

# VMware Workspace ONE UEM

Guide for Microsoft Endpoint Manager Administrators

## Table of contents

|  |    |
|--|----|
| <b>Introduction</b> .....  | 3  |
| <b>Workspace ONE UEM for Windows 10 Management</b> .....                                     | 4  |
| <b>Windows 10 Device Onboarding and Enrollment</b> .....                                     | 5  |
| Zero IT Touch Onboarding with Out-of-Box PC Setup .....                                      | 6  |
| Other Windows 10 Enrollment Methods .....  | 7  |
| Workspace ONE Intelligent Hub for Windows Enrollment .....                                   | 7  |
| Azure AD Integration Enrollment .....  | 8  |
| Device Staging .....   | 8  |
| Native MDM Enrollment.....   | 9  |
| <b>Use Case: Windows 10 Onboarding Experience with Workspace ONE and Windows Autopilot</b> . | 11 |
| Configuring Workspace ONE for Windows 10 Management .....                                    | 12 |
| Securing and Updating Windows 10 .....   | 12 |
| Managing and Delivering Windows 10 Apps .....  | 14 |
| Windows Application Delivery.....  | 14 |
| Application Management.....  | 15 |
| <b>Use Case: Native Supported App Deployment with VMware Workspace ONE</b> .....             | 18 |
| Windows 10 Real-Time and Automated Security Protection and Compliance.....                   | 18 |
| Identity and Conditional Access.....   | 18 |
| OS Health and Threat Protection.....   | 19 |
| Data Loss Prevention.....  | 20 |
| Security Risk Dashboard .....  | 20 |
| <b>Getting Started</b> .....   | 21 |

## Introduction

Windows 10 introduces major changes—built-in mobile management APIs, more frequent cloud updates, modern apps, and more. Much like how IT has managed mobile devices, these changes are now driving modern management of the operating system (OS) from the cloud. It is anticipated that 50 percent of all employees will be working outside the corporate network over the next few years, so IT administrators need to manage, secure, and deliver modern applications and achieve deep, granular control over global workforce devices. The struggle to manage Windows 10 devices with hybrid and co-management scenarios can make the path to modern management seem complex and unclear. Microsoft has introduced Microsoft Endpoint Manager formerly known as SCCM for modern endpoint management (MEM), but it still has a long way to go to become a unified endpoint management (UEM) solution.

Yet, waiting for this unified management experience can be restrictive and expensive. With VMware Workspace ONE, there's no need to wait. VMware Workspace ONE is a cloud-based endpoint management solution that manages a broad range of endpoints, including Windows 10 devices. This unified solution provides intelligent automation to simplify IT, secure business, and empower users to work anywhere. VMware Workspace ONE provides a digital workspace platform with the following comprehensive modern management capabilities to best meet your requirements:

- **Native modern management with Workspace ONE for Windows 10:** Take advantage of Workspace ONE modern management as a native solution for Windows 10 and other devices. It delivers an end-to-end modern management lifecycle—onboarding, configuration, patching, security, distribution, automation, and support.
- **Coexistence and migration from SCCM with Workspace ONE AirLift:** Workspace ONE AirLift bridges administrative frameworks between Microsoft System Center Configuration Manager (SCCM) and Workspace ONE UEM. Workspace ONE AirLift offers an automated and progressive approach that simplifies your migration to native modern management with Workspace ONE.

This guide is for Microsoft Endpoint Manager (formerly SCCM) administrators and IT pros who are excited about the prospects of modern management. Throughout the guide, we explore unique scenarios in which Workspace One UEM helps with Windows 10 management. This guide breaks down technical challenges and demonstrates how Workspace ONE can help you achieve modern management. We also review how to manage the full lifecycle of every endpoint (including desktop, mobile, rugged, and IoT) and ensure enterprise security at each layer—all with the help of VMware Workspace ONE for Windows 10 management.

## Workspace ONE UEM for Windows 10 Management

VMware Workspace ONE is an intelligence-driven digital workspace platform with integrated access control, application management, and multi-platform endpoint management. This single platform is available as a cloud service or on-premises deployment. Workspace ONE for Windows 10 provides a robust set of mobility management solutions for enrolling, securing, configuring, and managing Windows 10 device deployments. It is the only UEM to uniquely combine modern OS mobile device management (MDM) efficiencies with traditional PC management requirements to enable policy configuration, automated patching, zero capital expenditure (CapEx) software distribution, and real-time security from silicon to software.

If you are considering a gradual transition to modern management, Workspace ONE also features optimal modern endpoint management coexistence and automation to speed your journey. VMware continues to work with Microsoft to help customers modernize Windows 10 by using their existing investments in Modern Endpoint Management, Workspace ONE, and cloud intelligence. This allows administrators and IT pros to focus their time on more impactful priorities.

