Deploy a modern and secure desktop with Microsoft

Architect end-to-end solutions for deployment, protection, and change management of the modern desktop with Windows 10 and Office 365 ProPlus.

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

For more architecture resources like this, see aka.ms/cloudarch.

Deploy and manage Windows 10 and Office 365 ProPlus on the modern and secure desktop

Create the modern and secure desktop by deploying Windows 10 and Office 365 ProPlus in your organization. Use this guide to learn about Windows 10 protection capabilities and about deploying and managing updates for Windows and Office, whether it's from the cloud with Windows AutoPilot and the Office 2016 Deployment Tool, or from a local source on your network with System Center Configuration Manager.

Windows 10

The Windows 10 operating system introduces a new way to build, deploy, and service Windows: Windows as a service. Microsoft has reimagined each part of the process to simplify the lives of IT pros and maintain a consistent Windows 10 experience for you.

Office 365 ProPlus

Office 365 ProPlus is a full version of Office that's installed on client devices. It's delivered as a user-based service that allows people to access Office on up to 5 PCs or Macs and on their mobile devices. You can deploy and manage Office from the cloud or with your existing software management tools.

Implementing the modern and secure desktop solution

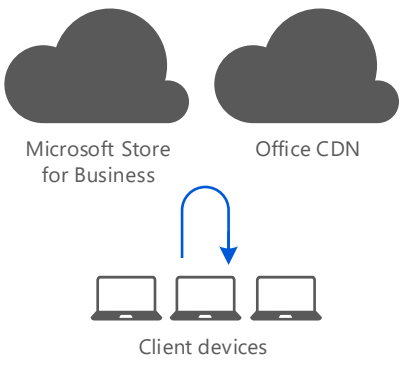
Deciding how to deploy and manage the modern and secure desktop depends on three core decisions: what action you want to take, what tools you want to use, and the location from which you want to deploy and manage Office and Windows: a local source on your network or from the cloud (Windows Store for Business and Office Content Delivery Network).

WHAT ACTION?
- ☐ Deploy
- ☐ Manage updates

WHAT TOOL?
- ☐ Windows Autopilot
- ☐ Office Deployment Tool
- ☐ Configuration Manager

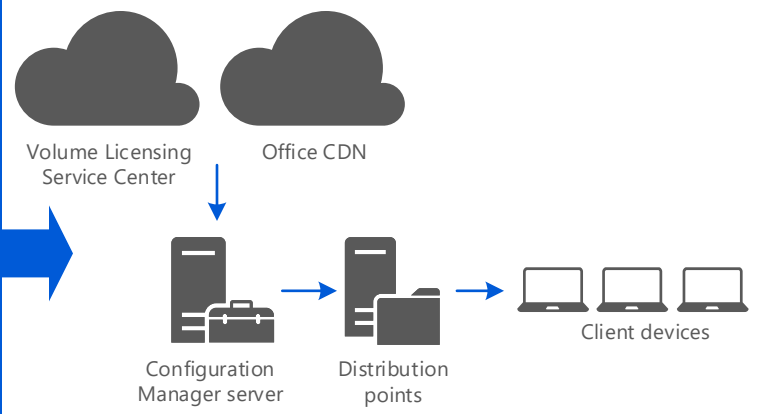
WHAT LOCATION?
- ☐ Windows cloud
- ☐ Office cloud
- ☐ Local source

Deploy from the cloud (topic 2)



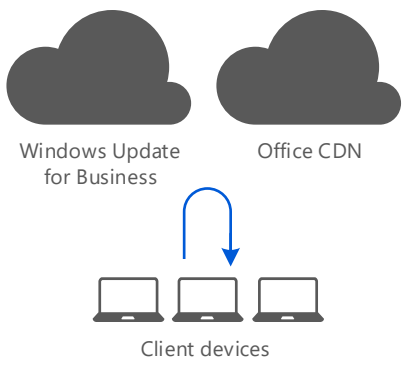
We recommend deploying Windows 10 from the cloud with Windows AutoPilot for new devices when simple configuration is all that is required, and when it can be used in combination with a mobile device management (MDM) service like Microsoft Intune. Deploying Office from the cloud is recommend for organizations or parts of organizations that want minimal administrative investment while still managing Office on the devices.

