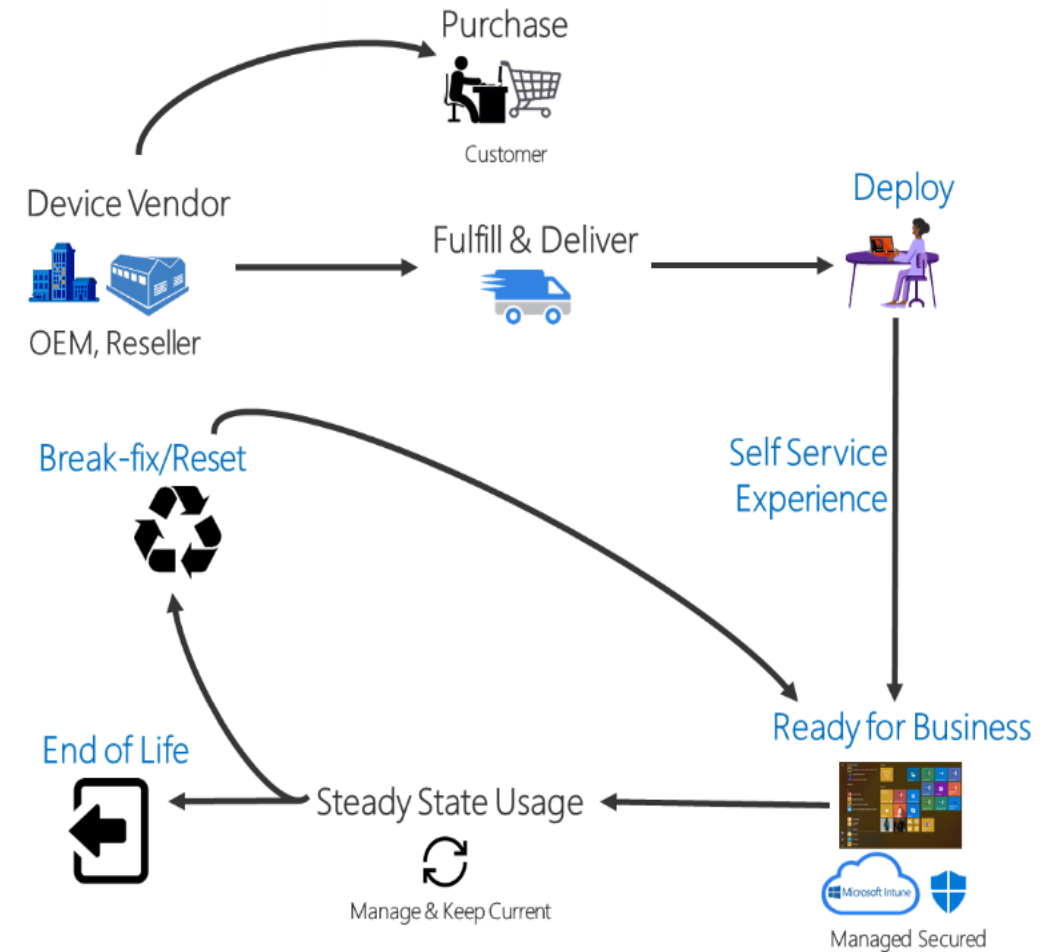
Suitable for scenarios, where enrolment into Windows MDM is required for specific capabilities available via MDM (say Windows Store Management)

