Deploy Windows 10 in an enterprise

What IT professionals need to know to successfully deploy Windows 10 in their enterprise environments.

This topic is 1 of 6 in a series 1 2 3 4 5 6

To successfully deploy the Windows 10 operating system in your organization, it is important to understand the different possibilities, especially now that there are new scenarios to consider. Choosing among these scenarios, and understanding the key capabilities and limitations of each, is a key task.

Deploying Windows 10

Deployment scenarios

Pick the scenario that suits your environment most, to deploy Windows 10.

Windows AutoPilot:
Quickly and Simply set up devices without using images

2

In-place upgrade:
Keep your data, apps, and settings while moving from older Windows versions

3

Clean installation:
Install Windows 10 cleanly, if other scenarios aren't available to you

4

Protecting Windows 10

Protection solutions

Find the full range of solutions to protect your Windows 10 devices.

5

Out-of-box protection:
Review the strong, baseline protections included with Windows 10

Increased protection:
Protect higher risk data or environments with a set of increased protections that can be easily turned on

Updating Windows 10

Windows servicing

Understand how to keep your Windows 10 devices up-to-date.

6

Servicing model:
Plan and execute different update deployment rings for different audiences within your organization

Servicing tools:
Choose the best option to update devices in your environment

Microsoft

Deploy Windows 10 in an enterprise: Windows AutoPilot

What IT professionals need to know to successfully deploy Windows 10 in their enterprise environments.

Windows AutoPilot is a collection of solutions that enables you to set up and pre-configure new and existing Windows 10 devices. Users in your environment will go through a new operating system out-of-the-box experience(OOBE), without needing a Windows image.

Windows AutoPilot scenarios

Cloud-Driven: Use the Windows AutoPilot Deployment program to fully configure devices

IT-Driven: Use the Windows Configuration Designer to automate provisioning with a high degree of control

Teacher-Driven: Use the Set Up School PCs app as a simpler solution for simpler scenarios

Windows AutoPilot Deployment program

Pre-register devices to be fully configured based on a device profile that includes skipping OOBE steps, MDM auto-enrollment, and app installation.

Requirements:
- Devices registered to your organization
- Devices with internet access
- Windows 10, version 1703, or later
- Azure AD Premium P1 or P2
- Microsoft Intune or 3rd party MDM

Register devices to your organization through Microsoft Store for Business or Partner Center

- Create device profiles
- Configure settings for device profiles
- Configure MDM auto-enrollment through Azure AD

Device will be fully configured after going through customized OOBE

Windows Configuration Designer

Create provisioning packages that contain configuration and customization settings. Apply these packages to setup your Windows 10 devices.

Requirements:
- Target devices have Windows 10 installed
- Management station is Windows 7 \ Windows Server 2008 R2 or later

Install WCD through the Store or Windows ADK

- Create provisioning package
- Select and configure desired settings
- Build the provisioning package

Apply provisioning packages through USB drive or a network location

Set up School PCs

IT administrators and technical teachers can use the Set up School PCs app to quickly and simply set up PCs for students.

Requirements:
- Set up School PCs app
- Connectivity to internet and school network on the administrator's machine
- an Administrator account on Office 365 and Azure Active Directory
- Microsoft Store for Education configured
- USB drive of 1 GB or larger

Install the Set up School PCs through the Store

- Sign-in with your administrator account
- Configure initial device settings
- Pick apps to provision
- Save package to USB drive

Apply package through USB drive

Cloud-Driven points of consideration

- Easily scalable
- No on-premises infrastructure required
- Simple configuration and customization
- Most controls available through Microsoft Intune or other MDM solutions

IT-Driven points of consideration

- Highest degree of control on initial provisioning
- Does not require any cloud resources
- Hard to scale without additional infrastructure
- Lowest requirements to get started

Teacher-Driven points of consideration

- Suited for smaller or simpler environments
- Limited scalability due to USB drive reliance
- Simplest configuration experience
- Some education cloud resources are required

For more information on this topic, visit aka.ms/WindowsAutoPilot

July 2017

Microsoft

Deploy Windows 10 in an enterprise: In-place upgrade

What IT professionals need to know to successfully deploy Windows 10 in their enterprise environments.

