ENROLLING WINDOWS 10 DEVICES USING AZURE AD: VMWARE WORKSPACE ONE UEM OPERATIONAL TUTORIAL

VMware Workspace ONE
Table of Contents

Overview

– Introduction

– Audience

Enrolling Windows 10 Using Microsoft Azure AD

– Introduction

– Prerequisites

– Planning Your Implementation

– Integrating Azure AD with Workspace ONE UEM

– Leveraging the Workspace ONE First-time Launch Experience for Windows 10

– Enrolling using Out-of-Box-Experience

– Enrolling with Autopilot

– Enrolling using Azure AD Join

– Enrolling Using On-Premises Active Directory Domain

– Enrolling using Azure Connect

Summary and Additional Resources

– Conclusion

– Terminology Used in This Tutorial

– Additional Resources

– Searching for More Information

– About the Authors
Feedback
Enrolling Windows 10 Using Azure: VMware Workspace ONE UEM Operational Tutorial

Overview

Introduction
VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. This tutorial provides you with practical information and exercises to help you set up device enrollment in your Windows ONE UEM management solution in conjunction with Microsoft Azure Active Directory, and to address the unique circumstances of your use cases.

Audience
This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. 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 Workspace ONE® Access (formerly VMware Identity Manager) and VMware Workspace ONE® UEM is also helpful.

Enrolling Windows 10 Using Microsoft Azure AD

Introduction
VMware Workspace ONE UEM integrates with Microsoft Azure Active Directory (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

Note: The Azure AD Premium license supports onboarding capabilities. If you want only Windows Store for Business (Business Store Portal) integration, this step is not required.

Prerequisites
Microsoft Azure is generally used for new devices, and to co-manage existing SCCM-managed devices. Most organizations maintain both for new and existing devices.

Before you can perform the procedures in this tutorial, verify that your system meets the following prerequisites:

- Workspace ONE UEM 1810 or later
- Workspace ONE UEM Admin Account
- Microsoft Azure AD Premium P1 or greater license, or any bundle which includes this license
- Microsoft Azure AD Admin Account to add the AirWatch by VMware app
- A valid, configured Directory Type under Directory Services in the Workspace ONE UEM console. If Azure AD is your source of truth directory (Pure AAD Model), select None for your Directory Type.

Note: The Azure AD Premium license supports onboarding capabilities. If you want only Windows Store for Business (Business Store Portal) integration, this step is not required. See Business Store Portal Integration for Automated Delivery in Planning Your Windows
10 Deployment: VMware Workspace ONE UEM Operational Tutorial

For more information, see the VMware Identity Manager Documentation and VMware Workspace ONE UEM Documentation.

Planning Your Implementation

Azure AD supports many configurations including managed (password hash sync or Pass-through Authentication) or federated (using an identity provider which supports both WS-Trust and WS-Fed protocols). To simplify these options, we will focus on how you add your users into Azure AD. If you create your users directly in Azure AD, we will call this pure Azure AD. If you create users in on-premises AD or another third-party user source, we will call this hybrid Azure AD. Because users are synced into Azure AD in the Hybrid model, users will obtain an Immutable ID attribute. This Immutable ID attribute is required in later steps.

Azure AD Onboarding Workflow

1. Administrator configures the integration between Azure AD and Workspace ONE UEM.
2. End-users begins one of the Azure AD-based onboarding flows. Based on the users email/UPN, Azure AD retrieves the authentication endpoint (managed/federated) and redirects users to authenticate and provide MFA if configured.
3. After the user is successfully authenticated, Azure AD sends the JWT token along with the Terms of Use and Enrollment URLs to the device.
4. Device redirects to Workspace ONE UEM and enrollment restrictions are checked, if enabled. Workspace ONE UEM parses the JWT token to obtain Azure AD directory ID (TID), Object ID (OID), and the UPN for the user. Workspace ONE UEM uses these attributes to query Azure AD for the user’s attributes, including the Immutable ID if present.
5. If there is no Immutable ID, then we follow the Pure Azure AD model and the user is created in Workspace ONE UEM using the obtained attributes from Azure AD. If there is an Immutable ID, then Workspace ONE UEM attempts to match this attribute with the Immutable ID Mapping Attribute configured in the Workspace ONE UEM Console.
6. After a successful match, Workspace ONE UEM prompts for any optional enrollment prompts or terms of use if configured.
7. Azure AD sends Access Token to device which is forwarded to Workspace ONE UEM. Workspace ONE UEM parses token and saves the device into the database, keeping track of the Azure AD Device ID.
8. Lastly, Workspace ONE UEM performs any additional configured enrollment restrictions. If triggered the device is wiped, if not the device has successfully joined Azure AD and enrolled into Workspace ONE UEM.
Integrating Azure AD with Workspace ONE UEM

This exercise walks you through the procedures for configuring enrollment for both SaaS and On-Premises applications. Screenshots are from the Microsoft Azure tenant available at the time this document was written.