VMware Workspace ONE enables cloud-based, modern management across five main areas (Figure 1):

- **Device onboarding:** Replace traditional OS deployment and imaging tools that are high touch for IT, and use modern onboarding workflows with UEM integration with Windows 10 Out-of-Box Experience (OOBE) and Windows Autopilot.
- **Configuration management:** Apply firmware/BIOS settings and MDM-based configuration service providers (CSPs), and deploy industry-recommended GPO settings and configurations with template-based policies using Workspace ONE UEM baselines. Curate GPO baselines based on industry standards, including the Windows 10 security baseline from Microsoft and CIS Benchmarks.
- **OS patch management:** Take advantage of the Windows-as-a-service framework to create and update distribution rings for Windows patches, set deferment periods, and define which updates should be automatically approved by the administrator. Distribution rings can be configured based on the requirements of your organization. Integrate Common Vulnerability and Exposure (CVE) feeds to automate patch deployment and protect against vulnerabilities in real time.
- **Software distribution:** Deliver applications from different sources to users via the Workspace ONE catalog. Administrators can deliver executable file format (EXE), Microsoft Installer files

(MSIs), and scripted install (ZIP) applications from the Workspace ONE UEM console; for public apps, there is direct integration with the Microsoft Store for Business. Use native peer-to-peer (P2P) technology to improve delivery speed and reduce software distribution infrastructure and bandwidth costs.

- **Client health and security:** Enable IT to enforce BitLocker encryption and set security policies on endpoints. Administrators can also set policies related to Windows Information Protection (WIP), Windows Hello, Windows Defender Exploit Guard, device health attestation, device security baselines, full Conditional Access, antivirus software, firewall rules, and other OS security features.



FIGURE 1. FIVE AREAS WHERE VMWARE WORKSPACE ONE ENABLES MODERN MANAGEMENT

## Windows 10 Device Onboarding and Enrollment

VMware Workspace ONE includes smarter ways to deploy, control, and manage Windows 10. The primary use cases for a Windows 10 deployment are as follows: employee-owned machines, remote worker devices, and corporate office devices. For all scenarios, the process begins with

device enrollment, which establishes initial communication between Workspace ONE UEM and modern device management capabilities in Windows 10. For a hybrid modern management solution, Workspace ONE provides a variety of ways to enroll and onboard Windows 10 devices.

Before enrolling devices, be sure that you have the required enrollment information. See [Windows Desktop Enrollment Requirements](#) for more details.

### Zero IT Touch Onboarding with Out-of-Box PC Setup

Windows 10 offers a simplified PC onboarding experience, providing an OOB that walks a user through the first-time setup process. This capability is enabled by Windows Autopilot, which is fully supported by Workspace ONE for Windows 10. With the advanced PC onboarding capabilities of Windows Autopilot, IT teams can register a device with an original equipment manufacturer (OEM)—including Dell Provisioning for VMware Workspace ONE to provide Zero IT Touch Onboarding features, such as customized opening OOB screens, pre-loaded applications in the factory, and the ability to enroll the device into VMware Workspace ONE. Dell Provisioning for VMware Workspace ONE delivers better end-user productivity and simplified IT administration, including the following features:

- Pre-configured devices with automated setup of applications and settings ship directly to customers or end users to eliminate the manual PC configuration and enable user productivity in minutes.
- Zero Touch Restore functionality minimizes downtime by allowing applications and management to persist if a device is required to recover or reset.
- Zero IT Touch gives better control over remote devices, locking down them to single or specific sets of apps for dedicated device uses, like kiosks or rugged devices.
- Aside from pre-configured applications, Dell Provisioning also provides self-service application catalogs that display personalized applications to users and administrators.

When a user receives a new Windows 10 device, Workspace ONE OOB enrollment automatically enrolls the device with Windows Autopilot and Workspace ONE UEM (Figure 2). From there, the Windows 10 Provisioning Service enables the automatic provisioning of the Workspace ONE application to the device.

