GUIDE – NOVEMBER 2018

PRINTED 7 MARCH 2019

ONBOARDING WINDOWS 10 USING COMMAND-LINE ENROLLMENT: VMWARE WORKSPACE ONE UEM OPERATIONAL TUTORIAL

VMware Workspace ONE

vmware®

Table of Contents

Enrolling Windows 10 Using Command-Line Provisioning: VMware Workspace ONE UEM Operational Tutorial

Overview

Introduction

The *Enrolling Windows 10 Using Command-Line Enrollment: VMware Workspace ONE UEM Operational Tutorial* introduces you to command-line provisioning, one of a variety of Windows 10 onboarding methods supported by Workspace ONE UEM.

You have several onboarding options when using command-line enrollment, including staged provisioning, onboarding with a PC Lifecycle Management (PCLM) solution such as SCCM using Workspace ONE AirLift, or deploying a script via a group policy object (GPO), such as a logon script. All of these options have one thing in common: using the command-line parameters supported with the Workspace ONE Intelligent Hub, which streamlines enrollment.

Purpose

This operational tutorial provides you with discussions and exercises to help with your existing VMware Workspace ONE® production environment. VMware provides operational tutorials to help you with

- Common procedures or best practices
- Complex manual procedures
- Troubleshooting

Note: Before you begin any operational tutorial, you must first deploy a production environment. For information about deployment, see the VMware Workspace ONE Documentation.

Audience

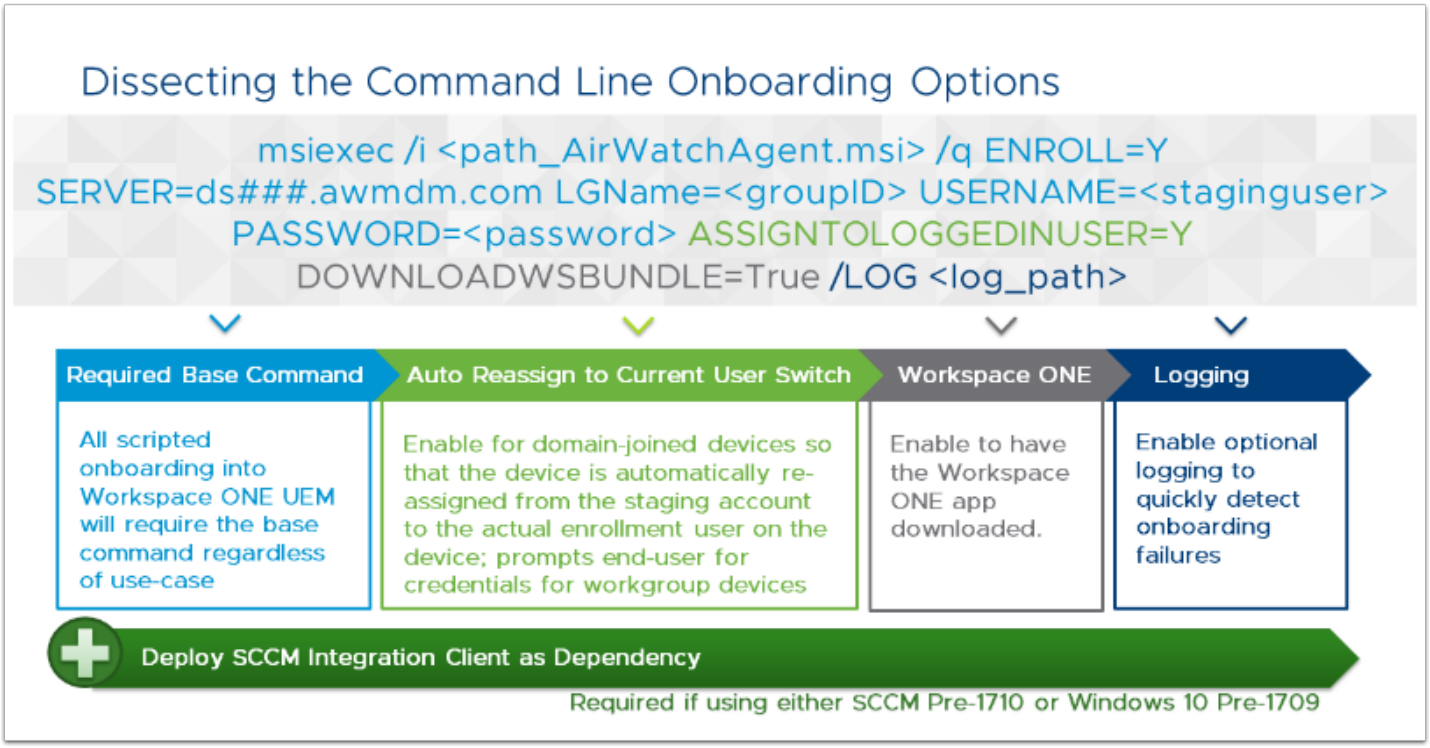
This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Identity Manager™ and VMware Workspace ONE® UEM (unified endpoint management), powered by VMware AirWatch, is also helpful.