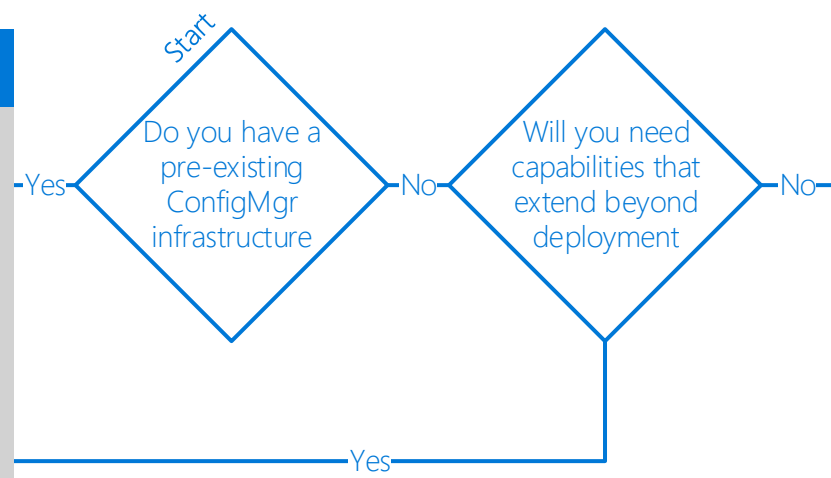
Why choose In-place upgrade

- To keep existing applications and data
- When you don't plan to significantly change the device or OS configuration
- To migrate from one Windows 10 release to another

System Center Configuration Manager Deployment

Deploy and configure Windows operating systems and Windows applications.

Requirements:
- Latest version of Configuration Manager
- Windows Server Update Services (WSUS)
- Internet Information Services (IIS)
- Dynamic Host Configuration Protocol (DHCP)



MDT Deployment

Deploy pre-configured desktop or server operating systems.

Requirements:
- Windows 7 (or above) client or Windows Server 2008 R2 (or above) server
- Windows Assessment and Deployment Kit (ADK) for Windows 10
- Windows PowerShell
- .Net Framework

Setup ConfigMgr infrastructure: ConfigMgr Server, Database, WSUS, IIS, DHCP

- Create an OS upgrade package
- Create an upgrade task sequence
- Deploy the Windows 10 in-place upgrade

Start the Windows 10 in-place upgrade task

Not available for this scenario

- Changing between Windows x86 and x64
- Systems using Windows To Go or Boot from VHD
- Dual boot and multi-boot systems

Install Windows ADK for MDT

- Create a deployment share
- Add Windows 10 setup files and applications
- Create an upgrade task sequence

Deploy the Windows 10 in-place upgrade

ConfigMgr points of consideration

- Relatively high infrastructure requirements
- Scalable for large environments
- Multiple roles and capabilities allow for a higher degree of control
- Initial setup and configuration takes a substantial amount of time

Visit aka.ms/ConfigMgrInplace for additional information.

Key points

- ConfigMgr offers more capabilities at an additional infrastructure and management cost
- MDT is simpler, but is focused strictly on the OS deployment process

MDT points of consideration

- Low infrastructure requirements
- Hard to manage at a large scale
- Capabilities limited to OS deployment
- Relatively short time to first deployment

Visit aka.ms/MDTinplace for additional information.

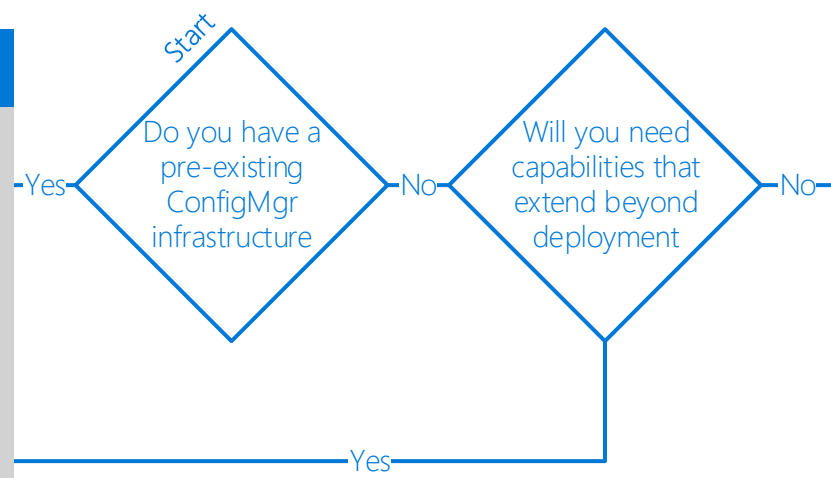
Microsoft

Deploy Windows 10 in an enterprise: Clean installation

What IT professionals need to know to successfully deploy Windows 10 in their enterprise environments.