Windows Auto Pilot

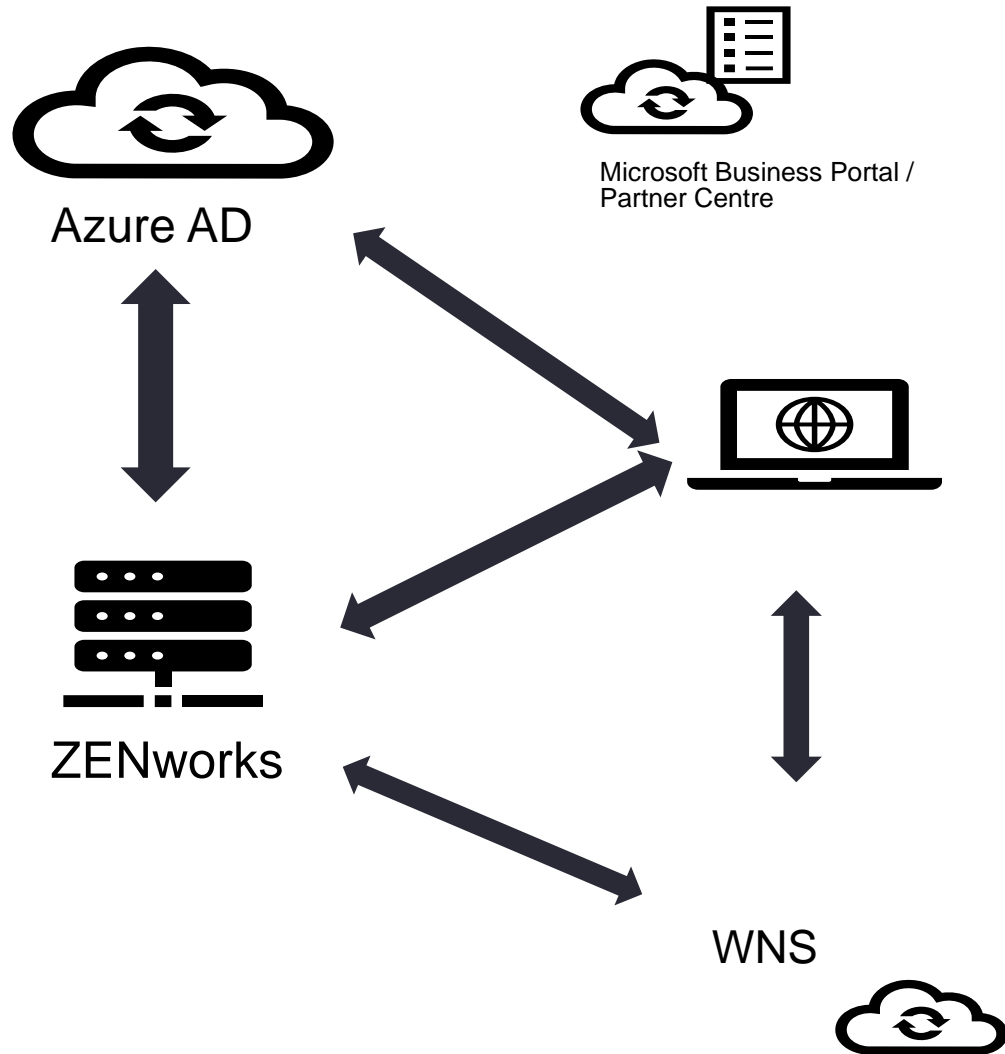


What is Windows Autopilot ?

- Setup & pre-Configure new devices
- Allows reset, repurpose & recover devices
- Leverages OEM version of Windows without needing to re-image the device
- Allows Skipping of panes during Setup and restriction of Admin Account creation
- Once device is setup, it can be managed through Windows MDM



ZENworks & Windows Autopilot - Prerequisites



Configuration

In ZENworks

- Configure ZENworks to communicate with WNS
- Configure ZENworks to communicate with Azure AD using Azure AD MDM Application
- Create a Terms of Use Policy in ZENworks

Outside ZENworks

- Upload / Ask Vendor for Device List in MS Partner Centre
- Create an Auto Pilot Profile in MS Partner Centre
- Ensure ZENworks Root CA certificate is either installed or trusted by device
- Make sure User has licenses assigned in Azure and is part of user scope linked to Azure AD MDM Application
 - More details are [here](#) about Azure licensing

ZENworks & Windows Autopilot - Setup

- Configure Windows Push Notification Service in ZENworks
- This requires a onetime creation of Microsoft Developer Account

[Configuration](#) > Windows Notification Service

Windows Notification Service

Configure Windows Notification Service to communicate with Windows 10 devices.

Windows Notification Service Configuration

To enable ZENworks to communicate with Windows 10 managed devices using Modern Management, Windows Notification Service (WNS) should be configured.

To configure WNS, you need to create a Windows app in the [Microsoft Developer portal](#).

After creating the app, note down the Package Full Name (PFN), Package SID and Application Secret associated with the app. Specify these details while configuring WNS in the section below.

For more information, see the [Online Documentation](#).

Important: Creation of a Windows app in the Microsoft Developer portal requires a paid subscription from Microsoft.

i If ZENworks MDM servers are behind a corporate Firewall, then ensure that the servers are connected to the WNS servers through TCP port 443.

Edit Configuration

Package Family Name(PFN): 49323ZENworksDevelopmentT.forDocTeam_1mjmn4jr5vbc2

Package SID: ms-app://s-1-15-2-3529616055-4044007213-4247776934-532728179-3587883396-2296632434-3229047325

Application Secret: *****

Test Configuration

OK

Cancel

ZENworks & Windows Autopilot - Setup

Home > olytest13 | Mobility (MDM and MAM) >

Configure

VikramZCM

Save Discard Delete

MDM user scope

None **Some** All

Groups

1 group selected

MDM terms of use URL

<https://zcm2020u2.zorg.co.in:443/zenworks-winmdm-tou/index.jsp> ✓

MDM discovery URL

<https://zcm2020u2.zorg.co.in:443/zenworks-win-mdm/registration/disc...> ✓

On-premises MDM application settings

Home > olytest13 | Mobility (MDM and MAM) > Configure >

VikramZCM

Search (Ctrl+/)