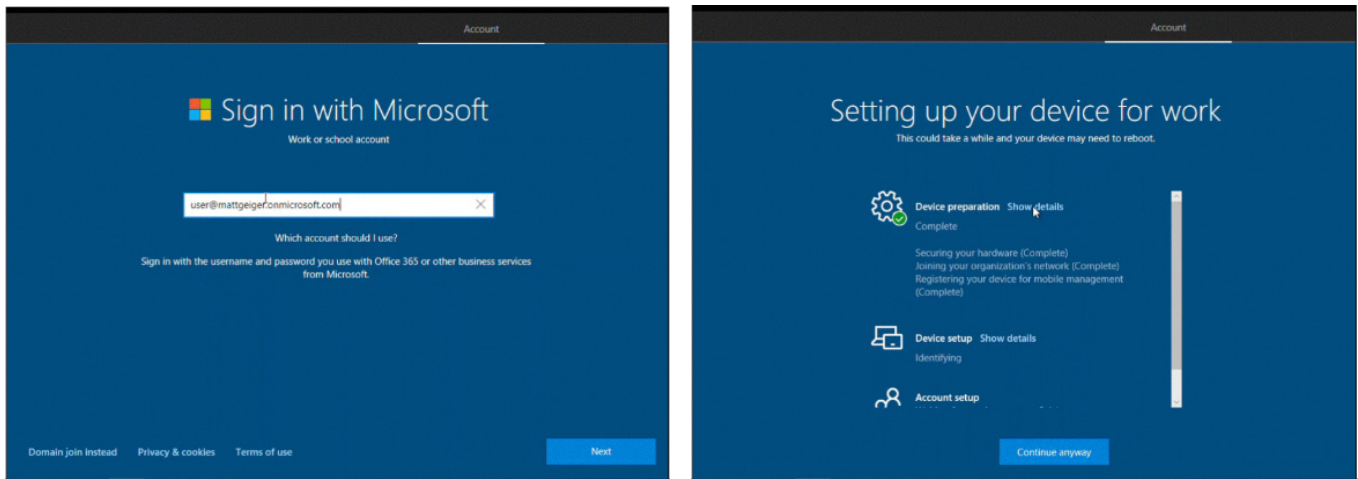


FIGURE 2. OOB Screens for Enrolling a New Windows 10 Device

[Learn more](#) about enrolling Windows 10 devices through OOB.

### Other Windows 10 Enrollment Methods

In addition to OOB, Workspace ONE supports other enrollment methods, including the use of Workspace ONE Intelligent Hub for Windows, Microsoft Azure Active Directory (Azure AD) integration, device staging, and native MDM functionality of the Windows OS.

Workspace ONE supports many different types of onboarding methods. These can be user-driven scenarios with Azure OOB and Windows Autopilot or with the self-enrollment capabilities of Workspace ONE Intelligent Hub for Windows. Onboarding methods also include administrative scenarios, including command-line enrollment, Azure enrollment, and Dell Provisioning.

### Workspace ONE Intelligent Hub for Windows Enrollment

Workspace ONE Intelligent Hub initiates the enrollment of Windows 10 devices using full MDM functionality (Figure 3). As such, it offers the simplest enrollment flow for users. Once Workspace ONE is configured, you simply download Workspace ONE Intelligent Hub from [getws1.com](http://getws1.com). When enrollment is completed, the Workspace ONE app automatically launches and configures based on your Workspace ONE UEM deployment. Workspace ONE Intelligent Hub can also be used seamlessly with the release of Workspace ONE for Microsoft Endpoint Manager to access resources across your organization.

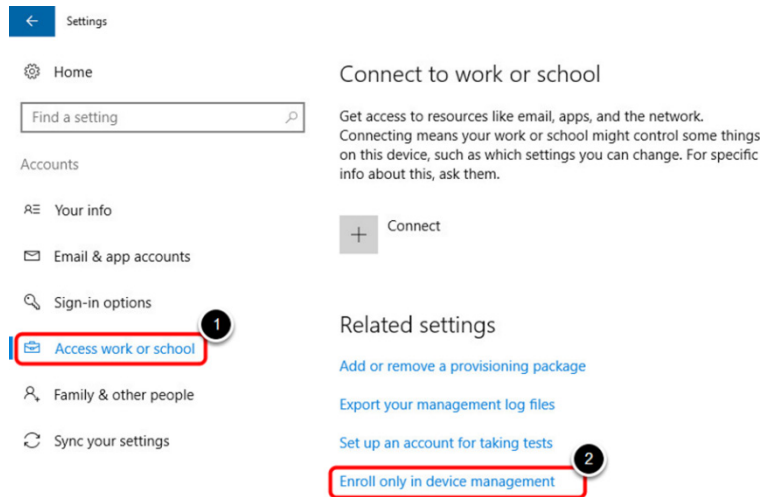


FIGURE 3. USING WORKSPACE ONE INTELLIGENT HUB TO ENROLL A WINDOWS 10 DESKTOP DEVICE

[Learn more](#) about enrolling Windows Desktop devices with VMware Workspace ONE Intelligent Hub.

### Azure AD Integration Enrollment

Windows 10 devices can be enrolled into Workspace ONE using integration with Azure AD, requiring minimal end-user effort. Before devices can be enrolled using Azure AD integration, administrators must configure both Workspace ONE UEM and Azure AD. This configuration requires information to be entered into the Azure AD and Workspace ONE UEM deployments to facilitate communication. Azure AD integration enrollment supports three different flows: joining Azure AD, OOB enrollment, and Office 365 enrollment.

[Learn more](#) about Windows 10 enrollment through Azure AD integration.

### Device Staging

If you want to configure device management on a Windows 10 device before shipping it to an end user, consider using Windows Desktop device staging (Figure 4). This workflow allows you to enroll a device through Workspace ONE Intelligent Hub and install device-level profiles before shipment. The two methods of device staging are manual installation and command-line installation. With manual installation, devices are required to be domain-joined. Command-line installation works for all Windows 10 64-bit and 32-bit operating systems from all OEMs.