Why choose clean installation

- To deploy to a significant number of devices in a short period of time
- To move between an x86 and an x64 architecture
- When in-place upgrade isn't possible



System Center Configuration Manager Deployment

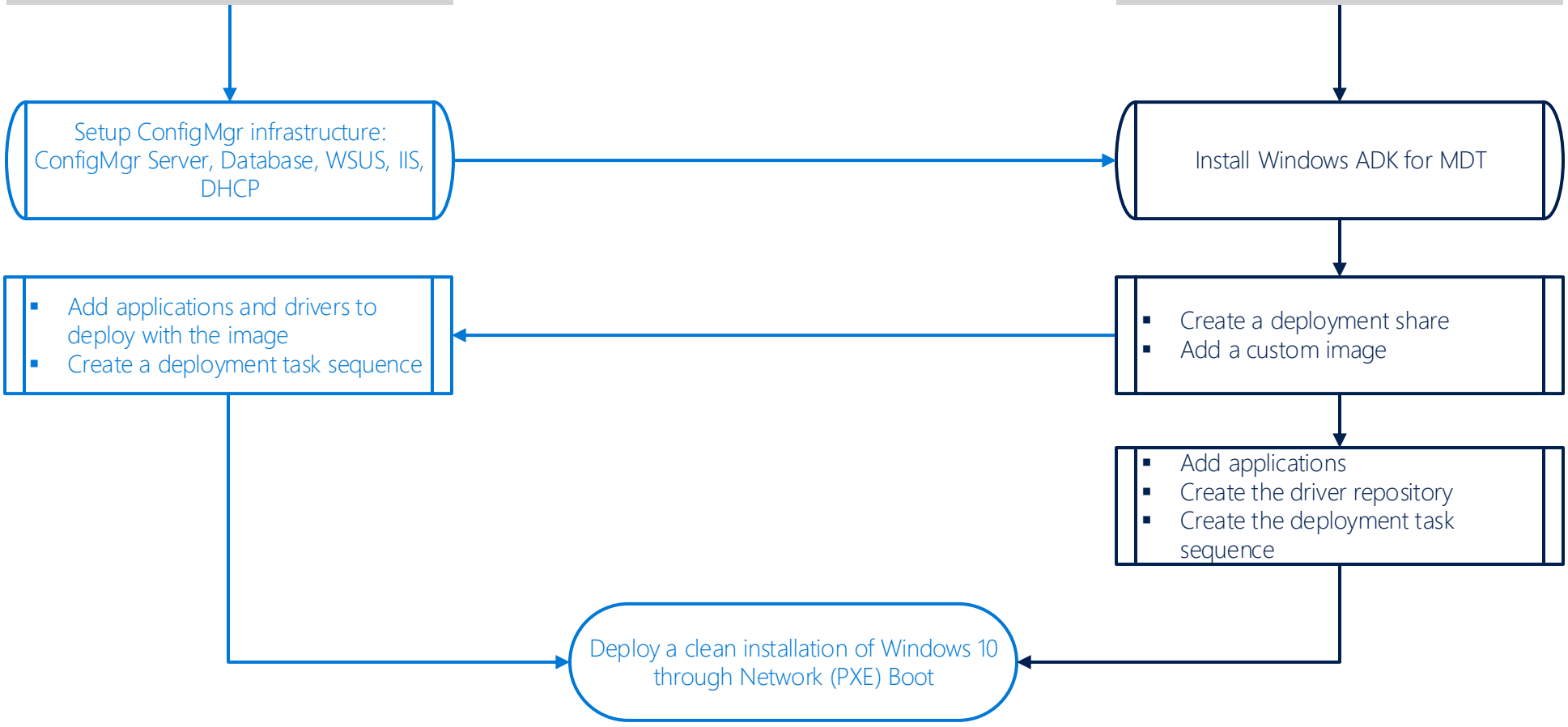
Deploy and configure Windows operating systems and Windows applications.

Requirements:
- Windows ADK for Windows 10
- Latest version of Configuration Manager
- Windows Server Update Services (WSUS)
- Internet Information Services (IIS)
- Dynamic Host Configuration Protocol (DHCP)

MDT Deployment

Deploy pre-configured desktop or server operating systems.

Requirements:
- Windows 7 (or above) client or Windows Server 2008 R2 (or above) server
- Windows Assessment and Deployment Kit (ADK) for Windows 10
- Windows PowerShell
- .Net Framework



ConfigMgr points of consideration

- Relatively high infrastructure requirements
- Scalable for large environments
- Multiple roles and capabilities allow for a higher degree of control
- Initial setup and configuration takes a substantial amount of time

Visit aka.ms/ConfigMgrDeploy for additional information.

