PLANNING YOUR WINDOWS 10 DEPLOYMENT: VMWARE WORKSPACE ONE
OPERATIONAL TUTORIAL
VMware Workspace ONE
Table of Contents

Overview

– Introduction

– Audience

Meeting Windows 10 Security Priorities

– Introduction

– Establishing User Trust

– Assessing Device Posture

– Preventing Data Loss

Determining Your Use Cases

– Introduction

– Understanding Windows 10 Use Cases

Selecting an Onboarding Workflow

– Introduction

– Understanding Onboarding Options

– Selecting an Onboarding Workflow

Configuring Workspace ONE Profiles

– Introduction

– Understanding General Settings

– Reviewing Windows 10 Payloads

Delivering and Managing Software
– Introduction
– Determining a Software Delivery Method
– Managing Applications

Managing Windows 10 Updates
– Introduction
– Understanding Patch Management

Summary and Additional Resources
– Conclusion
– Terminology Used in This Tutorial
– Additional Resources
– Searching for More Information
– About the Authors
– Feedback
Planning Your Windows 10 Deployment: VMware Workspace ONE Operational Tutorial

Overview

Introduction

VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. This tutorial provides practical information to help you plan your VMware Workspace ONE® UEM (unified endpoint management) management solution to address the unique circumstances of your use cases.

Workspace ONE® UEM, powered by VMware AirWatch®, includes capabilities for Windows 10 that introduce smarter ways to deploy, control, and manage an organization’s PC fleet.

Traditional approaches use multiple administrative tools to manage the PC life cycle, including separate tools for staging and imaging, for maintaining drivers, for managing OS updates, for configuring firewall, antivirus, and encryption policies, and more. In contrast, Workspace ONE UEM unifies enterprise mobility management in a single administrative console.

The release of Windows 10 introduced fundamental changes to the Windows operating system to address the security and data concerns of today's digital workspace. To take advantage of Workspace ONE UEM capabilities, you can fold the Windows 10 functionality into an existing VMware management solution. Combining traditional client requirements with modern enterprise management capabilities creates a simplified, cost-effective management solution.

Audience

This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager™ and VMware Workspace ONE® UEM, is also helpful.

Meeting Windows 10 Security Priorities

Introduction

You can use Workspace ONE UEM to establish user trust, assess the device posture, and enable data loss prevention.

![User Trust, Device Posture, Data Loss Prevention](image.png)

*Figure: Security Priorities for the Modern Digital Workspace*
Establishing User Trust

Workspace ONE UEM uses new identity features to establish user trust. These features include two-factor authentication, which requires that an enrolled, managed, and compliant device meet two forms of authentication.

To fulfill the first half of two-factor authentication, the device must be onboarded, a process of enrolling devices into Workspace ONE UEM for management in the Workspace ONE UEM Console (the Console).

For the second authentication factor, users with Microsoft Azure AD can use Windows Hello capabilities like biometric access and PIN authentication. Workspace ONE UEM enforces the PIN strength requirements and can allow or disable the biometric feature for end users' devices.

Workspace ONE UEM also integrates with Windows Hello for biometric authentication while providing certificate authentication (or another authentication type) into the apps and corporate resources, thus providing a layered authentication model for added security.

Assessing Device Posture

Workspace ONE UEM assesses device posture by evaluating, locally enforcing, and remediating devices using the compliance engine, a Workspace ONE UEM tool that ensures that all devices abide by specified policies. A policy can include basic security settings or more critical security configurations.

The compliance engine detects non-compliant devices and sends end users a warning. If the end user addresses the issue after the warning, no further action is taken. If the end user fails to correct the issue in the specified time-frame, it escalates, and disciplinary actions occur.

Use the Workspace ONE UEM Console to specify the escalation steps, disciplinary actions, grace periods, and messages. For example, the following figure demonstrates a tiered approach to compliance. With each security action, an end user’s non-response escalates the risk level.

![Figure: Tiered Risk Escalations and Compliance Actions](image)

Preventing Data Loss

Modern Windows 10 management with Workspace ONE UEM maximizes native Windows Information Protection capabilities to help you minimize the risk of data loss. Use Windows Information Protection to define:

- Privileged applications
- Application access
- Enterprise boundaries
- Protection levels

Windows Information Protection encrypts all corporate data at the file level and decrypts only when accessed by a privileged application. An enterprise wipe removes all corporate data from the device.