Deploy with System Center Configuration Manager (topic 3)



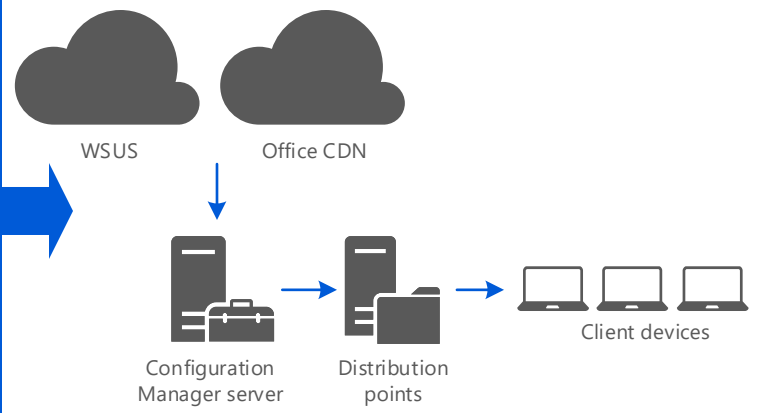
We recommend this deployment for organizations that use System Center Configuration Manager to distribute and manage software. Configuration Manager scales for large environments and enables extensive control over installation, updates, and settings.

Manage updates from the cloud (topic 4)



If you have the network capacity, we recommend managing updates automatically. Updates will be installed directly on client devices from Windows Update for Business and the Office CDN.

Manage updates with Configuration Manager (topic 4)



You can update Windows and Office with Configuration Manager by using the same workflow you use for other software updates.

Tiers of protection for Windows 10 devices (topic 5)

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.

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.

September 2017

Microsoft

Deploy a modern and secure desktop with Microsoft

Architect end-to-end solutions for deployment, protection, and change management of the modern desktop with Windows 10 and Office 365 ProPlus.

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

For more architecture resources like this, see aka.ms/cloudarch.

Deploy Windows and Office from the cloud

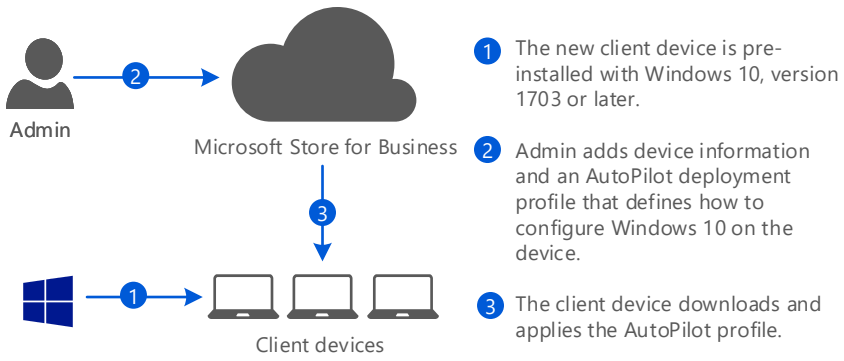
Deploy Windows 10 on new devices from the Windows Store for Business with Windows Autopilot, and deploy Office 365 ProPlus from the Office Content Delivery Network (CDN) with the Office 2016 Deployment Tool.

ACTION
- Deploy

TOOL
- Windows Autopilot
- Office Deployment Tool

LOCATION
- Windows cloud
- Office cloud

Deploy Windows 10 on new devices with Windows AutoPilot

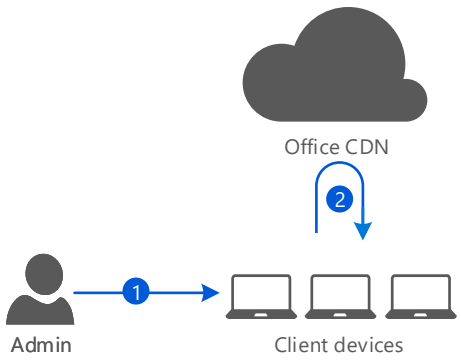


1. The new client device is pre-installed with Windows 10, version 1703 or later.
2. Admin adds device information and an AutoPilot deployment profile that defines how to configure Windows 10 on the device.
3. The client device downloads and applies the AutoPilot profile.