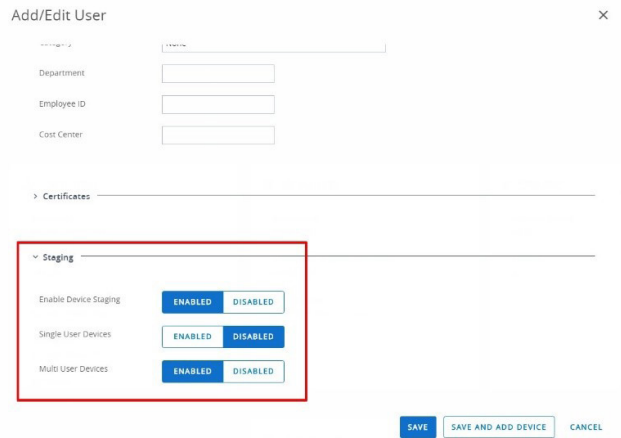


FIGURE 4. USING DEVICE STAGING TO ENROLL A WINDOWS DEVICE

[Learn more](#) about device staging enrollment.

### Native MDM Enrollment

Workspace ONE UEM supports enrolling Windows Desktop devices using the Windows 10 native MDM enrollment workflow (Figure 5). This means both corporate-owned and bring-your-own devices can be enrolled through the same flow. Windows Auto-Discovery for Windows 10 devices enables this quick and easy enrollment flow for end users.

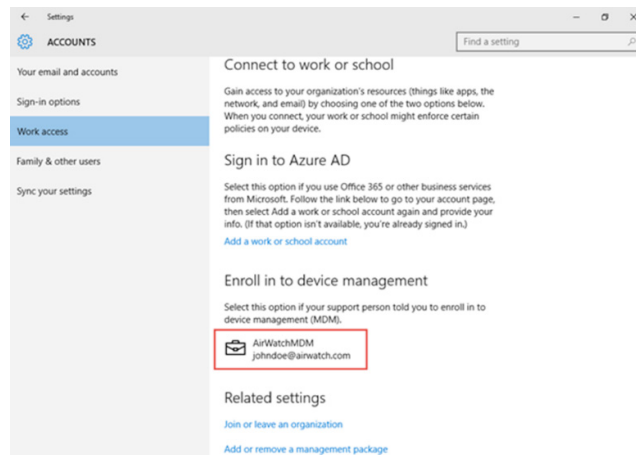


FIGURE 5. NATIVE MDM WORKFLOW FOR ENROLLING A WINDOWS 10 DEVICE

[Learn more](#) about native MDM enrollment for Windows Desktop devices.

### **SCCM Device Enrollment with Workspace ONE for Coexistence**

Workspace ONE AirLift enrollment allows SCCM and Workspace ONE UEM to coexist on devices. To enroll Windows 10 devices into Workspace ONE UEM using Workspace ONE AirLift, simply configure the enrollment application that switches between Workspace ONE AirLift, Workspace ONE UEM, and SCCM. The app connects with SCCM collections and maps them into Workspace ONE UEM, simplifying device enrollment and moving the device to a coexisting state.

Coexistence is a short-term bridge to full modern management. We recommend transitioning to modern management as quickly as possible to streamline administrator operations and improve the end-user experience. This enables faster boot and login times by design.



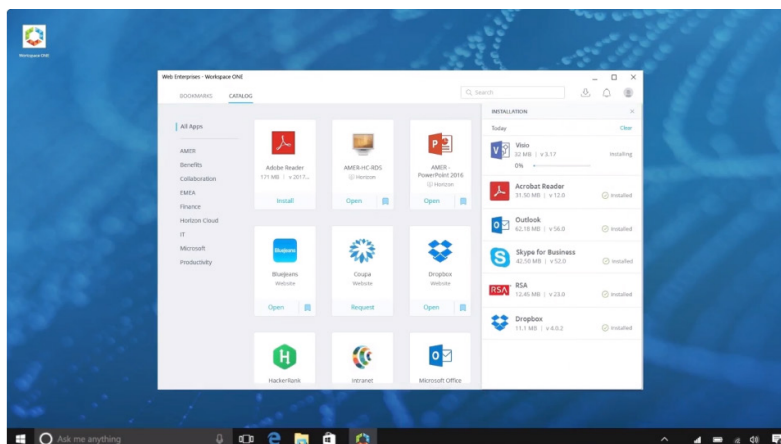
## Use Case: Windows 10 Onboarding Experience with Workspace ONE and Windows Autopilot

As an IT administrator, you undoubtedly know that Windows device lifecycle management can be a time-consuming and complex process, involving the need to image, reimagine, or manually set up devices before releasing them to users. Traditionally, organizations either dedicate internal resources or pay third-party companies to handle this process, which can result in long delays for users who are waiting to receive a first-time or replacement device.