Delete Endpoints

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : VikramZCM

Application (client) ID : b9c20678-e0b5-493f-9dc-d-2afceb7a58f7

Directory (tenant) ID : 83fb08c6-612c-474d-8ba5-2a0563147403

Object ID : 61cc3677-3f41-4a38-aa22-0074136addf7

Supported account types : My organization only

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : <https://zcm2020u2.zorg.co.in>

Managed application in l... : VikramZCM

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Configuration > Configure Azure MDM Application

Configure Azure MDM Application

Enable ZENworks to manage Windows 10 MDM devices and enforce Intune App Protection Policies

Azure MDM Application

To enroll Windows 10 devices and enforce Intune App Protection Policies, you must create an MDM Application in the Azure portal. For more information on creating an MDM Application, see [Online Documentation](#). Note: Creating an MDM Application requires a paid subscription from Microsoft.

Add Application Remove Application

Application Name	Application ID
<input type="checkbox"/> ZCM2020U2TTP	b00956eb-98c2-4d44-8564-4f6de574c
<input type="checkbox"/> VikramZCM	b9c20678-e0b5-493f-9dc-d-2afceb7a5

OK

Azure MDM Application

MDM Server
Select a Primary Server to manage Windows 10 devices that are enrolled through Azure AD MDM Application.

MDM Server: [/Devices/Servers/zcm2020u2](#)

MDM Application
Sign into [Azure](#) and create an on-premise MDM Application. When prompted in the Azure portal, use the following URLs:

Terms of Use URL: <https://zcm2020u2.zorg.co.in:443/zenworks-winmdm-tou/index.jsp> Copy URL

Discovery URL: <https://zcm2020u2.zorg.co.in:443/zenworks-win-mdm/registration/discovery/service> Copy URL

Access Token
While creating or editing the MDM Application in the Azure portal, use the following redirect URL. Make a note of the application details such as the Application ID, Tenant ID and Application Password (Client Secret). Click the Generate Token button displayed below and specify the application details.

Redirect URL: <https://zcm2020u2.zorg.co.in:443/zenworks/MicrosoftGraphCallback> Copy URL

Edit Token... Test Token Renew Token...

Token details:

User Name: harsh

User Email: harsh@olytest13.onmicrosoft.com

Tenant Name: olytest13

Tenant ID: 83fb08c6-612c-474d-8ba5-2a0563147403

Application Name: VikramZCM

Application ID: b9c20678-e0b5-493f-9dc-d-2afceb7a58f7

Permissions: DeviceManagementApps.ReadWrite.All, Directory.AccessAsUser.All, Group.Read.All, User.Read.All, profile, openid, email

OK Cancel

- Create a Mobility (MDM & MAM) application in Azure AD
- Configure ZENworks to communicate with Azure AD using Azure AD MDM Application

ZENworks & Windows Autopilot - Setup

- Create a Terms of Use Policy in ZENworks
- Add Languages as per your end user needs

The screenshot shows the 'Edit Terms of Use' dialog box in the ZENworks interface. The dialog has the following fields:

- Title:** Zorg Terms of Use
- Language:** English
- Ownership:** Corporate
- Terms of Use Content:** A text area containing the following text:
END USER LICENSE AGREEMENT
ZENworks 2020 Suite 2017
ZENworks 2020 Configuration Management 2017
ZENworks 2020Asset Management 2017
ZENworks 2020 Full Disk Encryption 2017

The background shows the 'Terms of Use' policy page with a table of languages and ownership:

Language	Ownership
English	Corporate
Dutch	Corporate
Deutsch	Corporate

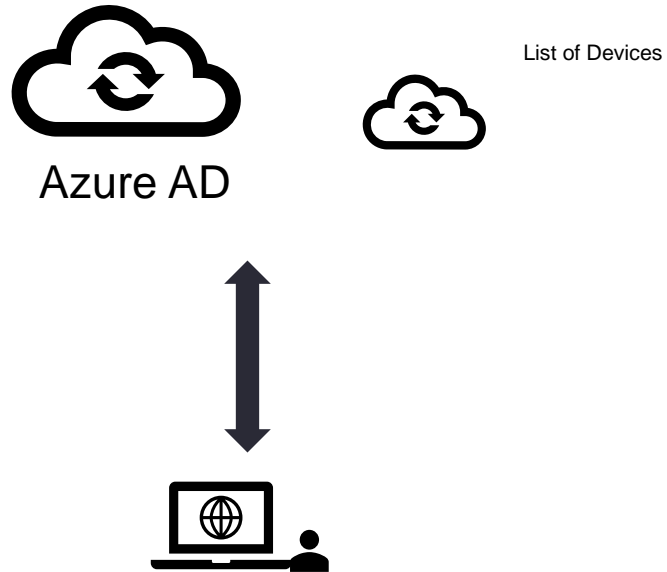
ZENworks & Windows Autopilot - Setup

- Provision Purchased Devices in [Microsoft Business Store](#)
- Ask OEM Vendor / Reseller to upload details
- If not purchased, device details can be extracted using [PowerShell](#) script and uploaded
- Create an Auto Pilot Profile and assign it to purchased devices