Note: Windows Information Protection operates on a device level. If data is transferred to a file share or cloud repository, Windows Information Protection cannot guarantee data protection. Instead, shared data requires integration with a rights management service (RMS).
Privileged Applications

In addition to delivering managed applications to devices through enrollment, Windows 10 can also place device apps that were not pushed through Workspace ONE UEM Mobile Device Management into a managed state when you designate them as privileged applications.

The updated Windows 10 SDK enables application developers to handle personal and corporate data on privileged applications, creating enlightened apps. For all options, administrators can set a policy that prevents an application from sharing corporate data to a personal app, site, or repository.

Application Access

Per-App VPN prevents Windows 10 applications from gaining unauthorized access to internal or public endpoints. Its client-side micro-segmentation capabilities define which IP addresses, ports, and IP protocols Windows 10 applications can access.

You can also use privileged applications to simplify per-app VPN configurations. Depending on the needs of the organization, use one or both of the following options:

- Every privileged application can have a unique VPN configuration.
- All privileged applications can use the same VPN configuration.

Enterprise Boundaries

Enterprise boundaries on Windows 10 use specified IP ranges or domains to identify and encrypt work data downloaded to a device. The downloaded files are encrypted and can be opened only with a privileged application. For example, if the domain air-watch.com is specified as a protected network, data downloaded from sharepoint.air-watch.com can only be accessed by the privileged applications on that device.

Protection Levels

You can configure varying levels of protection for user groups to address organizational demands and device use cases. Protection levels include:

- **Block** - Corporate data can be accessed only from privileged applications.
- **Override** - If a user attempts to access corporate data with a non-privileged application, a warning prompt appears. A user can choose to complete the action, but the action is logged in an audit log.
- **Audit** - A user can access corporate data with a non-privileged application, but the action is logged in an audit log.
- **Off** - Windows Information Protection is disabled.

Determining Your Use Cases

Introduction

VMware Workspace ONE UEM modernizes Windows management and security across any use case. This section explores a variety of use cases and how you can use Workspace ONE UEM to manage them.

Understanding Windows 10 Use Cases

The primary use cases for a Windows 10 deployment are: employee-owned machines, remote-worker devices, and corporate office devices. Review the following table to gain a high-level understanding of each use case.
This tutorial addresses the required components and recommended configurations for the most common Windows 10 use cases. Since configuration requirements and recommendations vary by use case, when applicable, the following sections specify which use cases a particular configuration applies to.

### Selecting an Onboarding Workflow

**Introduction**

Workspace ONE UEM supports a variety of onboarding workflows that address multiple use cases. The onboarding method impacts other configuration decisions, and therefore is an important starting point when planning a Workspace ONE UEM deployment. In this section, learn about the available onboarding options for Windows 10, and evaluate which option is best for your organization.

**Understanding Onboarding Options**

The following table lists recommended and supported onboarding workflows by use case - as well as some requirements. Keep in mind, many of these requirements are driven by the operating system.

For a decision tree to help you identify the enrollment flows that best suit your organization, see Selecting an Onboarding Workflow.

#### Common Windows 10 Device Use Cases

<table>
<thead>
<tr>
<th>Type of Device</th>
<th>Use Case Name</th>
<th>Primary End User</th>
<th>EMM Priority</th>
<th>Domain Joined</th>
<th>App Footprint</th>
<th>SCCM Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee-Owned Machines</td>
<td>BYOD</td>
<td>Varied</td>
<td>User privacy</td>
<td>No</td>
<td>Light</td>
<td>No</td>
</tr>
<tr>
<td>Remote Employee Devices</td>
<td>Remote</td>
<td>Mobile</td>
<td>Enablement</td>
<td>Maybe</td>
<td>Light</td>
<td>No</td>
</tr>
<tr>
<td>Corporate Office Devices</td>
<td>Enterprise</td>
<td>Static</td>
<td>Security</td>
<td>Yes</td>
<td>Heavy</td>
<td>Maybe</td>
</tr>
</tbody>
</table>

This tutorial addresses the required components and recommended configurations for the most common Windows 10 use cases. Since configuration requirements and recommendations vary by use case, when applicable, the following sections specify which use cases a particular configuration applies to.