By working closely with Microsoft engineering teams and strategic customers, VMware Workspace ONE with Dell Provisioning seamlessly integrates with Windows Autopilot to provide Zero IT Touch capabilities for simplified device enrollment. You can easily set up and preconfigure new devices and reset, repurpose, or recover devices. The following management capabilities are enabled by Workspace ONE with Windows Autopilot:

- Automatically join and enroll devices: Workspace ONE with Windows Autopilot enables users to automatically join devices to Azure AD and then auto-enroll them into Workspace ONE.
- Gain visibility into device configuration status: Unique to VMware, when a user's first launch experience is powered by Workspace ONE, they can see the status of their device as it's being configured, including the apps IT has made available to them.
- Provide robust, dynamic configuration: Workspace ONE dynamically configures all corporate policies, removes bloatware, installs all provisioned Win32 applications, and applies security settings over the air in minutes based on the user's role in the organization (Figure 6).

FIGURE 6. DASHBOARD SHOWING DYNAMIC CONFIGURATION WITH WORKSPACE ONE



- Enable single sign-on access: Once a user logs in, they can access the Workspace ONE application catalog for single sign-on (SSO) access to any Win32, software as a service (SaaS), Universal Windows Platform (UWP), or remote/virtual applications.
- Deliver a truly self-service experience: Workspace ONE allows users to download additional applications or get pre-installed apps on OEM devices or partner-shipped Windows 10 devices with an OOBE. Additional self-service capabilities reduce help desk requests for things like resetting passwords or finding BitLocker recovery.

### Configuring Workspace ONE for Windows 10 Management

Profiles in Workspace ONE provide the primary mechanism for managing devices. A profile consists of settings, configurations, and restrictions. When combined with compliance policies, the profile enforces corporate rules and procedures. Windows Desktop profiles apply to a device at either the user level or the device level. When creating Windows Desktop profiles, you select the level the profile applies to. Workspace ONE UEM executes commands that apply to the device context even if the device has no active enrolled user login. Below are some Windows Desktop profiles types that can be configured for Windows 10:

|                              |                               |
|------------------------------|-------------------------------|
| Passcode profile             | Windows updates profile       |
| Wi-Fi profile                | Web Clips profile             |
| VPN profile                  | Exchange ActiveSync profile   |
| Credentials profile          | SCEP profile                  |
| Restrictions payload profile | Application control profile   |
| Data Protection profile      | Exchange Web Services profile |
| Windows Hello profile        | Windows licensing profile     |
| Firewall profile             | BIOS profile                  |
| Single App Mode profile      | OEM updates profile           |
| Antivirus profile            | Kiosk profile                 |
| Encryption profile           | Custom settings               |

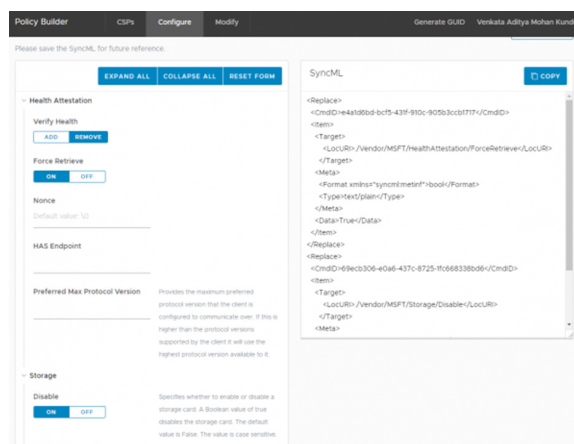
[Learn more](#) about Windows Desktop profiles.

## Windows 10 Policy Management

With Workspace ONE, you can easily enable dozens of contextual policy combinations that use Workspace ONE device enrollment, network and SSO policies, automated device remediation, and third-party information. Workspace ONE is the only modern management solution that provides full compatibility for managing Windows 10 group policy object configurations from the cloud and without domain dependency. The following are the capabilities of Windows 10 policy management in Workspace ONE:

- **Defining policies with profiles:** The Workspace ONE UEM console allows administrators to configure policies through profiles. These policies are used often across industries and provide easy configuration through the graphical user interface. The administrator can simply toggle switches or use the text fields to set up these policies. The Workspace ONE UEM console also provides a custom settings profile that is extensible to any custom XML and can be sent to the device using the existing infrastructure to securely communicate with the device.
- **Real-time configuration service provider policies for Windows 10 management:** Workspace ONE provides support for CSPs, which are interfaces used to read or set policies on the Windows 10 device. Modern management uses CSPs to push registry and file system settings to devices over the air. The XML used to configure a CSP that the Open Mobile Alliance Device Management (OMA DM) client in the OS can use to apply the appropriate settings is called SyncML. *VMware Policy Builder* is a tool that helps administrators generate SyncML in minutes using an experience similar to Windows Desktop profiles. Policy Builder allows administrators to use all the latest platform updates without the hassle of writing error-free XML (Figure 7). [Learn more](#) about Policy Builder.

FIGURE 7. WINDOWS 10 POLICY BUILDER



- **Baselines to secure Windows 10 Devices:** Workspace ONE curates the best practices of your particular enterprise into configurations called baselines. With Workspace ONE's Baselines capability, you can keep all your devices secure with industry-recommended settings and configurations. To ensure that Baselines use only the best settings and configurations, VMware is certified by CIS to provide industry favorites like CIS benchmarks for Windows 10 to provide easy and secure solutions. Baselines are based on the Windows OS version and can be updated whenever you want. During configuration, you can choose which baseline to use or upload a custom baseline to suit your needs. These configurations significantly reduce the time it takes to set up and configure Windows devices. [Learn more](#) about Workspace ONE UEM Baselines.