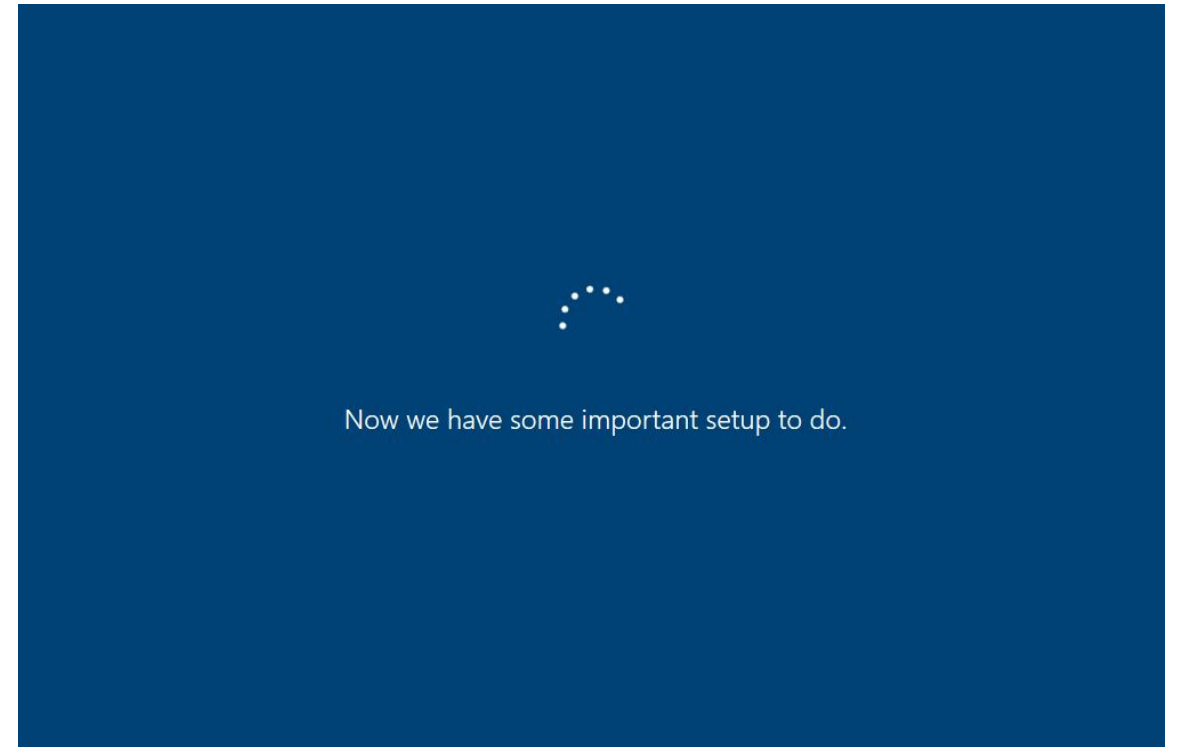
The screenshot shows the Microsoft Store for Business interface. The top navigation bar includes 'Shop for my group', 'Private store', 'Manage', and 'Find a solution provider'. The left sidebar lists various options: Home, Quotes, Products & Services, Billing accounts, **Devices**, Billing & payments, Order history, Partners, Permissions, Settings, and Support. The main content area is titled 'Manage / Devices / All devices'. It shows a search bar, a 'Refine results' section with filters for Profile, Group, and Order number, and a table of devices. The table has columns for Device model, Profile, Serial number, Windows product ID, and Date added. Two devices are listed: VMWare7,1 with profile VikramTTP Profile and VMWare7,1 with profile Harsh-Profile1. Below the table, there are buttons for '+ Add devices', 'AutoPilot deployment', and 'Remove devices'.