When deploying Windows 10 on new devices with Windows AutoPilot, the version of Windows 10 that's pre-installed on the device is automatically configured and updated based on settings defined by the admin. The deployment is scalable, with no on-premises infrastructure required, and is simple to configure and customize.

We recommend this deployment for new devices when simple configuration is all that is required, and when it can be used in combination with an MDM service like Microsoft Intune.

Deploy Office 365 ProPlus from the cloud



1. Admin sends configuration settings for Office to client devices using the Office 2016 Deployment Tool.
2. Based on configuration settings, client device downloads appropriate Office package from the Office cloud and applies settings.

When deploying Office 365 ProPlus from the Office CDN, admins retain control over the configuration and deployment options, including the appropriate update channel, architecture, applications, and languages. The Office packages are defined by the admin but delivered from the Office cloud directly to the client device. You can deploy Office from the cloud to new or existing devices.

We recommend this deployment for organizations or parts of organizations that want minimal administrative investment while still managing Office on the devices.

Assess

1. Assess your infrastructure, including system requirements, network capabilities, deployment and management tools, existing and required Office 365 components, licensing and identity requirements, current versions of Office and Windows, and required languages.

2. Assess application compatibility, including applications running on Windows 10 and third-party add-ins, complex documents, and custom VBA script running on Office 365 ProPlus.

Plan

1. Define the deployment rings for your client devices: Deployment rings determine when client devices receive feature updates for Windows 10 and Office. For example, you might create a "targeted" ring with a small group of devices that receives the Windows and Office feature updates earlier than the rest of your organization. For more control over settings and applications, you can define deployment groups within each ring.

2. Create Windows device profiles and configure MDM auto-enrollment through Azure AD. Client devices must have internet access and come pre-installed with Windows 10, version 1703 or later. Organization must have Azure AD Premium P1 or P2 and Microsoft Intune or another MDM service.

Install

1. Register the Windows client devices to your organization: To do this, upload the hardware IDs for your devices to the Microsoft Store for Business or Partner Center.

2. Device is configured automatically: When the end user turns on the device and provides an email address, it will join Azure AD automatically and auto-enroll in the MDM service. The MDM service ensures policies are applied, apps are installed, and settings are configured on the device.

3. Device is updated automatically. Windows Update for Business applies the latest updates to ensure the device is up to date.

4. Build the Office installation packages: Use the Office 2016 Deployment Tool to define an Office package for each of your deployment rings and groups, with the appropriate update channel, architecture, applications, and languages.

5. Install the Office applications: Using a script or batch file, the appropriate Office packages are downloaded from the Office CDN and installed on client devices.

6. After installing Office, add languages and Office apps: You can add language packs and additional Office apps, including Visio and Project, with the ODT.

For more details on deploying from the cloud, see: aka.ms/WindowsAutopilot
aka.ms/deploy_Office

Microsoft

Deploy a modern and secure desktop with Microsoft

Architect end-to-end solutions for deployment, protection, and change management of the modern desktop with Windows 10 and Office 365 ProPlus.

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

For more architecture resources like this, see aka.ms/cloudarch.