### Selecting an Onboarding Workflow

**Introduction**

Workspace ONE UEM supports a variety of onboarding workflows that address multiple use cases. The onboarding method impacts other configuration decisions, and therefore is an important starting point when planning a Workspace ONE UEM deployment. In this section, learn about the available onboarding options for Windows 10, and evaluate which option is best for your organization.

**Understanding Onboarding Options**

The following table lists recommended and supported onboarding workflows by use case - as well as some requirements. Keep in mind, many of these requirements are driven by the operating system.

For a decision tree to help you identify the enrollment flows that best suit your organization, see Selecting an Onboarding Workflow.

#### Onboarding Options by Use Case

<table>
<thead>
<tr>
<th></th>
<th>BYOD</th>
<th>REMOTE</th>
<th>ENTERPRISE</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent-Based Enrollment</td>
<td></td>
<td></td>
<td></td>
<td>Admin privileges required for end user</td>
</tr>
</tbody>
</table>
| Azure Enrollment     |      |        |            | Microsoft Azure Active Directory Premium license required
|                      |      |        |            | Admin privileges required for end user (except Autopilot enrollment) |
| Command-Line Enrollment |    |        |            | Supports Workgroup and domain joined device enrollment
|                      |      |        |            | Supports automated onboarding using current PCLM
|                      |      |        |            | Non-admin end user must run in SYSTEM
|                      |      |        |            | To avoid username and password prompts, pre-populate device serial numbers in the console |
| Dell Provisioning    |      |        |            | Dell Provisioning Services required
|                      |      |        |            | Supports Workgroup, on-premises domain joined, and Azure based enrollments
|                      |      |        |            | (On-Prem Domain Joining Only) Access to corporate domain required on first boot |

? Recommended    ? Supported    ? Not Supported
For requirements and up-to-date information about all onboarding scenarios, see Microsoft mobile device enrollment.

Selecting an Onboarding Workflow

The following figure is a decision tree intended to help you select an appropriate onboarding workflow. Examine the tree to determine which enrollment flows best suit your organization. Then, refer to the descriptions of the enrollment flows in following sections to learn more.

![Windows 10 Onboarding Decision Tree](image)

**Agent-Based Enrollment**

The agent-based enrollment method now uses VMware Workspace ONE Intelligent Hub (formerly known as AWAgent). The primary use case for agent-based enrollment is existing company-owned or BYOD devices that the end user self-onboards. The workflow is similar to the standard onboarding workflows for iOS and Android devices.

To walk through this enrollment workflow, see the article Enrolling Your Windows 10 Device with a Basic Account.

**Microsoft Azure Active Directory Enrollment**

Workspace ONE UEM integrates with Azure AD, providing a robust selection of onboarding workflows that apply to a wide range of Windows 10 use cases. However, Azure licensing requirements stipulate that you must purchase an additional Azure AD Premium license to complete this integration.

Enterprises that are leveraging Azure AD typically use one of the following onboarding options for corporate-owned devices:

- Enrolling using Out-of-Box-Experience
Enrolling using Azure AD Join
Enrolling with AutoPilot
Enrolling using On-Premises Active Directory Domain

For personal-owned (BYOD) devices:

Enrolling using Azure Connect

For step-by-step instructions on how to configure these options, see the Enrolling Windows 10 Devices Using Azure AD: VMware Workspace ONE Operational Tutorial.

Command-Line Enrollment

You have several onboarding options when using command-line enrollment. From onboarding with a PC Lifecycle Management (PCLM) solution such as SCCM using Workspace ONE AirLift, to deploying a script via a group policy object (GPO), all options have one thing in common. All of these options use the command-line parameters supported with the Workspace ONE Intelligent Hub.

Organizations utilizing command-line enrollment typically use one of the following onboarding options:

- Enrolling with SCCM using Workspace ONE AirLift
- Enrolling Domain Joined devices
- Enrolling Workgroup devices
- Enrolling during Imaging/ In-Place upgrades
- Enrolling using a Group Policy Logon Script

To walk through the Workspace ONE AirLift enrollment workflow, see the article Migrating Devices and Users from SCCM. For step-by-step instructions on how to configure the remaining command-line enrollment options, see Onboarding Windows 10 Using Command-Line Enrollment: VMware Workspace ONE UEM Operational Tutorial.