The screenshot shows the 'Edit profile' page in the Microsoft Store for Business. The top navigation bar is the same as the previous screenshot. The left sidebar is also the same. The main content area is titled 'Manage / Devices / Edit profile'. It shows a dropdown menu for 'VikramTTP Profile'. Below this, there are several settings for 'AutoPilot deployment default features'. The settings are: 'Skip Cortana, OneDrive and OEM registration setup pages' (On), 'Automatically setup for work or school' (On), 'Sign in experience with company brand' (On), 'Skip privacy settings' (On), 'Disable local admin account creation on the device' (On), and 'Skip End User Licence Agreement (EULA)' (On). At the bottom, there are buttons for 'Cancel', 'Save', and 'Delete profile'. A note at the bottom states: 'Profile changes are applied to devices that have not been through setup or the next time Windows is installed on the device.'

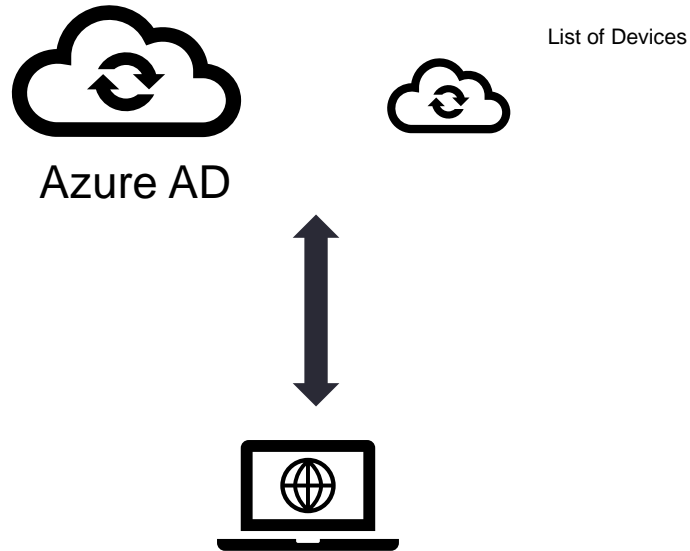
ZENworks & Windows Autopilot - Enrolment



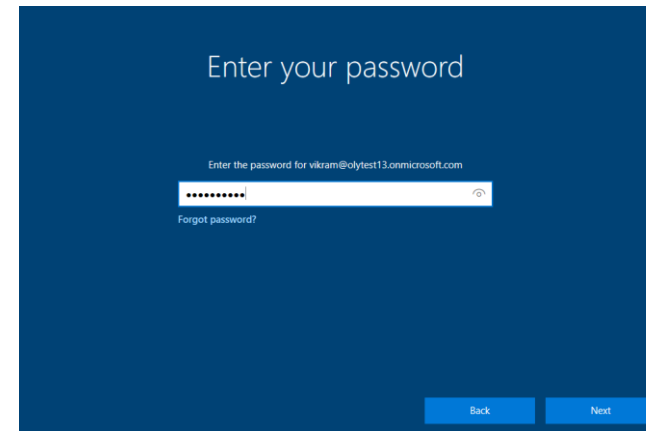
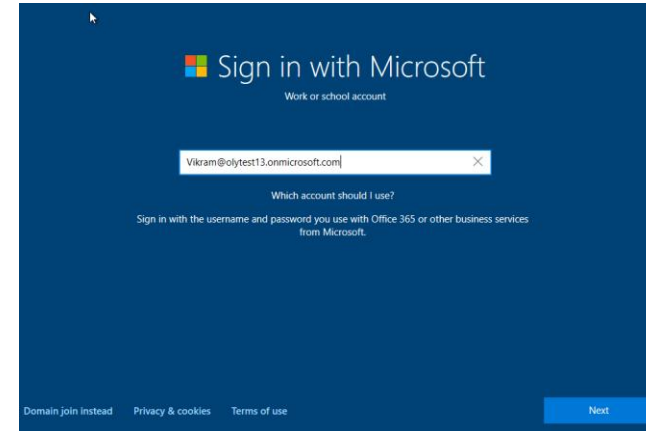
1. While setting up, Windows queries and identifies that device is registered with Autopilot



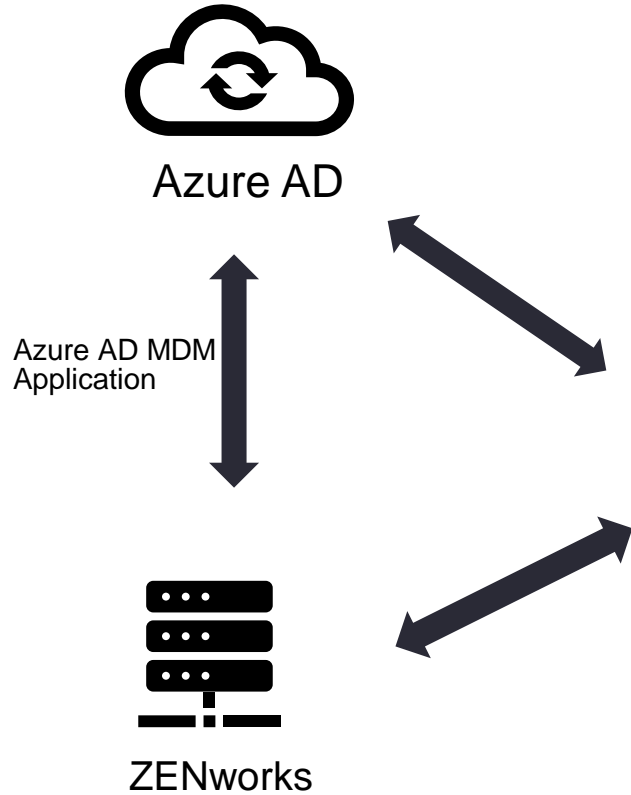
ZENworks & Windows Autopilot - Enrolment