Deploy with System Center Configuration Manager

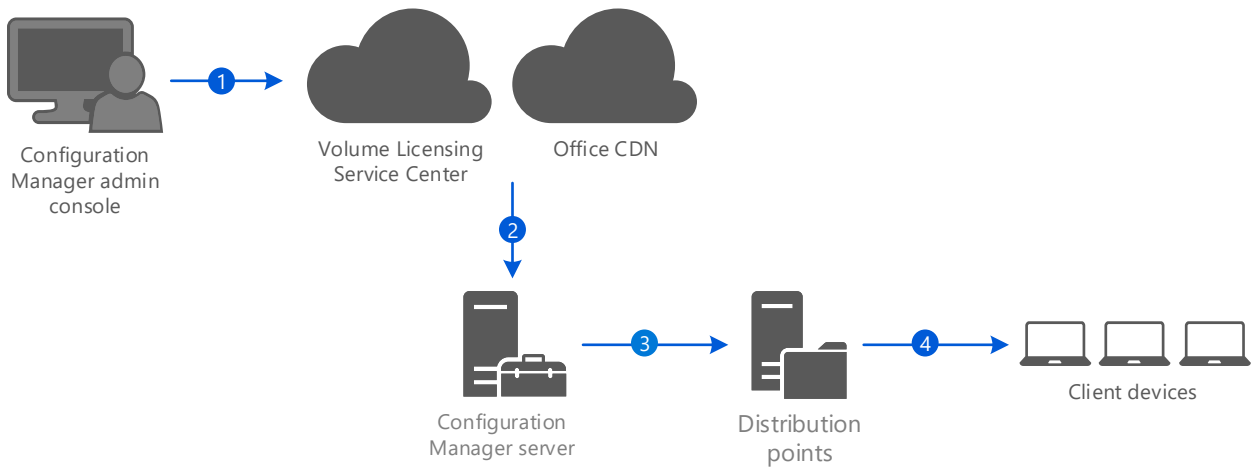
Deploy Windows 10 and Office 365 ProPlus from a local source on your network with System Center Configuration Manager.

ACTION □ Deploy

TOOL □ Configuration Manager

LOCATION □ Local source

Deploy Windows 10 and Office 365 ProPlus with System Center Configuration Manager



1. Admin configures Windows and Office deployment packages in Configuration Manager.
2. Windows 10 packages are downloaded from VLSC and Office packages are downloaded from the Office CDN.
3. Packages are sent to Configuration Manager distribution points.
4. Office and Windows are installed on client devices.

We recommend this deployment for organizations that use System Center Configuration Manager to distribute and manage software. Configuration Manger scales for large environments and enables extensive control over installation, updates, and settings.

Assess

1. Assess your infrastructure, including system requirements, network capabilities, deployment and management tools, existing and required Office 365 components, licensing and identity requirements, current versions of Office and Windows, and required languages.

2. Assess application compatibility, including applications running on Windows 10 and third-party add-ins, complex documents, and custom VBA script running on Office 365 ProPlus.

Plan

3. Define the deployment rings for your client devices: Deployment rings determine when client devices receive feature updates for Windows 10 and Office. For example, you might create a "targeted" ring with a small group of devices that receives the Windows and Office feature updates earlier than the rest of your organization. For more control over settings and applications, you can define deployment groups within each ring.

4. Choose the type of Windows deployment: Depending on the existing Windows versions and business requirements, Windows can be upgraded in-place or newly installed.

5. Download and install the required deployment tools: In addition to Configuration Manager, you need the Windows Assessment and Deployment Kit (Windows ADK), which includes the Microsoft Deployment Toolkit (MDT).

Install

1. Create a Windows 10 package: Using images from the Volume Licensing Service Center and the Windows ADK, create a custom image of Windows and add it to a deployment share. Include any required applications and drivers.

2. Create device collections: In Configuration Manager, create device collections that match your deployment rings.

3. Create a task sequence. In Configuration Manager, create deployment task sequences for each device collection. You can define task sequences to upgrade or do a clean install of Windows.

4. Deploy Windows 10. Run the deployment task sequences.

5. Build the Office installation packages: Use the Office 365 Client Installation wizard in Configuration Manager to build an Office package for each of your deployment rings and groups, with the appropriate update channel, architecture, applications, and languages.

6. Deploy the Office applications: Use the Installation wizard or a task sequence to deploy Office packages to your deployment rings and groups.