Enrolling Windows 10 Using Command-Line Enrollment

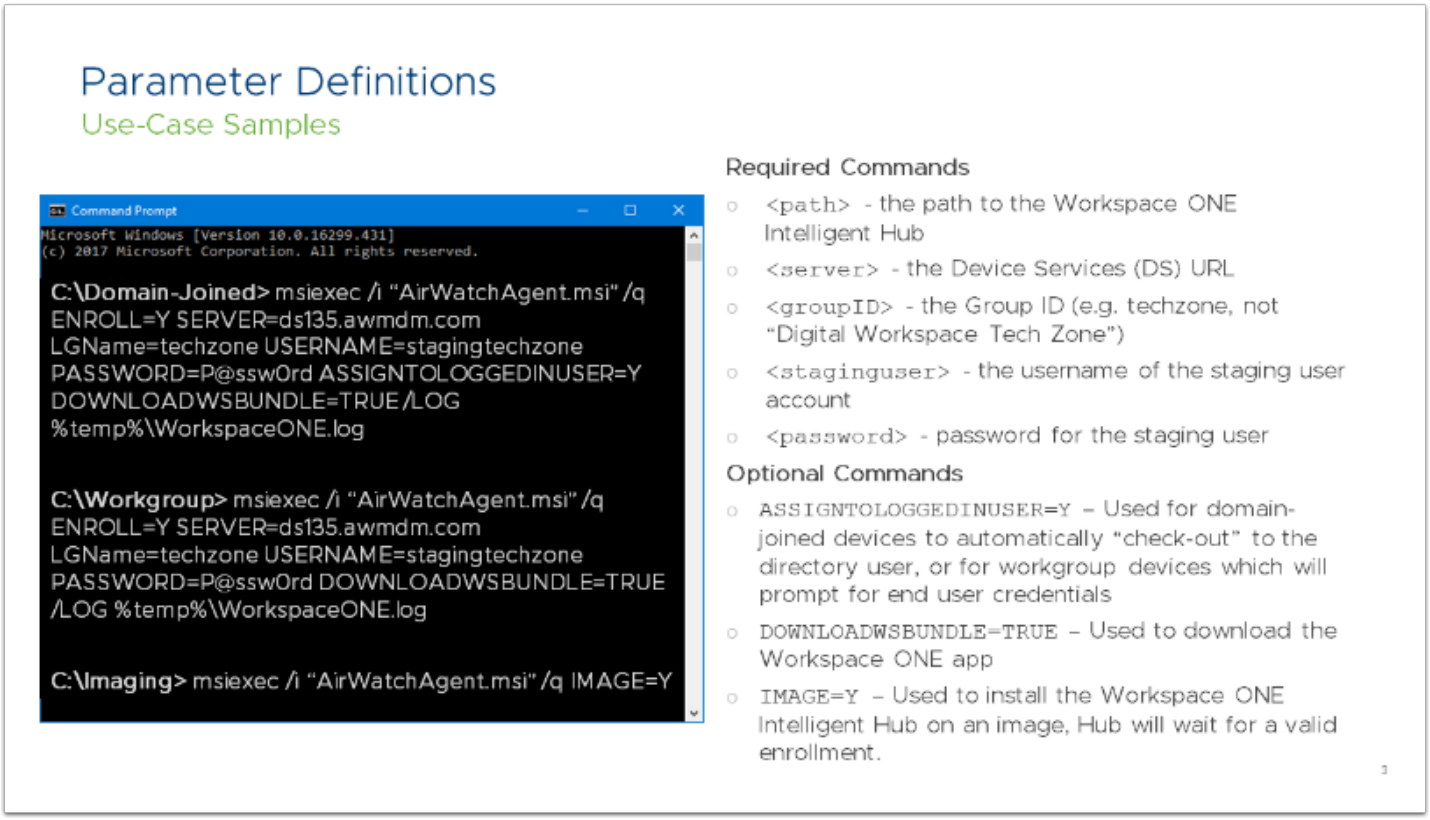
Introduction

You have several options when using command-line enrollment. This includes staged provisioning, onboarding with a PC Lifecycle Management (PCLM) solution such as SCCM using Workspace ONE AirLift, and deploying a script via a group policy object (GPO), such as a login script. All of these options have one thing in common: using the command-line parameters supported with the Workspace ONE Intelligent Hub, which streamlines enrollment.

The following figure shows the command-line options that you can use to append the required base command:



The following figure shows examples of command lines:



For more information, see *Migrating Devices and Users from SCCM* in Operational Tutorial for VMware Workspace ONE: Moving Windows 10 to Modern Management.

Additional Command-Line Enrollment Workflows

The procedures and requirements for enabling command-line enrollment depend on the following variables:

- **Client Type** — Domain-joined clients have different requirements from Workgroup (non domain-joined) devices.
- **Enrollment Scenario** — Bare metal imaging and in-place upgrade are staging workflows that have distinct enrollment requirements.

These variables lead to three primary command-line enrollment workflows:

- **Command-Line Enrollment for Domain-Joined Devices With or Without Admin Rights** (*Shown in Operational Tutorial*) — You can leverage VMware Workspace ONE AirLift when devices are currently managed by SCCM, for a more streamline experience. Overall for domain joined devices, you deploy the Workspace ONE Intelligent Hub with the proper command-line parameters to the device to enroll the current logged-on domain user (silently). If end users do not have admin rights, make sure you are executing the Hub install in System Context.
- **Command-Line Enrollment for Workgroup Devices With or Without Admin Rights** — Previously, administrators had to pre-register device serial numbers in the Workspace ONE UEM Console to enable device auto-reassignment. But now with the support of the `ASSIGNTOLOGGEDINUSER` parameter, you can enable this parameter (=Y) and the end user receives a credentials prompt from the Hub to complete enrollment. This eliminates the administrative overhead of having to pre-register devices. End users require admin rights unless the Hub install is executed using system context which requires admin rights.
- **Command-Line Enrollment During Imaging/In-Place Upgrades** — For the imaging use case, all you have to do is set the `IMAGE` parameter to `Y`. The VMware Workspace ONE Intelligent Hub is pre-installed on the image, and waits for a valid enrollment. This decreases the time after enrollment to wait for the Hub to be installed on the device. For In-Place Upgrades, you can set up the Hub using the staging command-line parameters so that enrollment automatically flips to the user account for the next domain user who logs onto the device.

Command-Line Enrollment Requirements

The following table compares the requirements (left column) of each of the onboarding options (top row).

In this table, ***Yes*** indicates that the workflow must meet the listed requirement. Following the same logic, ***No*** indicates the workflow does not need to meet the listed requirement. Footnotes provide additional details about the requirements.