2. User logs in with Azure AD creds and is Authenticated



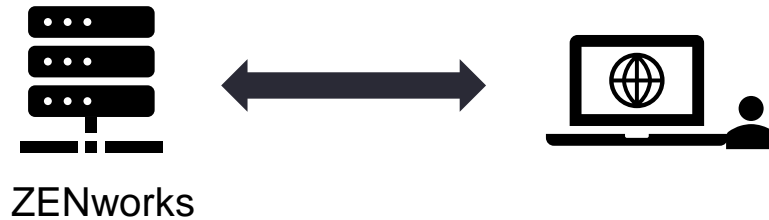
ZENworks & Windows Autopilot - Enrolment



3. Based on user, appropriate MDM App is looked up in Azure and corresponding ZENworks URL's are passed to device

ZENworks & Windows Autopilot - Enrolment



4. Device contacts ZENworks and is presented with Terms of Use



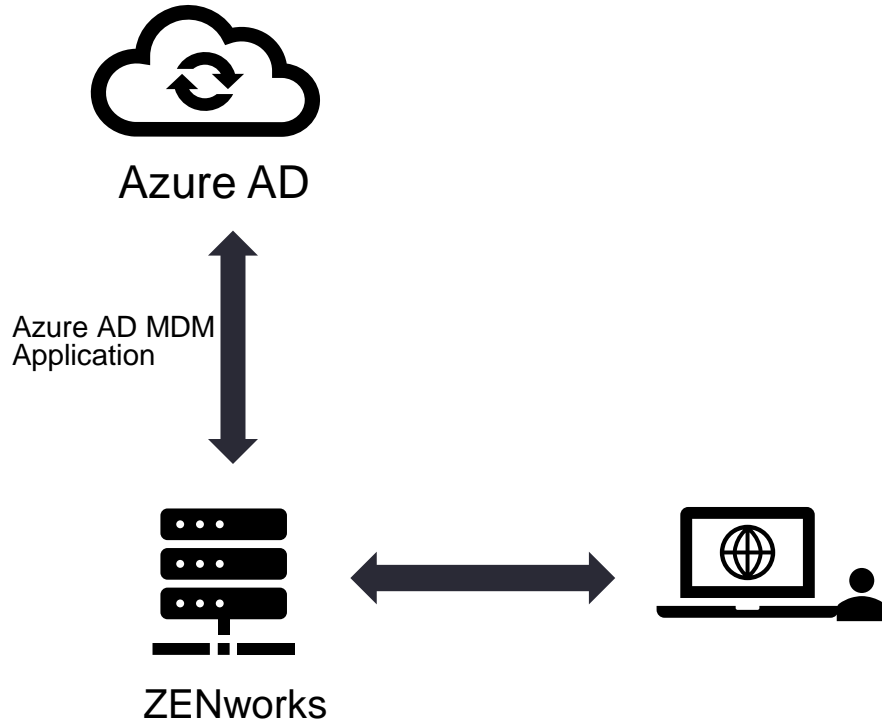
ZENworks®
Zorg Terms of Use

END USER LICENSE AGREEMENT
ZENworks 2020 Suite 2017
ZENworks 2020 Configuration Management 2017
ZENworks 2020Asset Management 2017
ZENworks 2020 Full Disk Encryption 2017
ZENworks 2020 Patch Management 2017
ZENworks 2020 Endpoint Security Management 2017
ZENworks 2020 Asset Inventory for Linux
ZENworks 2020 Asset Inventory for Mac/Windows
ZENWORKS 2020 CONFIGURATION MANAGEMENT 2017 MOBILE DEVICE