Dell Provisioning

In partnership with Dell Configuration Services, Workspace ONE UEM supports creating provisioning packages to install applications and configurations on your Dell Windows 10 devices before they leave the factory. To use Dell Provisioning for VMware Workspace ONE, you must participate in Dell Configuration Services.

Dell Provisioning supports the following Workspace ONE onboarding methods:

- Azure AD Joining with Premium licenses
- Azure AD Joining without Premium licenses
- On-premises Domain Joining
- Workgroup

For instructions on how to configure these options step-by-step, see the Dell Provisioning: VMware Workspace ONE Operational Tutorial.

Configuring Workspace ONE Profiles

Introduction

Profiles 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. To create a profile, you first specify the General settings and then configure a payload. General settings determine how the profile is deployed and who receives it. The payload settings apply to the device when the profile is installed. For optimal device and console management, configure one payload per profile.

Understanding General Settings

To create a profile, you first specify the General settings and then configure a payload. General settings determine how the profile is deployed and who receives it. The General settings include the following options:
**Profile General Settings Table**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Profile name to display in the Workspace ONE UEM Console.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Read only. Version of the profile.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Brief description of the profile’s purpose.</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>If set to Managed, the profile is automatically removed if the device is unenrolled. If set to Manual, the user must manually remove the profile after the device is unenrolled.</td>
</tr>
<tr>
<td><strong>Assignment Type</strong></td>
<td>Specify how the profile is to be deployed to devices.</td>
</tr>
<tr>
<td></td>
<td>- Auto – The profile is deployed to all devices automatically.</td>
</tr>
<tr>
<td></td>
<td>- Optional – An end user can install the profile from the Self-Service Portal, or the administrator can choose which individual devices will receive the profile. End users can also install profiles representing web applications using a Web Clip or Bookmark payload. If you configure the payload to appear in the App Catalog, you can install it from the App Catalog.</td>
</tr>
<tr>
<td></td>
<td>- Compliance – The profile is applied to the device by the compliance engine when users fail to take corrective action to make their device compliant. For more information, search for Compliance Profiles Overview in VMware AirWatch Documentation.</td>
</tr>
<tr>
<td><strong>Allow Removal</strong></td>
<td>Specify whether the end user can remove the profile.</td>
</tr>
<tr>
<td></td>
<td>- Always – The end user can remove the profile at any time.</td>
</tr>
<tr>
<td></td>
<td>- With Authorization – The end user can remove the profile with the authorization of the administrator. This option adds a Password text box.</td>
</tr>
<tr>
<td></td>
<td>- Never – The end user cannot remove the profile from the device.</td>
</tr>
<tr>
<td><strong>Managed By</strong></td>
<td>The organization group with administrative access to the profile.</td>
</tr>
<tr>
<td><strong>Assigned Groups</strong></td>
<td>Specify smart groups to configure granular profile assignment. Enter an existing smart group, or click Create a new smart group.</td>
</tr>
<tr>
<td></td>
<td>The platform specified in the device profile or compliance policy takes precedence over the smart group’s platform. For example, a Windows Desktop profile is always assigned to Windows Desktops devices, even if the smart group includes other platforms.</td>
</tr>
<tr>
<td><strong>Exclusions</strong></td>
<td>To exclude selected smart groups from profiles and policies, select Yes.</td>
</tr>
<tr>
<td></td>
<td>In the Excluded Groups option that appears, select the groups to exclude from this profile or policy. If you need to create a new group, click the Create Assignment Group button.</td>
</tr>
<tr>
<td></td>
<td>If the same group is selected in Assigned Groups and Excluded Groups, you cannot save the profile or policy.</td>
</tr>
<tr>
<td><strong>View Device Assignment</strong></td>
<td>Preview the assigned devices, smart groups, and exclusions.</td>
</tr>
<tr>
<td><strong>Additional Assignment Criteria</strong></td>
<td>Select Enable Scheduling and install only during selected time periods to configure a time frame in which devices can receive the profile. In the Assigned Schedules text box, enter the name of a configured time schedule.</td>
</tr>
<tr>
<td></td>
<td>To configure a time schedule, navigate to Devices &gt; Profiles &amp; Resources &gt; Profiles Settings &gt; Time Schedules &gt; Add Schedule &gt; Add Schedule.</td>
</tr>
<tr>
<td><strong>Removal Date</strong></td>
<td>Specify a future date formatted as MM/DD/YYYY to schedule the profile’s device-side removal.</td>
</tr>
</tbody>
</table>