	Domain Joined Devices	Workgroup Devices	Imaging/ In-Place Upgrades
Requirements			
Workspace ONE UEM Console 1810 and later Workspace ONE Intelligent Hub for Windows 1810 and later	Yes	Yes	Yes
Domain-Joined Client	Yes	No[1]	N/A
Workspace ONE Intelligent Hub for Windows deployed using System Context in your PCLM solution (such as SCCM)	Yes	Yes	Yes[2]
Staging Account, with Standard Single User Devices Enabled	Yes	Yes	Yes
Staging Organization Group	Yes[3]	Yes[3]	Yes
PowerShell Execution Policy Set to Bypass	No	Yes[4]	No
User Group Mapping Enabled at highest Organization Group[5]	Yes	Yes	Yes
Additional Resources			
Production Sample	Blog	Blog	Blog

1. The mismatch between the local account and the domain users in the Workspace ONE UEM Console causes auto-reassignment to fail for Workgroup devices. After auto-reassignment fails, the system prompts for a username and password.
2. Your PCLM solution (such as SCCM) only — this requirement does not apply to MDT.
3. Required only if SAML is enabled in your Workspace ONE UEM environment. No longer required starting in Workspace ONE UEM 1811.
4. In the SCCM Console, navigate to **Administration** > **Client Settings** > **Default Settings** > **Computer Agent**. Scroll down to **Powershell execution policy** and set it to **Bypass**.
5. User Group Organization Group or Fixed Organization Group enabled so that end users are not prompted for a Group ID. To configure this setting, navigate to **Settings** > **Devices & Users** > **General** > **Shared Device**.

Prerequisites

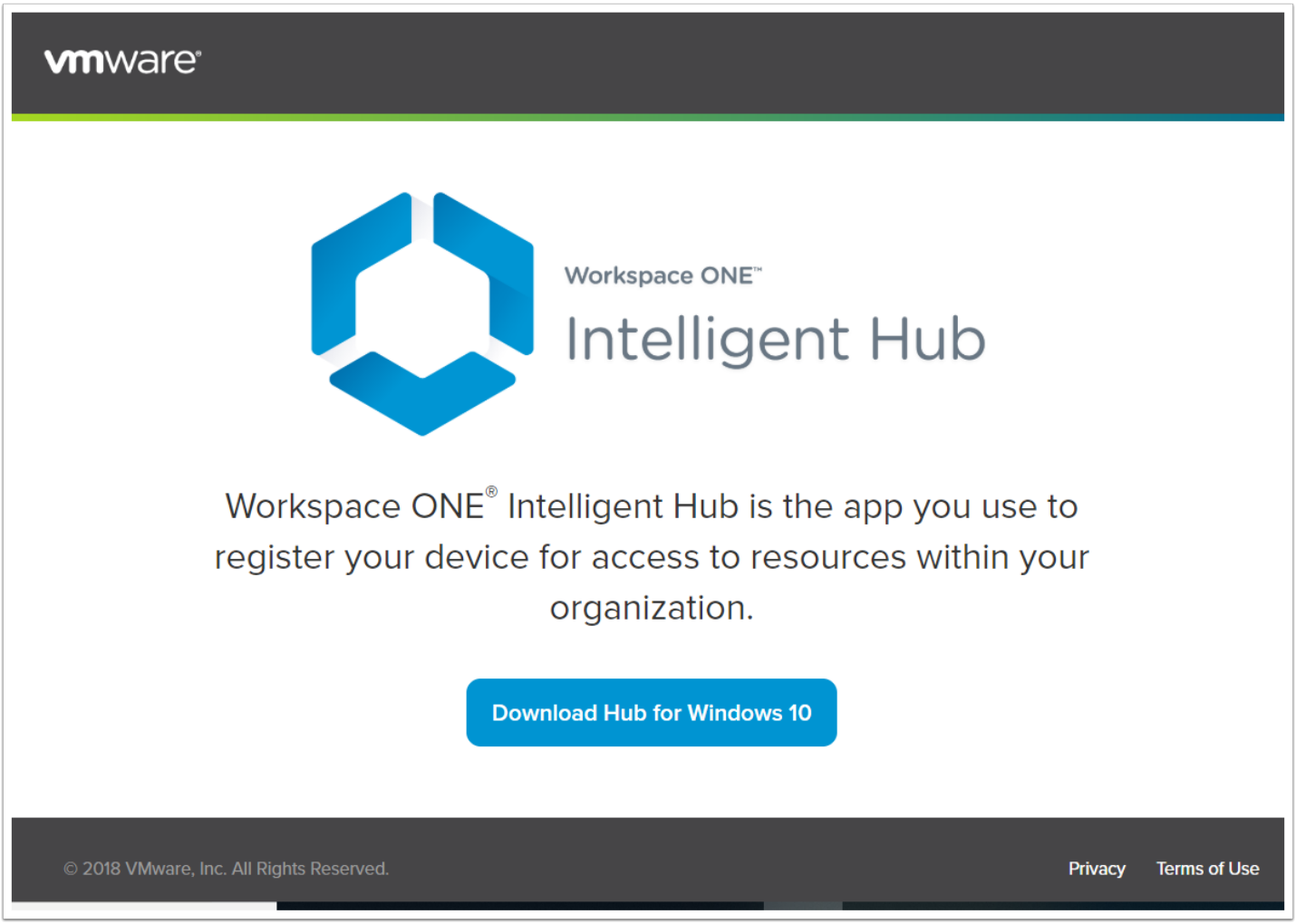
Before you can perform the procedures in this tutorial, verify that your system meets the following prerequisites:

- Workspace ONE UEM 1810 or later
- Workspace ONE UEM Admin Account
- Admin privileges for the end user with credentials for the staging account, which is the user account to pre-register it on behalf of the end user
- Uses login scripts
- Domain-joined device

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

Configuring Command-Line Enrollment

1. Download the Workspace ONE Intelligent Hub



1. On the Windows 10 device to enroll and provision, navigate to https://getwsone.com.
2. Download the latest VMware Workspace ONE Intelligent Hub.

2. Create a *.BAT File

1. Create a script to check for enrollment and if not already enrolled, perform the enrollment with the parameters for your given use-case. A sample BATCH script has been provided below.

```
REM Check if device is already registered with Workspace ONE, if not then
proceed with installing Workspace ONE Intelligent Hub
for /f "delims=" %%i in ('reg query
HKLM\SOFTWARE\Microsoft\Provisioning\OMADM\Accounts /s') do set status=%%i
if not defined status goto INSTALL
:INSTALL
REM Run the Workspace ONE Intelligent Hub Installer to Register Device with
Staging Account
REM msiexec /i “<PATH>\AirwatchAgent.msi” /quiet ENROLL=Y SERVER=<DS URL>
LGName=<GROUP ID> USERNAME=<STAGING USERNAME> PASSWORD=<STAGING PASSWORD>
ASSIGNTOLOGGEDINUSER=Y DOWNLOADWSBUNDLE=True /log <PATH TO LOG>
msiexec /i “\\192.168.6.87\AirWatchAgent.msi” /q ENROLL=Y
SERVER=ds135.awmdm.com LGName=techzone USERNAME=stagingtechzone
PASSWORD=P@ssw0rd ASSIGNTOLOGGEDINUSER=Y DOWNLOADWSBUNDLE=TRUE /LOG
%temp%\WorkspaceONE.log
```

3. Revise the Script

1. Revise the script command example so that it uses the correct information for your deployment. The REM portion of the script explains the syntax, as follows:
    - For `<PATH>`, enter the path to the Hub that you downloaded to the device.
    - For `<DS URL>`, enter the enrollment (Device Services) URL.
    - For `<GROUP ID>`, enter the short name (Group ID) of the organization group.
    - For `<STAGING USERNAME>` and `<STAGING PASSWORD>`, enter the credentials of the staging user account that has permission to stage the device on behalf of the user.
2. For more information, see

4. Create a Group Policy Object

- On the domain controller, open **Group Policy Management**, create a new Group Policy Object, and link it to your devices and users.