IMPORTANT: LICENSOR IS PROVIDING THIS LICENSED SOFTWARE TO LICENSEE (THE ORIGINAL PURCHASER EITHER AS AN INDIVIDUAL OR ON BEHALF OF ANOTHER LEGAL ENTITY AS ITS EMPLOYEE OR AUTHORIZED AGENT) FOR ITS USE SUBJECT TO LICENSEE'S AGREEMENT TO THE TERMS AND CONDITIONS SET FORTH BELOW. THESE TERMS AND CONDITIONS MAY BE DIFFERENT FROM THE END USER LICENSE AGREEMENT(S) THAT ACCOMPANIED EARLIER RELEASES OF THE LICENSED SOFTWARE. PLEASE READ THEM CAREFULLY TO ENSURE FULL UNDERSTANDING BEFORE PROCEEDING, AS THEY MAY CONTAIN ADDITIONAL RESTRICTIONS ON YOUR USE OF THE SOFTWARE. PLEASE DIRECT ANY QUESTIONS TO THE MICRO FOCUS LEGAL DEPARTMENT AT LEGALDEPT@MICROFOCUS.COM. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU WILL NOT BE AUTHORIZED TO USE THE LICENSED SOFTWARE. BY CLICKING THE ACCEPT BUTTON OR SIMILAR ACCEPTANCE MECHANISM DURING INSTALLATION, OR BY COPYING OR USING THE LICENSED SOFTWARE, LICENSEE ACKNOWLEDGES THAT IT HAS READ THIS LICENSE AGREEMENT, UNDERSTOOD IT, AND AGREED TO BE BOUND BY ITS TERMS AND CONDITIONS. THE LICENSED SOFTWARE IS

 English 

ZENworks & Windows Autopilot - Enrolment



5. ZENworks validates details with Azure and enrolls Device

6. ZENworks sets Device Status in Azure

Devices > Workstations > DESKTOP-B51E29B

DESKTOP-B51E29B

Summary	Inventory	Assignments	Memberships	Settings	Content	Locations	Audit	Antimalware	Geolocation	Patches
General										
Alias:	DESKTOP-B51E29B									
Host Name:	DESKTOP-B51E29B									
IP Address:										
Last Full Refresh:	N/A									
Last Contact:	N/A									
ZENworks Agent Version:	N/A									
ZENworks Updater Service Last Contact Time:	N/A									
ZENworks Updater Service Version:	N/A									
ZENworks Agent Status:	Unable to connect to the agent service through the IP Address or DNS.									
MDM Enrolled:	Yes									
MDM Agent Version:	10.0.18363.0									
MDM Agent Sync Time:	2:37 PM									
MDM Enrolment Mode:	Azure AD Join									
Operating System:	Microsoft Windows 10 Enterprise x64 Version 1909 Build 18363									

Microsoft Azure

Home > olytest13 >

Devices | All devices (Preview)

olytest13 - Azure Active Directory

« ✓ Enable ⚙ Disable 🗑 Delete ⚙ Manage ↻ Refresh 📄 Columns ❤ Got feedback?

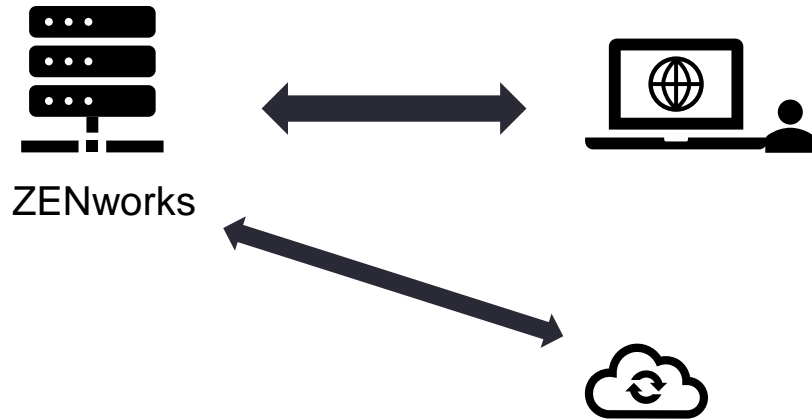
Want to switch back to the legacy filtering experience? Click here to leave the preview. →

You can use the activity timestamp to efficiently manage stale devices in your environment. Learn more

DESKTOP-B51E29B Add filters

Name	Enabled	OS	Version	Join Type	Owner
DESKTOP-B51E29B	Yes	Windows	10.0.18363.0	Azure AD joined	gvikram

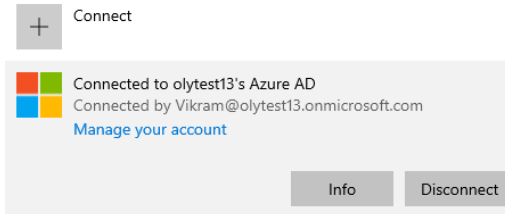
ZENworks & Windows Autopilot - Enrolment



7. Device gets Setup and sync is initiated with ZENworks

Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



Managed by ZENworks

Connecting to work or school allows your organization to control some things on this device, such as settings and applications.