### Securing and Updating Windows 10

The Workspace ONE UEM update service for Windows 10 provides functionality tailored to address the unique constraints of mobility and the cloud. Traditional OS upgrades use a wipe-and-replace model, but the update-as-a-service model pushes periodic OS and feature updates. Windows 10 updates occur on a frequent and dynamic basis to ensure that end users always have access to the most recent security and productivity features.

- **Windows 10 patch management options:** Deploying Windows 10 fixes, patches, and updates on client servicing plans creates overhead. Using branches enables you to create a customized deployment schedule based on preference and update sensitivity. There are a variety of Windows 10 patch management options (Figure 8):
  - **Semi-Annual Channel:** New features and functionality are introduced twice per year around March and September rather than every three to five years. Changes are presented in bite-sized chunks rather than all at once.
  - **Insider – Fast:** Major builds are introduced, including new and existing feature changes, limited servicing, and/or cumulative updates.
  - **Insider – Slow:** Major builds are introduced, including new and existing feature changes, all servicing, and/or cumulative updates.
  - **Insider – Release:** Major builds are introduced, including the latest feature changes, updates, bugs fixes, and application changes.

The screenshot displays the Windows 10 Patch Management Options screen with the following settings:

- Windows Update Source:** MICROSOFT UPDATE SERVICE (selected) and WSUS.
- Update Branch:** A dropdown menu is open, showing options: Semi-Annual Channel (checked), Insider - Fast (Less Stable, Dev Build), Insider - Slow (More Stable, Dev Build), and Insider - Release (Most Stable, Public Build).
- Insider Builds:** (This label is present but has no visible input field).
- Defer Feature Updates Period in Days:** 0.
- Pause Feature Updates:** ENABLE (selected) and DISABLE.
- Defer Quality Updates Period in Days:** 0.
- Pause Quality Updates:** ENABLE (selected) and DISABLE.
- Enable Settings for Previous Windows Versions:** (checkbox is unchecked).

FIGURE 8. WINDOWS 10 PATCH MANAGEMENT OPTIONS SCREEN

[Learn more](#) about managing updates for Windows 10.

- **Intuitive OS Updates dashboard:** The OS Updates dashboard displays version data for operating system by platform. OS Updates data informs you if your environment is fragmented and running older operating systems on devices. Within dashboards, the configurable widgets allow you to customize the data that is displayed. In the Windows Desktop module, the Patches tab lists data about patch update statuses for Windows, including certain Microsoft applications discovered from the Microsoft Updates channel. Integrating CVE and Common Vulnerability Scoring System (CVSS) into a unified view allows IT teams to proactively manage security vulnerabilities with automated patch remediation based on a CVE risk profile. The dashboard provides visibility into the impact of vulnerabilities reported through CVEs and correlated to the existing patches on each of your managed Windows 10 devices. You can use filters to find data on patches using a specific knowledge base (KB) number, patch KB title, patch update classification, or date range.

[Learn more](#) about the [OS Updates dashboard](#) and [CVE integration](#).

## Managing and Delivering Windows 10 Apps

For many customers, the primary problems associated with PC management arise from app delivery, integration, and support. These problems become more complex as organizations adopt more apps and the number of variables and configuration possibilities grows exponentially. To help solve such application integration and management woes, Microsoft has introduced a variety of features and tools in Windows 10. Unified applications are designed to service administrators, developers, and, most importantly, users in ways that are difficult to achieve today.

With the seamless implementation of these capabilities, VMware Workspace ONE UEM delivers unified application delivery and management. The following sections dive into the details.

### Windows Application Delivery

Applications delivered in today's dynamic and fluid world need to be available at any time, on any device, and across any network. As a result, most users require access to local apps, hosted apps, SaaS apps, classic apps, and cloud apps.

- **Software Distribution**

You can deploy Win32 applications from the Apps & Books section of the Workspace ONE UEM Console and, in doing so, use the application lifecycle flow that exists for all internal applications. This feature is called software distribution. Use software distribution to deliver Win32 applications, track installation statuses, keep application versions current, and delete old applications.

[Learn more](#) about software distribution.

- **Business Store Portal Integration**

Microsoft UWP applications consist of a single code base that can run on virtually any Windows device. Integrate Workspace ONE UEM with the online or offline Microsoft Store for Business portal to deploy UWP applications.

[Learn more](#) about business store portal integration.

- **Product Provisioning**

Product provisioning delivers custom or complex files to managed devices. When a file cannot be directly installed on devices, you can package it in the Workspace ONE UEM Console to create a product, then provision the product to managed devices based on configured conditions and smart group assignment in the console.

[Learn more](#) about product provisioning.