1. Log in to the Workspace ONE UEM Console

![Login to the Workspace ONE UEM Console]

User name

Password

Log In

Trouble Logging In

1. In the Workspace ONE UEM Console login window, enter your user name and password.
2. Click Log In.

2. Navigate to All Settings
ENROLLING WINDOWS 10 DEVICES USING AZURE AD: VMWARE WORKSPACE ONE UEM OPERATIONAL TUTORIAL

Click Groups & Settings.

1. Click Groups & Settings.
2. Click All Settings.

3. Navigate to Directory Services

1. In the left-hand navigation bar, click System.
2. In the System menu, click Enterprise Integration.
3. In the Enterprise Integration menu, click Directory Services.
4. Enable Azure AD

1. Scroll down to the Advanced options.
2. Click Use Azure AD For Identity Services.

5. Copy URLs

1. In the organization group configured to enroll Windows 10 devices, copy the following:
   - MDM Enrollment URL
   - Terms of Use URL
2. Save the URLs to a text file.

6. Navigate to Azure Active Directory
Log in to the Microsoft Azure tenant, and in the navigation bar on the left, click Azure Active Directory.

1. Click Mobility (MDM and MAM).
2. Click Add application.
   
   Note: Make sure that you do not assign the same users to both Workspace ONE and other third-party MDM providers.

7. Add a SaaS Application
1. Select the **AirWatch by VMware** app.
2. Click **Add**.
3. Close the Add an Application window, after the application has been added.

You are taken back to the Mobility (MDM and MAM) page. Select the **AirWatch by VMware** app which you just added, to begin
8. Assign the SaaS App MDM

1. Assign the proper MDM user scope. You can select All or Some and choose a group of users.
2. Complete the following:
   - Paste your MDM Terms of Use URL from the Workspace ONE console into the MDM terms of use URL field in Azure.
   - Paste your MDM Enrollment URL from the Workspace ONE console into the MDM discovery URL field in Azure.
3. Click Save.

9. Add an On-Premises Application
Click **Add application**.

**Note**: Generally, you need to add the on-premises app only if you have a custom host name. This means you have a dedicated SaaS or on-premises. However, adding the app causes no harm to your setup. It also enables you to avoid the need to troubleshoot Azure enrollment errors when enrolling devices.

### 10. Select the On-Premises Application
1. Select the On-premises MDM application.
2. Click Add.
Click On-premises MDM application which was just added, to begin configuration.

11. Assign the On-Premises App MDM

1. Assign the proper MDM user scope. You can select All or Some and choose a group of users.
2. Complete the following:
   - Paste your MDM Terms of Use URL from the Workspace ONE console into the MDM terms of use URL field in Azure.
   - Paste your MDM Enrollment URL from the Workspace ONE console into the MDM discovery URL field in Azure.
3. Under Configure, click Save.
4. Click On-premises MDM application settings.
Click Expose an API.

1. Click Edit next to Application ID URI.
2. Enter your Device Services URL (hostname of the other URLs) into the Application ID URI text box.
3. Click Save.

12. Navigate to Licenses
1. Click Azure Active Directory.
2. Click Licenses.

13. Select Premium Licenses
1. Click **All Products**.
2. Select the proper license (onboarding requires Azure AD Premium P1 or later, or any bundle which includes this license).

### 14. Assign Premium Licenses

1. Click **Assign**.
2. Choose the users or groups to add, and click **Assign**.

### 15. Copy Directory Data

1. Click **Assign**.
2. Choose the users or groups to add, and click **Assign**.
To find the Directory ID,

1. Click **Properties**.
2. To the right of Directory ID, click the copy icon and copy to a text file for later.

### 16. Copy Domain Name
1. Click Custom domain names.
2. Copy the Name which is listed as the primary domain and paste into a text file for later.

17. Paste the Tenant Data
Return to the Workspace ONE UEM Console.

1. Paste the copied directory ID into the Directory ID text box.
2. Paste the copied domain name into the Tenant Name text box.
3. Update the Immutable ID Mapping Attribute if needed.
   - Specify the AD attribute Source Anchor in Azure AD Connect. The Source Anchor is mapped to the Immutable ID in Azure AD. Workspace ONE UEM uses this to assign devices to AD users during enrollment through Azure AD.
4. Click Save.