### Reviewing Windows 10 Payloads

This section reviews the payloads that are the most relevant in a Windows 10 deployment. Use the following table to determine whether the payload is relevant to your device use case.
### Windows 10 Profile Payloads Recommended by Use Case

<table>
<thead>
<tr>
<th></th>
<th>BYOD</th>
<th>REMOTE</th>
<th>ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passcode</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>EWS (Outlook)</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Credentials</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Restrictions</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

? Always | ? Sometimes | ? Never

### Passcode Profile for Windows 10

A passcode payload secures devices by requiring users to enter a passcode to return from an idle state. When configuring a profile for the passcode payload, use existing corporate policies to inform decision-making. Best practice is to balance organizational security requirements with usability. The preconfigured password policies on on-premises domain-joined Windows 10 devices override the Workspace ONE UEM passcode profile. Therefore, the Workspace ONE UEM passcode profile best addresses BYOD and other non-domain-joined device use cases.

### Email Profiles for Windows 10

Email profiles enable corporate email access on end-user devices. For Windows 10 devices, the available licensing for Microsoft Office applications determines which email payload to configure.

- **Device does NOT have Microsoft Office license:** Configure Exchange ActiveSync with the native mail client: The Exchange ActiveSync payload enables end users to access corporate email on their devices using the native mail client. When published, this profile relies on the Workspace ONE mobile email management infrastructure to block access to corporate email and requires integration with Secure Email Gateway or PowerShell. For more information, see VMware AirWatch Mobile Email Management in VMware Docs.

- **Device HAS Microsoft Office licenses:** Configure Exchange Web Services with the Outlook web client: The Exchange Web Services payload enables end users to access corporate email on their devices using the Outlook web client. When published, this profile uses granular conditional access policies through Workspace ONE adaptive management to grant or deny access to Outlook and the Microsoft Office suite. Office 2016 supports modern authentication -- that is, Active Directory Authentication Library (ADAL)-based sign-in -- but earlier versions do not. Earlier versions use the source network, user or group, protocols, or user agent or client type to control access.

### Credentials Profile for Windows 10

A credentials profile pushes root, intermediate, and client certificates to support Public Key Infrastructure and certificate authentication use cases. The profile pushes configured credentials to the required credentials store on the Windows desktop. The certificate handles authentication into Wi-Fi, VPN, and other corporate endpoints, providing end users with a seamless experience.

To use certificates:

1. Configure a Credentials payload with a certificate authority.
2. Configure the Wi-Fi and VPN payloads.
3. Associate the certificate authority defined in the Credentials payload when configuring the Wi-Fi and VPN payloads.
Wi-Fi Profile for Windows 10

A Wi-Fi profile auto-connects devices to corporate Wi-Fi, even if the network is hidden, encrypted, or password-protected. This payload is useful to end users who travel and use their own wireless network or are in an office setting where they can connect their devices to a wireless network onsite.

Restriction Profile for Windows 10

To help prevent data loss, a Restriction profile limits native device functionality. The icon displayed next to some settings on the Restrictions payload window indicates the OS version required to enforce the restriction.

For Windows 10, the Restriction profile limits what end users can configure in the Start > Settings menu. After the restrictions are applied, the option is grayed out in the UI. A notification that organizational policies restrict this setting is shown.

The following screenshot shows an example of a system setting enforced by a Restriction profile.

![Date and time](image)

**Date and time**
4:58 PM, Monday, April 3, 2017
Set time automatically

**Figure:** Example of a System Setting Enforced by a Restriction Profile

Customize the Restrictions profile to enforce corporate policies and apply appropriate controls to settings. The following table lists some common restrictions options across use cases.