Note: For domain-joined devices, you can do the following to deploy this script using a Group Policy Object (GPO):

- If you are using a PCLM tool, you can leverage your PCLM to push out the Workspace ONE Intelligent Hub with command parameters.
- If you are using Microsoft SCCM, use Workspace ONE AirLift.

5. Navigate to Scripts

1. In the Group Policy Management Editor, navigate to **User Configuration** > **Policies** > **Windows Settings** > **Scripts (Logon/Logoff)**.
2. Click **Show Files**.
3. Transfer the `DeployWorkspaceONE.bat` script to the location which opens.
4. Click **Add** and select the `DeployWorkspaceONE.bat` script.
5. Confirm that the Group Policy Object is assigned to the domain user account that logs in to each device; that is, the staging account.

6. Log in

- On the device, log in as the staging admin.

  Workspace ONE UEM onboards and provisions the device profiles.

7. Ship the Device to the End User

1. When complete, shut down.
2. Provide the device to the end user.

   When the end user logs into the device, the Hub listener reads the User Principal Name (UPN) from the device registry and sends the information to the Workspace ONE UEM Console. The device registry is updated to register the device to the user.

Summary and Additional Resources

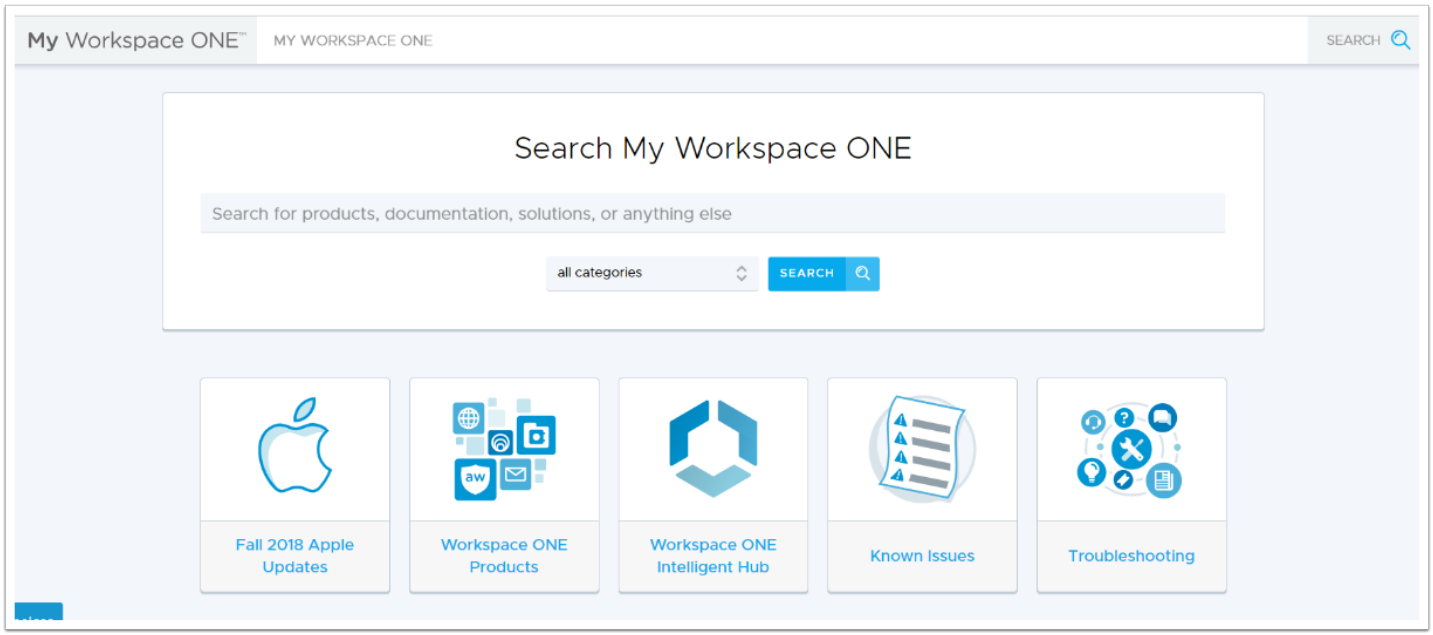
Conclusion

This tutorial introduces you to the command-line enrollment functionality of Workspace ONE UEM, and explains how to use this functionality to enroll Windows 10 devices before delivery. A set of exercises describe how to configure this workflow method on your system. The end result is your ability to manage the Windows 10 device enrollment before the device ever reaches the end user, or to enroll a Windows 10 device silently to devices already out in the field being managed by the domain, SCCM, or another PLCM solution.

Appendix: Deploying the Integration Client

If you are using SCCM, you can leverage

1. Download the Integration Client



1. From

2. Install the Client

1. In a production environment, use your PCLM solution (such as SCCM) or domain group policies to push the MSI file to managed devices and install the client.
   Note: For more information about SCCM, see Microsoft support and documentation.
2. After installation, end users can enroll Windows 10 devices using any onboarding method.

Terminology Used in This Tutorial

The following terms are used in this tutorial:

Term	Description
adaptive access	The ability to control access and authentication methods to sensitive apps based on a device's managed status.
additive	Includes only changes developed after the latest version of the application or the last additive patch.
app dependencies	Applications required by the environment and devices to run the Win32 application.
app patches	Files that apply additive or cumulative fixes, updates, or new features to applications.
app transforms	Files that control application installation and can add or prevent components, configurations, and processes during the process.
app uninstall process	Scripts that instruct the system to uninstall an application under specific circumstances.
application store	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.
auto-enrollment	Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.
BitLocker	Full disk encryption available for Windows, focused on addressing data leakage or data theft scenarios from stolen, lost, or incorrectly decommissioned devices.