**Note:** By default, objectGUID is used for the Immutable ID Mapping Attribute. However, in some cases this value will differ if the sourceAnchor attribute was changed when setting up Azure AD Connect or if using a third-party user source. You must match the sourceAnchor attribute being sent to Azure AD with the Immutable ID Mapping Attribute in the Workspace ONE UEM Console. The most common attribute used after the default objectGUID is mS-DS-ConsistencyGuid. For more details about sourceAnchor attributes, see Azure AD Connect: Design Concepts.

**Leveraging the Workspace ONE First-time Launch Experience for Windows 10**

Enhance the end-user experience while onboarding into Workspace ONE UEM by enabling and customizing the Workspace ONE first-time launch experience. Workspace ONE first-time launch works with any onboarding method if the Workspace ONE app is installed before or during enrollment, including using the `DOWNLOADWSBUNDLE=True` command line parameter. Shortly after enrollment
Enrolling using Out-of-Box-Experience

This enrollment option is used primarily for new company-owned devices that are not domain joined, and is triggered the first time an end user powers on a device. The user joins the device to the Azure cloud domain as part of the initial setup process. This workflow does not require end users to have admin privileges.

**Note:** If you are leveraging Microsoft Windows Autopilot, end-user configuration is simplified and streamlined, but requires having the original equipment manufacturer (OEM) of your device preregister these devices with Microsoft.

When end users power on a device for the first time, they respond to the following device prompts:

1. Enter corporate credentials.
2. Set up multi-factor authentication.

**Note:** In most cases, end users are prompted to provide a phone number for a call or text. However, Windows Hello for Business provides more advanced options, such as facial recognition, retinal scanning, or creating a unique PIN.

Devices then join the Azure cloud domain, and register with VMware Workspace ONE UEM for management.

Enrolling with Autopilot

You can use Windows Autopilot to simplify device enrollment, and to set up and pre-configure new devices for productive use, or to reset, repurpose, or recover devices. You can avoid the need to build, maintain, and apply custom operating system images to the devices.

With every Autopilot deployment, devices do the following by default (you can create deployment profiles to customize additional options):
Skip Cortana, OneDrive, and OEM registration setup pages
Automatically set up for work or school
Get a customized Sign-In experience with company or school branding

For more information from Microsoft, see Manage Windows device deployment with Windows Autopilot Deployment. For a production example, see Microsoft Autopilot with VMware Workspace ONE UEM.

What Is Autopilot?

Windows Autopilot is a capability from Microsoft that allows pre-configuration for Windows 10 devices in conjunction with the Out-Of-Box-Enrollment (OOBE) experience. One of the most significant capabilities is that you can directly ship an end-user a Windows 10 device and as soon as it is powered on, it shows the user a customized login screen during OOBE requesting the user to enter their credentials. After successful authentication, the device is joined to Azure AD, automatically enrolled into Workspace ONE, and all the user's apps and configurations are automatically installed.

Autopilot Prerequisites

Before you can perform the procedures in this exercise, verify that the following components are installed and configured:

- A Windows 10 Professional, Enterprise, or Education device (physical or virtual) running version 1703 or later with internet access
- Azure AD Premium P1 or P2
- Azure AD integrated with Workspace ONE UEM (see Integrating Azure AD with Workspace ONE UEM)
- Users must have permission to join devices to Azure AD
  - Check this in your Azure Portal at Azure Active Directory > Devices > Device Settings and allow everyone, no-one, or a specific group. You can also configure adding other administrator accounts to the device during Azure AD join here.
- A functional Azure AD tenant and an Azure AD admin account that can log in to portal.azure.com
- A Microsoft Business Store account that can log in to businessstore.microsoft.com

Dell, HP, and Lenovo are Original Equipment Manufacturers (OEMs). When a new computer is purchased from an OEM, before the device leaves the OEM, the device has had several configuration tasks applied to it. These tasks include the initial installation of the Windows 10 Operating System (OS). Part of this process involves running an EXE file named Sysprep in Audit Mode. Audit Mode allows the OEM to install drivers, add applications, change windows settings, and generally get the PC ready to ship directly to an end user. Understanding the details behind Sysprep and Audit Mode is beyond the scope of this tutorial. What a VMware Workspace ONE UEM Administrator needs to understand is that when a person takes the computer out of the box and powers on the device for the first time, Sysprep has just exited Audit Mode. Thus, the first thing the end user is going to see on the device is a series of questions from Microsoft that are designed to finish the configuration of the computer. Microsoft named the Q&A section of the Windows Setup process the Out of Box Experience (OOBE). The purpose of Windows Autopilot is to reduce the number of questions the end-user is asked during OOBE by letting the IT Administrator pre-answer some of the questions.