<table>
<thead>
<tr>
<th>Windows 10 Restriction Settings Recommended by Use Case</th>
<th>BYOD</th>
<th>REMOTE</th>
<th>ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow MDM Unenrollment</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Allow Device to Send Telemetry Data</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Allow User to Change Sign-in Options</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Cortana</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Internet Sharing</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

? Allow/Enable   ? Depends on Corporate Policy   ? Don't Allow/Disable

The BYOD recommendations allow end users to control their own device. In comparison, the recommendations for remote and enterprise workers are more restrictive. These restrictions are similar to traditional GPO capabilities, so an easy way to configure this profile for enterprise users is to match the implemented GPO policies. For remote workers, weigh device security against user experience considerations.
Delivering and Managing Software

Introduction
Many issues in PC management arise from the delivery, integration, and support of software, particularly applications. This section overviews the software delivery and management options supported by Workspace ONE UEM for Windows 10.

Determining a Software Delivery Method
The recommended application delivery methods are based on the device use case, and the type of software being delivered.

The following tables show the recommendations by use case, and type of software.

<table>
<thead>
<tr>
<th>Windows 10 Software Delivery Options Recommended by Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BYOD</strong></td>
</tr>
<tr>
<td>Software Distribution</td>
</tr>
<tr>
<td>Business Portal Integration</td>
</tr>
<tr>
<td>Product Provisioning</td>
</tr>
<tr>
<td>? Recommended</td>
</tr>
</tbody>
</table>

The following table shows the recommended software delivery method for different types:

<table>
<thead>
<tr>
<th>Windows 10 Software Delivery Options Recommended by Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTERNAL APPS</strong></td>
</tr>
<tr>
<td>Software Distribution</td>
</tr>
<tr>
<td>Business Portal Integration</td>
</tr>
<tr>
<td>Product Provisioning</td>
</tr>
<tr>
<td>? Recommended</td>
</tr>
</tbody>
</table>

Together, these two tables show that software distribution addresses the majority of Windows 10 file delivery needs. For this reason, its helpful to think of software distribution as the default option, and the other methods as useful backups for edge cases software delivery cannot address.

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 life-cycle 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. For a step-by-step walk-through, see Deploying Win32 Applications: VMware Workspace ONE Operational Tutorial.
Business Store Portal Integration

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

Enabling the Business Store Portal has its own set of requirements and instructions. For more information, see the article Microsoft Store for Business and Workspace ONE UEM.

Product Provisioning

Product provisioning delivers custom or complex files to managed devices. When a file cannot directly install on devices, 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.

For a step-by-step walk-through, see the Using Product Provisioning to Deliver Files to Windows 10: VMware Operational Tutorial.

Managing Applications

Many issues in PC management arise from the delivery, integration, and support of applications. As end-user demand drives organizations to adopt more applications, these issues only grow in complexity and number. Fortunately, Windows 10 introduces features and tools that simplify application integration and management.

- **Whitelist or Blacklist by File Type** (executables, scripts, Windows installers, dynamic-link libraries, packaged apps)
- **Apply Granular Whitelists and Blacklists** (file hash, version, publisher, directory)
- **Use Role-Based Controls** (enrolled, standard, admin)
- **Provide Advanced Protection** (remove unwanted software, enforce software standardization)

Managing Windows 10 Updates

Introduction

Deploying Windows 10 fixes, patches, and updates on multiple client servicing plans creates overhead. By using branches, you can create a customized deployment schedule based on preference and update sensitivity. This section explores the available patch management options.

Understanding Patch Management

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

Windows 10 Patch Management Options

Deploying Windows 10 fixes, patches, and updates on a variety of client servicing plans creates overhead. By using branches, you can create a customized deployment schedule based on preference and update sensitivity.
Figure: Windows 10 Patch Management Options

Review the following descriptions to understand the available patch management options.

<table>
<thead>
<tr>
<th>Update Branch</th>
<th>Description</th>
<th>Feature Updates</th>
<th>Quality Updates</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Insider Build - Fast</td>
<td>Among the first to receive development builds from Microsoft; ability to provide direct feedback to Microsoft</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Used to provide feedback to Microsoft before builds are moved to slow ring</td>
</tr>
<tr>
<td>Windows Insider Build - Slow</td>
<td>More stable than fast ring and includes fixed reported during fast ring</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Used to provide feedback to Microsoft before builds are moved to release ring</td>
</tr>
<tr>
<td>Release Windows Insider Build</td>
<td>Close to public release but still early access, not on the development branch</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Used to provide feedback to Microsoft before builds are moved to public builds; IT pros and other interested employees</td>
</tr>
<tr>
<td>Semi-Annual Channel (Targeted)</td>
<td>Semi-Annual Channel</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Pilot deployments used for testing feature updates and for users such as developers. Use various teams for a wide sample set.</td>
</tr>
<tr>
<td>Semi-Annual Channel</td>
<td>Semi-Annual Channel</td>
<td>0-180 days</td>
<td>0-30 days</td>
<td>Board deployment of features, you can choose from the ranges to build your distribution rings across organization</td>
</tr>
</tbody>
</table>
Summary and Additional Resources

Conclusion
This tutorial introduces you to how Workspace ONE UEM manages Windows 10 through a product discussion and exploration of concepts.