### Migrate SCCM Apps to Workspace ONE AirLift

Workspace ONE AirLift exports Microsoft SCCM applications, allowing you to migrate applications to Workspace ONE UEM without repackaging them. Migrated applications can be deployed on Windows 10 devices that have been moved or added to Workspace ONE for modern management.

### Monitor Progress of Devices and Applications with a Co-Existence Dashboard

The management dashboard provides a visualization of the transition and indicates the progress for devices and applications. The dashboard also displays migration workloads to show how Workspace ONE AirLift functionality uses coexisting devices. This includes encryption, Windows updates, and compliance and software distribution, along with an enrollment history and fleet complete percentage within SCCM collections.

## Application Management

As end-user demand drives organizations to adopt more applications, PC management issues only grow in complexity and number. Workspace ONE allows users to:

- **Apply granular whitelists and blacklists:** Workspace ONE enables Application Control to whitelist and blacklist specific applications to allow or prevent use of applications on devices. Application Control uses Microsoft AppLocker configurations to enforce app control on Windows 10 devices. You can enable Executable Rules, Windows Installer Rules, and Script Rules enforcement by selecting Enforce Rules. [Learn more](#) about how to configure an Application Control profile.
- **Use role-based controls:** You can make roles that grant specific kinds of access to the Workspace ONE UEM console and define roles for individual users and groups based on UEM console access levels you find useful. Each Workspace ONE UEM includes default roles for both users and administrators that you can use as a template to create your own customized roles that better suit the needs of your organization. [Learn more](#) about role-based access control.
- **Enable SSO:** SSO allows end users to access Workspace ONE UEM apps and wrapped apps without entering credentials for each application. Using the Workspace ONE Intelligent Hub or the AirWatch Container as a “broker application,” end users authenticate once per session using their normal credentials or an SSO Passcode. [Learn more](#) about application-level SSO Passcodes.



## Use Case: Native App Deployment with VMware Workspace ONE

As an organization expands and evolves, application delivery overheads increase on IT teams. You need to ensure that application delivery is available anytime, while simultaneously ensuring that you are ready to deliver different types of applications, including local apps, hosted apps, SaaS apps, classic apps, or cloud apps. Application deployment on Windows 10 devices can be further granularized with advanced Windows Desktop profile-based policy management. Workspace ONE allows almost any type of app to be delivered to Windows 10 devices, including:

- **Universal applications:** Universal apps are written with a single set of code base that can run on virtually any Windows device. Universal applications can be provisioned right to the device and can also be made available through the Windows Store.
- **Classic Windows applications:** Classic Windows applications (Win32 and Win64) constitute the majority of the application portfolio that can easily migrate to Windows 10. Classic Windows applications are installed using EXE, MSIs, batch files, and scripts.
- **Cloud-based applications:** Cloud-based applications, such as those from SaaS providers (like Salesforce.com), can easily integrate into the Windows 10 application catalog.
- **Hosted or remote applications:** Windows 10 can also remotely connect to published Remote Desktop Server Hosted (RDSH) applications residing on Horizon, XenApp, or Terminal Services servers. Many clients will continue to use older releases of Windows while they test Windows 10 on devices by configuring Windows 10 devices to access virtual desktop infrastructure-based desktops running legacy Windows (XP, 7, and 8) images.

### Windows 10 Real-Time and Automated Security Protection and Compliance

Workspace ONE extends Windows 10 security to users, devices, apps, and data. It adds protection in three key areas: identity and Conditional Access, OS health and threat protection, and data loss prevention.

#### Identity and Conditional Access

- **Identity and Conditional Access:** Workspace ONE offers many Conditional Access options. Use VMware Identity Manager as your identity provider or use a third-party identity provider (such as Active Directory Federation Services, Azure AD Identity Services, Okta, OneLogin, or PingFederate) to offer the level of authentication that is best for the device, user, and app. Use more than one method for extra control. For example, you can set access policies at the

app level, set compliance policies at the device level, and use VMware Tunnel to secure the connection between the app and the device. With the release of Workspace ONE for Microsoft Endpoint Manager, VMware is more focused on extending Conditional Access controls for Microsoft 365 apps and services through both Workspace ONE and integration with Microsoft Endpoint Manager and Azure AD Premium across BYO use cases, which will be available in preview in the fourth quarter of fiscal year 2020. [Learn more](#) about Conditional Access.

- **Compliance policies:** The compliance engine is an automated tool by Workspace ONE that ensures all devices abide by your policies, which can include basic security settings like passcodes and minimum device lock periods. If devices are determined to be out of compliance, the compliance engine triggers a message to warn users to address compliance errors to prevent disciplinary action on the device. Additionally, you can automate escalations when corrections are not made, such as locking down the device and notifying the user to contact you to unlock it. [Learn more](#) about compliance policies.
- **Secure alternative for password-based authentication:** Windows Hello provides a secure alternative to using passwords for security. Workspace ONE with Windows Hello profile configures Windows Hello for Business for your Windows Desktop devices so end users can securely authenticate to access applications, websites, and networks on behalf of the user without sending a password. Windows Hello requires users to verify possession of a Windows 10 device before it authenticates with either a PIN or Windows Hello biometric verification. [Learn more](#) about the Windows Hello profile.