Key points

- MDT is required to create the custom image
- ConfigMgr offers more capabilities at an additional infrastructure and management cost
- MDT is simpler, but is focused strictly on the OS deployment process

MDT points of consideration

- Low infrastructure requirements
- Hard to manage at a large scale
- Capabilities limited to OS deployment
- Relatively short time to first deployment
- Some MDT configuration will be required either way

Visit aka.ms/MDTdeploy for additional information.

Microsoft

Deploy Windows 10 in an enterprise: Protection solutions

What IT professionals need to know to successfully implement Windows 10 protection capabilities in their enterprise environments.

Two tiers of protection for Windows 10 devices

Windows 10 includes many protection capabilities. We know it can be challenging to implement the right set of capabilities for your organization.

Our capabilities are recommended in two tiers — out-of-box protection and increased protection that you can turn on to strengthen your protections.

It's important to use consistent levels of protection across your data, identities, and devices. For example, if you turn on some of the increased protections for your data, you must also protect the identities and devices that access this data at a comparable level.

For full protection, use Windows 10 capabilities together with capabilities in Enterprise Management + Security (EMS) and Office 365. For more information, see these companion documents:

File Protection Solutions in Office 365

Identity and Device Protection for Office 365 and other SaaS Services

1 Out-of-box protection

Microsoft provides advanced security for protecting data, as well as the identities and devices that access your data. Windows 10 includes strong, out-of-the box baseline protections, which will meet the needs of many organizations. For organizations that need more protection than the baseline, there are the increased security features, which can be turned on alongside the out-of-box protections.

2 Increased protection

Some customers have a subset of users that must be protected at higher levels because they have access to sensitive data or they are greater targets for attackers. You can apply increased protection to specific users in your organization.

Summary of capabilities

Out-of-box protection

Windows Defender System Guard
Helps maintain and validate the integrity of a device's firmware, operating system, and system defenses by ensuring that only trusted software can run during start-up.

Windows Defender Exploit Guard
Includes a series automatic mitigations designed to block vulnerability exploit techniques that can let an attacker inject malicious code into a system to gain control of apps or the system itself.

Windows Defender Firewall
Protects against unauthorized access.

Windows Defender Antivirus
Uses the power of the cloud, wide-optics, precise machine learning models, and behavior analysis to protect devices from emerging threats, in real-time.

Windows Defender SmartScreen
Checks for malicious apps and sites, warning and blocking users from accessing content that could harm their devices.

BitLocker Encryption*
Auto-encrypts all data at rest on the device and protects it against offline attacks. No provisioning required.

* Only available on InstantGo devices.

Windows updates
Protects against new threats.

Increased protection

Windows Defender System Guard (with optional features enabled)
Allows sensitive services and data to be isolated, ensuring low-level tampering can be detected and remediated without impact.

Windows Defender Exploit Guard (with optional features enabled)
Uses a set of intrusion prevention capabilities to reduce the attack and exploit surface of apps; helping to prevent attacks from security threats, such as ransomware.

Windows Defender Application Guard
Malware and hacking threats encountered online while using Microsoft Edge won't be able to compromise the device, apps, data, or the broader business network.

Windows Defender Application Control
Helps address malware threats by enabling your IT department to decide which trusted software vendors and apps can run on devices.

Windows Defender Device Guard
Uses Hypervisor Code Integrity (HVCI) from Windows Defender Exploit Guard plus the "allow listing" feature from Windows Defender Application Control to provide advanced tamper-proofing for the system core and application control policies.

BitLocker Encryption
Allows provisioning of a customized encryption configuration on the broadest range of Windows device types; protecting data at rest on the device against offline attacks.

Windows Information Protection
Protects enterprise apps and data against accidental data leak on enterprise-owned devices and personal devices.

Windows Defender Advanced Threat Protection
Helps detect, investigate, and respond to advanced attacks on your networks.

Windows Defender Credential Guard
Uses virtualization-based security and Windows Defender System Guard container technology to isolate the Windows authentication stack and user secrets (such as, NTLM and TGT), so they can remain secure even if the operating system is compromised.

Windows Hello
Replaces passwords with strong two-factor authentication, providing instant access to your Windows 10 devices using fingerprint or facial recognition.