The use cases show how to configure Workspace ONE UEM to manage and deploy Windows 10 devices in your organization. Optimal management starts with selecting the onboarding method that best fits your particular use case, understanding which profiles best control device behavior, and evaluating software delivery options.

Terminology Used in This Tutorial
The following terms are used in this tutorial:
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adaptive access</td>
<td>The ability to control access and authentication methods to sensitive apps based on a device's managed status.</td>
</tr>
<tr>
<td>additive</td>
<td>Includes only changes developed after the latest version of the application or the last additive patch.</td>
</tr>
<tr>
<td>app dependencies</td>
<td>Applications required by the environment and devices to run the Win32 application.</td>
</tr>
<tr>
<td>app patches</td>
<td>Files that apply additive or cumulative fixes, updates, or new features to applications.</td>
</tr>
<tr>
<td>app transforms</td>
<td>Files that control application installation and can add or prevent components, configurations, and processes during the process.</td>
</tr>
<tr>
<td>app uninstall process</td>
<td>Scripts that instruct the system to uninstall an application under specific circumstances.</td>
</tr>
<tr>
<td>application store</td>
<td>A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.</td>
</tr>
<tr>
<td>auto-enrollment</td>
<td>Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box Experience.</td>
</tr>
<tr>
<td>BitLocker</td>
<td>Full disk encryption available for Windows, focused on addressing data leakage or data theft scenarios from stolen, lost, or incorrectly decommissioned devices.</td>
</tr>
<tr>
<td>bring your own device (BYOD)</td>
<td>The process of providing secure access to corporate data, apps, and content on an employee-owned device without invading employee privacy to their personal data, apps, or content.</td>
</tr>
<tr>
<td>business mobility</td>
<td>The concept of being able to provide secure access to your business services, infrastructure, and content to enable your workforce to work remotely.</td>
</tr>
<tr>
<td>catalog</td>
<td>A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.</td>
</tr>
<tr>
<td>cloud</td>
<td>Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.</td>
</tr>
<tr>
<td>conditional access</td>
<td>To provision access to a resource or service, based on user entitlements or roles.</td>
</tr>
<tr>
<td>container</td>
<td>The separation of corporate and personal data on employee-owned devices, allowing IT administrators to manage corporate applications and profiles without invading employee privacy or personal apps and content.</td>
</tr>
<tr>
<td>cumulative</td>
<td>Includes the entire application, including any changes since the latest version of the application, or the last patches.</td>
</tr>
<tr>
<td>data leakage protection</td>
<td>Software-controlled policies that determine how and where data can be transferred or shared to.</td>
</tr>
<tr>
<td>device enrollment</td>
<td>The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.</td>
</tr>
<tr>
<td>Device Health Attestation</td>
<td>Module that gathers device health measurements and reports these measurements to the Health Attestation Service for evaluation.</td>
</tr>
<tr>
<td>enrollment</td>
<td>The process of allowing your device to be managed by the software-defined policies of the chosen enterprise mobility management provider.</td>
</tr>
<tr>
<td>enterprise mobility management</td>
<td>The concept of using software and policies to both secure and provide access controls for mobile devices.</td>
</tr>
<tr>
<td>files and actions</td>
<td>The combination of the files delivered to a device and the actions that file performs on the device. Files and actions cannot be assigned directly to a device. Instead, assign files and actions to a product, which then provisions to devices.</td>
</tr>
<tr>
<td>Health Attestation Services</td>
<td>Cloud service that evaluates health measurements from the device to determine the health state.</td>
</tr>
<tr>
<td>identity-as-a-service</td>
<td>Identity and access management services through the cloud to provide SSO identity federation and user-access provisioning.</td>
</tr>
<tr>
<td>identity provider (IdP)</td>
<td>A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.</td>
</tr>
<tr>
<td>mobile application management</td>
<td>The concept of managing access, deployment, and restrictions of mobile applications using software and services.</td>
</tr>
<tr>
<td>mobile device management (MDM) agent</td>
<td>The concept of managing mobile devices using software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.</td>
</tr>
<tr>
<td>multi-factor authentication</td>
<td>Access control process that requires users to authenticate using more than one method of authentication by providing something the user knows (a password) and something the user has, such as a hardware token, smartphone, or phone, or something the user is, such as a fingerprint or retina.</td>
</tr>
<tr>
<td>one-touch login</td>
<td>A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.</td>
</tr>
<tr>
<td>per-app VPN</td>
<td>Policies that allow individual apps to access VPN configurations without granting device-wide access to the VPN connection.</td>
</tr>
<tr>
<td>public app stores</td>
<td>Portals where users can access and obtain publicly published applications, such as the iOS App Store and Google Play Store.</td>
</tr>
<tr>
<td>service provider (SP)</td>
<td>A host that offers resources, tools, and applications to users and devices.</td>
</tr>
<tr>
<td>smart groups</td>
<td>Groups that control which devices get which product, based on how the group is created.</td>
</tr>
<tr>
<td>step-up authentication</td>
<td>Restricting applications or services to require a stronger authentication method, depending on the sensitivity or severity of the resource.</td>
</tr>
<tr>
<td>unified endpoint management</td>
<td>A single platform that allows organizations to manage and secure every endpoint, any app, and content across deployment use cases.</td>
</tr>
<tr>
<td>virtual desktop</td>
<td>The user interface of a virtual machine that is made available to an end user.</td>
</tr>
<tr>
<td>virtual machine</td>
<td>A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.</td>
</tr>
<tr>
<td>Windows Information Protection</td>
<td>Formerly Enterprise Data Protection (EDP), a Windows solution to assist in preventing data leakage without impeding the user experience.</td>
</tr>
</tbody>
</table>