7. After installing Office, add languages and Office apps: You can add language packs and additional Office apps, including Visio and Project, by deploying them with Configuration Manager.

For more details on deploying with Configuration Manager, see: aka.ms/ConfigMgrDeploy
aka.ms/deploy_Office

September 2017

Microsoft

Deploy a modern and secure desktop with Microsoft

Architect end-to-end solutions for deployment, protection, and change management of the modern desktop with Windows 10 and Office 365 ProPlus.

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

For more architecture resources like this, see aka.ms/cloudarch.

Manage updates for Windows and Office

Manage updates for Windows 10 and Office 365 ProPlus, either from the cloud with Windows Update for Business and the Office CDN, or from a local source on your network with System Center Configuration Manager.

ACTION
- ☐ Manage updates

TOOLS
- ☐ Automated
- ☐ Configuration Manager

LOCATION
- ☐ Windows cloud
- ☐ Office cloud
- ☐ Local source

Choose how to manage updates

Manage updates from the cloud: If you have the network capacity, we recommend limiting your administrative overhead and managing updates automatically. Updates will be installed directly on client devices from Windows Update for Business and the Office CDN.

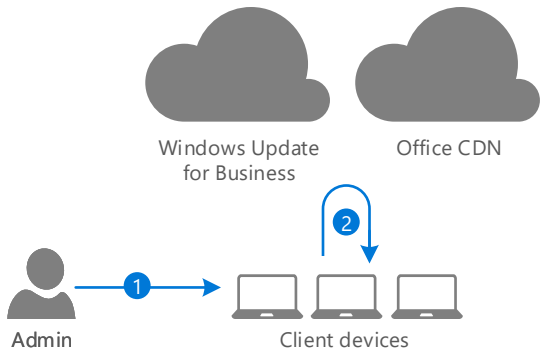
Manage updates with Configuration Manager: You can update Windows and Office with Configuration Manager by using the same software update management workflow you use for other software updates.

Define your deployment rings

Define the deployment rings for your client devices. Deployment rings determine when client devices receive feature updates for Windows 10 and Office. Deployment rings can be defined for updates for Office and Windows together, or separately.

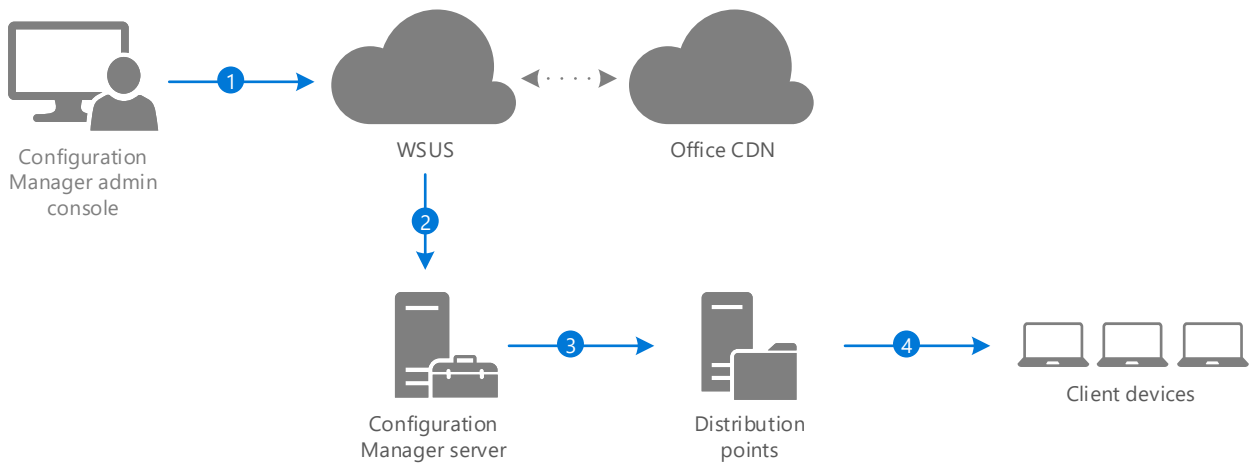
Best practice: As a baseline, we recommend defining a "Targeted" ring with a small group of devices and a "Broad" ring with the rest of your devices. Devices in the Targeted ring can receive updates earlier and validate those updates in your environment. After validation, you can deploy the updates to the devices in the Broad ring.