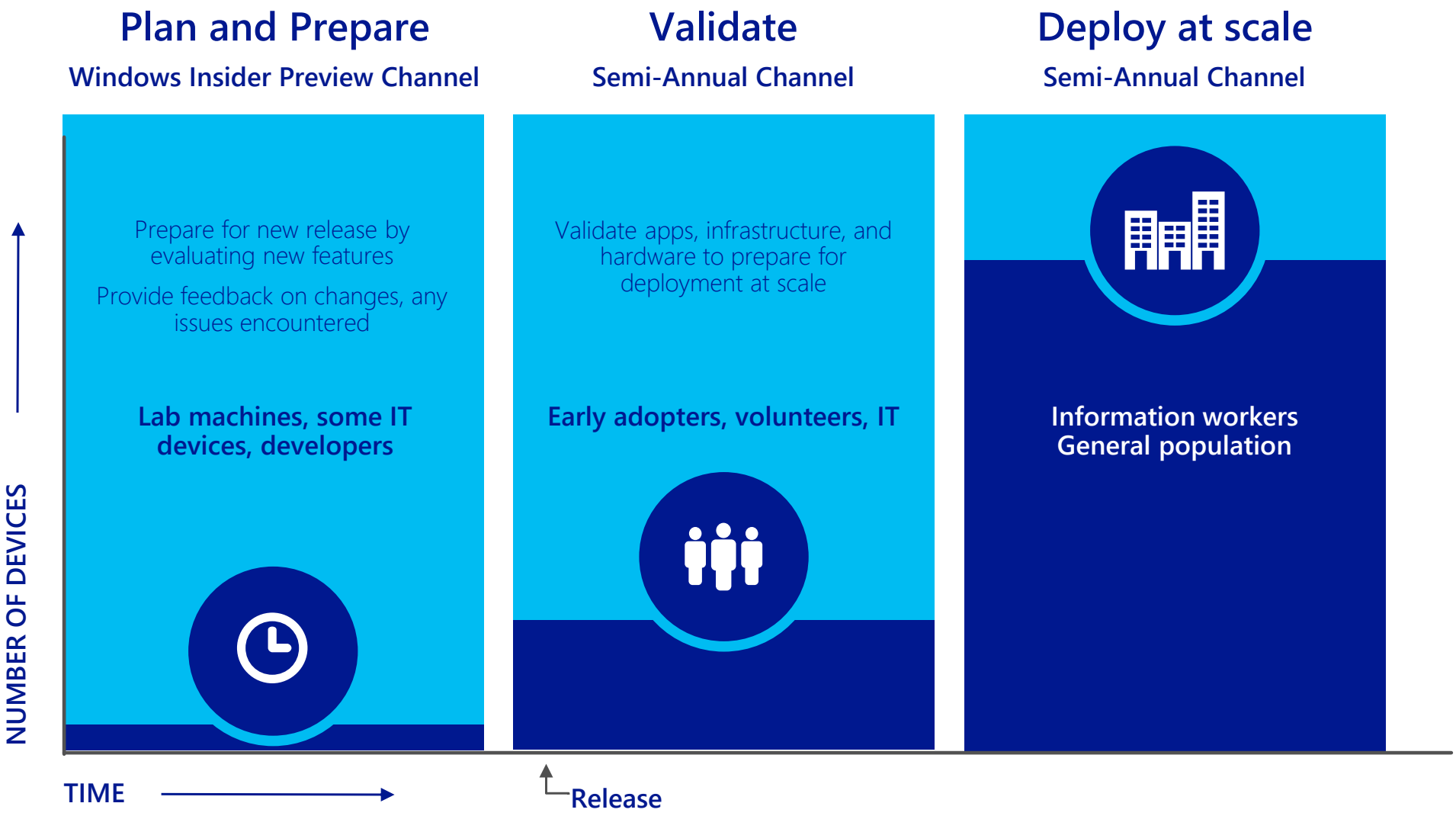
Microsoft

Deploy Windows 10 in an enterprise: Windows servicing

What IT professionals need to know to successfully update Windows 10 in their enterprise environments.

This topic is 6 of 6 in a series 1 2 3 4 5 6

Keep Windows up to date with the latest productivity and security capabilities, with a predictable semi-annual feature update cycle, and monthly cumulative updates containing security and functionality fixes.



Servicing tools available to update Windows 10

Multiple servicing tools to implement Windows as a service. Each option offers similar base capabilities with ranging control options, to offer simplicity and low administrative requirements when appropriate, and enhanced controls when they are required.

Windows Update

- Limited control over updates
- Requires IT Pros to manually configure devices
- Lowest administrative requirements
- Very hard to control in large environments

Windows Update for Business

- Enhanced controls over Windows Update
- Offers the option to defer and pause update rollout
- Controls available through Group Policy, MDM, and through User Interface in the Settings app
- No infrastructure requirements

Windows Server Update Services

- Extensive controls over update delivery, including the ability to time update delivery
- Option to easily create device deployment groups
- Option to create an approval layer
- Requires a minimum of one server to function

System Center Config Manager

- Greatest control over update delivery
- Biggest administrative requirements
- Can be used to deploy and configure devices
- Contains options of all other tools available

For more information on this topic, visit aka.ms/WaaS