## OS Health and Threat Protection

- **Managing the encryption lifecycle for Windows 10:** Powered by VMware technology, VMware Workspace ONE simplifies the traditionally complex process of enterprise device encryption. Workspace ONE UEM automates the entire encryption process, from enabling BitLocker to enforcing encryption on devices. Configure a BitLocker profile in the Workspace ONE UEM console to enable BitLocker on devices. Then, enforce encryption by configuring a compliance policy that includes encryption status as part of the device's general security posture. [Learn more](#) about BitLocker encryption lifecycle management.
- **Device health attestation:** Keep your devices secured with the Windows Health Attestation service for compromised device detection. This service allows Workspace ONE UEM to check device integrity during start up and take corrective actions. If any of the enabled checks fail, the Workspace ONE UEM compliance policy engine applies security measures

based on the configured compliance policy. This functionality allows you to keep your enterprise data secure from compromised devices. [Learn more](#) about compromised device detection with Windows Health Attestation.

- **Sensors for Windows Desktop Devices:** Windows 10 devices contain multiple attributes such as hardware, the OS, certificates, patches, apps, and more. Sensors in Workspace ONE UEM allow you to track additional device attributes, including driver details for a mouse driver, the warranty information for the OS, the registry value for your internal apps, and more. Taking the tracking functionality to the next logical step, Workspace ONE UEM integrates sensors with smart groups so you can provision apps, profiles, baselines, and more to your devices based on specific attributes. [Learn more](#) about creating sensors for Windows Desktop devices.

## Data Loss Prevention

- **Data loss prevention:** With Data Protection profiles, Workspace ONE allows you to configure rules to control how enterprise applications access data from multiple sources in your organization. Using Data Protection profiles ensures that your data is only accessible by secured, approved applications. Workspace ONE UEM uses the Microsoft WIP feature to protect your Windows 10 devices. Data Protection works by whitelisting enterprise applications to give them permission to access enterprise data from protected networks. If end users move data to non-enterprise applications, you can act based on the selected enforcement policies. [Learn more](#) about Data Protection profiles.
- **Workspace ONE with VMware Tunnel:** Using Workspace ONE with VMware Tunnel, control how end users access internal sites by configuring communication between the application and the VMware Tunnel. The VMware Tunnel serves as a relay between your mobile devices and enterprise systems by authenticating and encrypting traffic from individual applications to back-end systems. With the VMware Tunnel, organizations can prevent Windows 10 applications from gaining unauthorized access to internal or public endpoints. With client-side micro-segmentation capabilities, you can define granular access controls, such as which IP addresses, ports, and IP protocols Windows 10 applications can access. [Learn more](#) about VMware Tunnel.

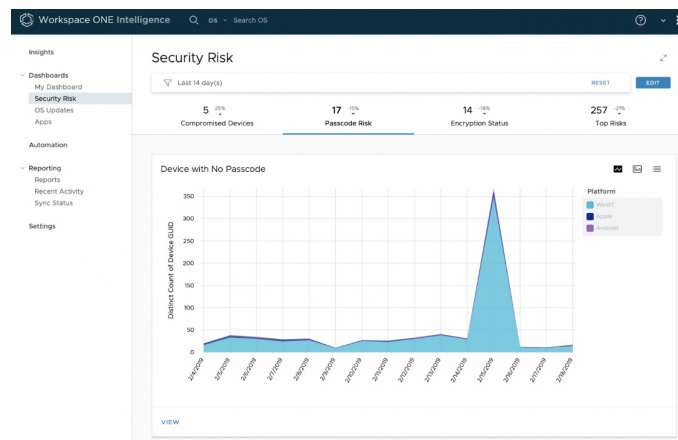
## Security Risk Dashboard

The Security Risk dashboard displays data concerning the security of managed devices in your Workspace ONE deployment (Figure 9). See data concerning compromised devices, passcode

risks, encryption status, and top risks. Risks represented in the Security Risk dashboard are grouped as Threats, Policy Risks, and Vulnerabilities.

- The Threats tab displays events identified by your Workspace ONE UEM compliance engine as compromised. It also displays and aggregates events reported by your Trust Network services in the Threats Summary module.
- The Policy Risks tab displays events that do not comply with configured policies as identified by your Workspace ONE UEM compliance engine. Events include devices with no passcode and devices that are not encrypted.
- The Vulnerabilities tab combines and displays information from third-party security reporting services and Workspace ONE UEM, which manages your Windows 10 devices.

Figure 9. Workspace ONE Security Risk Dashboard



[Learn more](#) about the Security Risk dashboard.

## Getting Started

- [Learn more](#) about Workspace ONE
- [Try Workspace ONE](#) for yourself
- [Check out the Hands-on Labs](#) for Windows 10 and Workspace ONE AirLift