For more information, see the [VMware My Workspace ONE Glossary](https://www.vmware.com/support/workspaceone/glossary.html) or the [VMware Technical Publications Glossary](https://www.vmware.com/support/pubs.html).
Additional Resources
For more information about Workspace ONE, you can explore the following resources:

- VMware Workspace ONE Action Path
- VMware Workspace ONE product page
- VMware Workspace ONE Documentation
- VMware Identity Manager product page
- VMware Identity Manager Documentation
- VMware Workspace ONE UEM, powered by VMware AirWatch product page
- VMware AirWatch Documentation
- VMware Workspace ONE free trial
- VMware Workspace ONE Cloud-Based Reference Architecture
- VMware Workspace ONE and VMware Horizon 7 Enterprise Edition On-premises Reference Architecture
- VMware End-User-Computing Blogs
- Workspace ONE UEM Hands-On Lab

Searching for More Information
When looking for more VMware documentation, you can focus the search using the Advanced Search option.

1. In the VMware Workspace ONE Documentation window, select the gear icon to start an advanced search.
2. Enter words or phrases to start the search.
   Example: To search for an article that you think is called Compliance Profile Overview, you might include just the key words, in case the article now has a different name.
3. Narrow the results by selecting specific criteria.
   Example: The search is limited to the specific product and version.
4. Click Advanced Search.
5. In the resulting hit list, you can select a hit. Or you can either apply Sort By filters, or narrow the results further by clicking...
About the Authors

This tutorial written by:

- Josué Negrón, EUC Staff Architect, End-User-Computing Technical Marketing, VMware
- Hannah Horton, EUC Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

Considerable contributions were made by the following subject matter experts:

- Varun Murthy, Product Line Manager, VMware
- Nigitha Alugubelli, Sr. Product Manager, VMware
- Jason Roszak, Sr. Director Product Management, VMware
- Darren Weatherly, Specialist Systems Engineer, VMware
- Robert Terakedis, Sr. Technical Marketing Manager, EUC Technical Marketing, VMware
- Aditya Kunduri, Group Product Marketing Manager, EUC Mobile Marketing, VMware
- Ajay Padmakumar, VMware alumni
- Pedro Bravo, VMware alumni

Feedback

The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.