The exact number of questions seen by the end-user during OOBE varies per OEM. Each OEM can choose to add more questions to the list based on the services they are providing with the computer. The specific version of Windows 10 also plays a factor in which questions are presented. The total number of questions seen by the end-user also varies based on if the user already has existing Windows 10 devices. It also varies based on how Windows Hello is configured. Regardless of the total number of questions asked, we can all agree that the fewer questions an end user must answer to start using Windows 10, the better the experience will be for everyone.

The most crucial point to remember about leveraging Workspace ONE UEM integrated with Windows Autopilot is that this process DOES NOT join a Windows 10 computer to an on-premises Active Directory Domain. If you want to automatically register your domain-joined devices, please refer to the Enrolling Using On-Premises Active Directory Domain section. If you want to domain-join your devices, consider using Dell Provisioning for VMware Workspace ONE for Dell devices or using the Command-Line Enrollment options.

The Windows 10 installation generates a unique hardware identifier. For Autopilot to start, the hardware identifier must be registered with Microsoft. Each OEM has a different process to handle this for all new hardware purchases made directly with the OEM. If a new computer is purchased from a third party like SHI, or Ingram Micro, or Best Buy, or the IT admin is using virtual machines, then the IT administrator is responsible for registering these systems with Microsoft. This tutorial covers how to register a single device.
The remainder of this tutorial walks through the entire setup and testing process for using Windows Autopilot with VMware Workspace ONE UEM.

1. Register Devices in the Microsoft Store for Business

Your Windows 10 devices need to be **pre-registered** in Microsoft Store for Business portal. This portal lists all devices for your organization so that you can assign an Autopilot profile. The easiest method is purchasing a device from participating OEM (as of May 2019 - Dell, HP, Lenovo, Surface or Toshiba) and they will automatically be added to your device portal.

If your OEM is not listed here or you have existing devices, it is still possible to get the required information to upload these devices to the Microsoft Store for Business portal manually.

There is a **Powershell script** `Get-WindowsAutoPilotInfo` which you can run against the machines to export the serial number and other required information into a CSV file to manually upload.

2. Install PowerShell Script

Install the `Get-WindowsAutoPilotInfo` script by opening a PowerShell session as an administrator.

1. Run the install command `Install-Script -Name Get-WindowsAutoPilotInfo -Force`

The `-Force` parameter is used to overwrite older versions of this script. You may also see a warning about using an untrusted repository, type `A`, then press `Enter` to continue.

3. Install PowerShell Script Using Group Policy or WMI
This script can also be run remotely using Group Policy or WMI. To get the current device info run:

```powershell
Get-WindowsAutoPilotInfo.ps1 -Output C:\Temp\W10.csv
```

If you are using a virtual machine, copy the W10.csv file to your local device. If using a physical device, you can copy the W10.csv to a USB drive or a network share. You upload this file in the next step.

The next step is to import the device into the Microsoft Store for Business and to create a Windows Autopilot profile which defines the steps and what the end-user sees during the OOBE process.

## 4. Import CSV File
Navigate to https://businessstore.microsoft.com/en-au/manage/dashboard then select Add Devices and import your W10.csv file containing the hardware information for your device.

5. Create New Profile
On success, you should see a message appear that confirms your device was added. You can also see your new device in the list of devices upon refreshing your browser.

1. Click Autopilot Deployment.
2. Click Create New Profile.

6. Save Autopilot Deployment Profile
Select the settings you want in the Profile:

1. Enter a name for your Autopilot Deployment profile.
2. Choose which optional settings you want to enable.
3. Click Create to save your profile.

- Skip privacy settings accepts the default settings on behalf of the users.
- Disabling local admin will not create any local admins on the device.
- Skip EULA also accepts on the end user’s behalf.

**7. Assign Autopilot Profile to Devices**
Now, assign the Windows Autopilot profile to your devices:

1. Select your device(s) in the list.
2. Click **Autopilot Deployment**.
3. Click **Apply Tech Zone Autopilot** or your newly created profile.

**Note:** It is critical that both the Device Model and the Profile are reflecting properly in the Microsoft Business Store portal before continuing. Notice that the Profile Column includes a Profile Name assigned to it. If the Profile column is blank, Autopilot will not function for the device.

### 8. Run Sysprep from Command Prompt
For your Windows 10 device to go through OOBE it must have the Sysprep process run against it. Open a Command Prompt (as an administrator) and run Sysprep using the command:

```
C:\Windows\System32\Sysprep\sysprep.exe /oobe /shutdown
```

**Note:** Do not use the `/generalize` switch as this changes the hardware identifiers which were generated using the `Get-WindowsAutoPilotInfo` script.