Areas managed by ZENworks

ZENworks manages the following areas and settings. Settings marked as Dynamic might change depending on device location, time, and network configuration.

[More information about Dynamic Management](#)

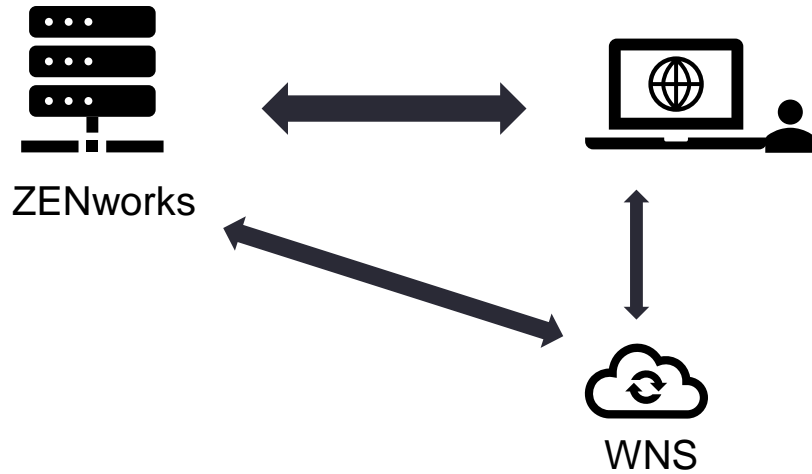
Connection info

Management Server Address:
<https://zcm2020u2.zorg.co.in/endpoint/windowsmdm/sync>
Exchange ID:
2138DECBF9474EDF48F8DF9E4132E2B1

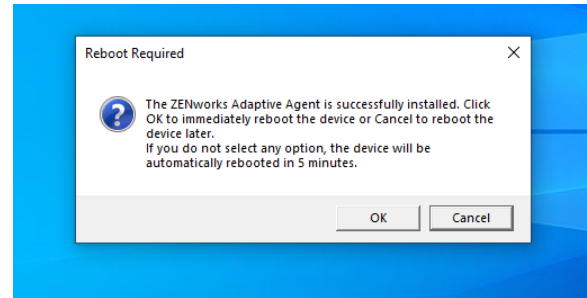
Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.
Last Attempted Sync:

ZENworks & Windows Autopilot – Deployment of ZENworks Agent (Optional)



8. If assigned, on sync, ZENworks Agent gets installed on device along with any other provisioned application



Devices > Workstations > DESKTOP-B51E29B

DESKTOP-B51E29B

Summary	Inventory	Assignments	Memberships	Settings	Content	Locations	Audit	Geolocation	Patches
General									
Alias:	DESKTOP-B51E29B								
Host Name:	DESKTOP-B51E29B								
IP Address:	172.17.2.23 169.254.67.97 fe80::8473:2ba4:54:a20d fe80::e016:fd42:7fe2:4361								
Test Device:	No Set								
Last Full Refresh:	4:19 PM								
Last Contact:	20.2.0.506								
ZENworks Agent Version:	N/A								
ZENworks Updater Service Last Contact Time:	20.2.0.506								
ZENworks Updater Service Version:	20.2.0.506								
ZENworks Agent Status:	Yes								
MDM Enrolled:	10.0.18363.0								
MDM Agent Version:	4:20 PM								
MDM Agent Sync Time:	Azure AD Enrollment								
MDM Enrolment Mode:	Microsoft Windows 10 Enterprise x64 Version 1909 Build 18363								
Operating System:	0								
Number of errors not acknowledged:	0								
Number of warnings not acknowledged:	No user sources configured								
Primary User:	Owner: Edit								
Owner:	Serial Number								
Serial Number	564d623c6b70aaad5c2b9de283192e58								
GUID:	df3b60a25547096695c253b21b3ba7e2								
Department:	Site								
Site:	Location								
Location:	Message Log								

A composite image of Earth from space. The Earth's horizon is visible on the right, with a bright orange and yellow glow from the sun. The Earth's surface is covered in blue oceans and white clouds. In the upper left, the Moon is visible as a blue sphere. A large, semi-transparent green plus sign is overlaid on the image, centered in the upper half.

Capabilities

Modern Management Capabilities

- Basic Management – Device Refresh, Un-enrolment, Deletion
- Deployment of ZENworks Agent through Win 10/11 Modern Management
- Deployment of MSI Applications to devices (Experimental)
- Deployment of any CSP (Experimental)
- [ZENworks CSP Repository](#)



opentext™

Thank you

 twitter.com/opentext

 linkedin.com/company/opentext

 opentext.com