Manage updates for Windows 10 and Office 365 ProPlus from the cloud



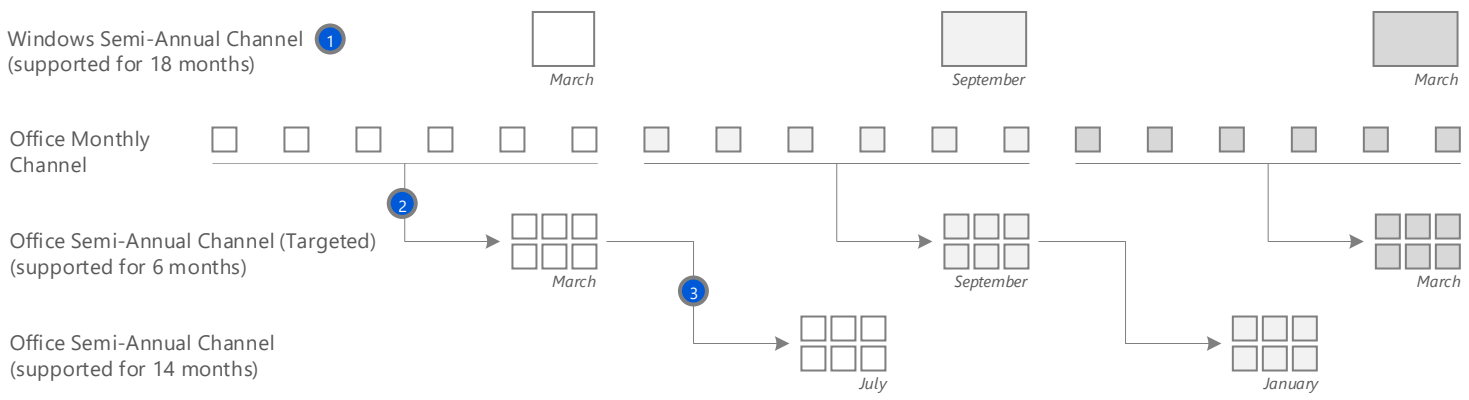
1. As part of deployment, admin configures client devices to receive updates directly from the cloud
2. Client devices automatically download and apply updates from Windows Update for Business and Office CDN

Manage updates for Windows 10 and Office 365 ProPlus with System Center Configuration Manager



1. Admin configures Windows and Office updates in Configuration Manager.
2. Windows updates are downloaded from WSUS. Although the Configuration Manager server communicates with WSUS, the Office updates are pulled directly from the Office CDN.
3. Updates are sent to Configuration Manager distribution points.
4. Updates are installed on client devices.

Schedule for feature updates for Windows and Office



1. Feature updates are released to the Windows Semi-Annual Channel every six months, around March and September.
2. Feature updates are also released in March and September to the Office Semi-Annual Channel (Targeted). The updates include feature updates from the Monthly Channel.
3. Four months after the Office update is released to the Semi-Annual Channel (Targeted), it's released to the standard Semi-Annual Channel.

September 2017

Microsoft

Deploy a modern and secure desktop with Microsoft

Architect end-to-end solutions for deployment, protection, and change management of the modern desktop with Windows 10 and Office 365 ProPlus.

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

For more architecture resources like this, see aka.ms/cloudarch.

Protection for Windows 10 devices

Windows 10 capabilities are recommended in two tiers: out-of-box protection and increased protection. 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.

Tiers of protection

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.

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 the 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.

For more details on protection, see: Identity and Device Protection for Office 365
File Protection Solutions in Office 365

September 2017

Microsoft