You have successfully configured Windows Autopilot to work with VMware Workspace ONE UEM and your Windows 10 device. The next step is to power on your Windows 10 device or virtual machine to see the benefits of streamlining the OOBE process for your end users. Remember that the OOBE process will look different depending on the build version, keep this in mind when creating end-user documentation.

**Enrolling using Azure AD Join**

This enrollment option is triggered from the device settings. Also referred to as cloud-domain join, this workflow is typically used for existing company-owned devices that are not already joined to an on-premises domain. End users must have admin privileges and use their corporate credentials to join the device to the Azure cloud domain.

1. From System Settings, users complete the following tasks:
   1. Enter corporate credentials.
   2. First-time Azure account users are prompted to provide a phone number for account recovery.
   3. Register for Windows Hello for Business by creating a unique PIN.  
      **Note:** Configure a Passport for Work profile to specify this PIN’s complexity.
2. Devices join the Azure cloud domain, and register with Workspace ONE UEM for management.

**Enrolling Using On-Premises Active Directory Domain**

This enrollment option allows domain-joined devices to automatically register with Azure AD and then automatically enroll into Workspace ONE UEM. This enrollment option works with Hybrid Azure AD meaning you connect to your on-premises AD with your Azure AD environment using Azure AD Connect. Ensure your devices are Azure AD registered, then you can auto-enroll into Workspace ONE UEM.

If your devices are not already Azure AD registered, you can control which devices automatically register with Azure AD by setting the **Register domain-join computers as devices GPO.** Be sure to properly scope your new GPO.
Note: To check if the device is Azure AD registered, run `dsregcmd /status` from the command line locally on the device.

After your on-premises domain-joined devices are Azure AD registered, you can leverage the Auto MDM Enrollment with AAD Token GPO to have the device attempt to get an AAD token and enroll into Workspace ONE UEM. This GPO is supported only on Windows 10 version 1709+. Be sure to properly scope your new GPO.
For more details, see Enroll a Windows 10 device automatically using Group Policy.

Enrolling using Azure Connect

This enrollment option is primarily used for existing company-owned or personal-owned devices that are not domain-joined, and is triggered when end users open a Microsoft Office app for the first time. End users must have admin privileges, and connect their Azure accounts to the device. Use this workflow if you already have Azure AD Premium licenses and do not want to join the device to the Azure cloud domain.

1. End users open a Universal Windows Platform version of any Office 365 app, which connects their Azure account to the device.
2. Enrollment begins.

Summary and Additional Resources

Conclusion

This tutorial introduces you to the device enrollment functionality of Workspace ONE UEM, and explains how to use this functionality to enroll Windows 10 devices. A set of exercises describe the process of configuring the Microsoft Azure onboarding method, including the procedures for configuring enrollment for both SaaS and On-Premises applications, and how to select the best enrollment option to meet your business needs. The end result is your ability to manage the Windows 10 device enrollment through the Azure AD.
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 Workspace ONE Access (formerly 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 status.</td>
</tr>
<tr>
<td>identity-as-a-service</td>
<td>Identify 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 grant the 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, smartcard, 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 publically 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://workspaceone.vmware.com/library/glossary) or the [VMware Technical Publications Glossary](https://www.vmware.com/support).
Additional Resources

For more information about Workspace ONE, explore the VMware Workspace ONE Activity Path. The activity path provides step-by-step guidance to help you level-up in your Workspace ONE knowledge. You will find everything from beginner to advanced curated assets in the form of articles, videos, and labs.

Additionally, you can check out the VMware Workspace ONE and VMware Horizon Reference Architecture which provides a framework and guidance for architecting an integrated digital workspace using VMware Workspace ONE and VMware Horizon.

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 Advanced Search.

About the Authors

This tutorial was written by:

- Josué Negrón, EUC Staff Architect, End-User-Computing Technical Marketing, VMware
Considerable contributions were made by the following subject matter experts:

- **Hannah Jernigan**, EUC Technical Marketing Manager, End-User-Computing Technical Marketing, VMware
- **Darren Weatherly**, Specialist Systems Engineer, VMware
- **Aditya Kunduri**, Group Product Marketing Manager, EUC Mobile Marketing, VMware
- **Bryan Garmon**, Sr. Solutions Engineer, VMware
- **Pete Lindley**, Sr. Specialist Systems Engineer, VMware
- **Mike Nelson**, Sr. Solutions Architect, VMware
- **Ameya Jambavalikar**, Sr. Solutions Architect, VMware

**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.