bring your own device (BYOD)	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.
business mobility	The concept of being able to provide secure access to your business services, infrastructure, and content to enable your workforce to work remotely.
catalog	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.
cloud	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.
conditional access	To provision access to a resource or service, based on user entitlements or roles.
container	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.
cumulative	Includes the entire application, including any changes since the latest version of the application, or the last patches.
data leakage protection	Software-controlled policies that determine how and where data can be transferred or shared to.
device enrollment	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.
Device Health Attestation	Module that gathers device health measurements and reports these measurements to the Health Attestation Service for evaluation.
enrollment	The process of allowing your device to be managed by the software-defined policies of the chosen enterprise mobility management provider.
enterprise mobility management	The concept of using software and policies to both secure and provide access controls for mobile devices.
files and actions	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.
Health Attestation Services	Cloud service that evaluates health measurements from the device to determine the health state.
identity-as-a-service	Identity and access management services through the cloud to provide SSO identity federation and user-access provisioning.
identity provider (IdP)	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.
mobile application management	The concept of managing access, deployment, and restrictions of mobile applications using software and services.
mobile device management (MDM) agent	The concept of managing mobile devices using software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.
multi-factor authentication	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.
one-touch login	A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.
per-app VPN	Policies that allow individual apps to access VPN configurations without granting device-wide access to the VPN connection.
public app stores	Portals where users can access and obtain publically published applications, such as the iOS App Store and Google Play Store.
service provider (SP)	A host that offers resources, tools, and applications to users and devices.
smart groups	Groups that control which devices get which product, based on how the group is created.
step-up authentication	Restricting applications or services to require a stronger authentication method, depending on the sensitivity or severity of the resource.
unified endpoint management	A single platform that allows organizations to manage and secure every endpoint, any app, and content across deployment use cases.
virtual desktop	The user interface of a virtual machine that is made available to an end user.
virtual machine	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.
Windows Information Protection	Formerly Enterprise Data Protection (EDP), a Windows solution to assist in preventing data leakage without impeding the user experience.

For more information, see the VMware My Workspace ONE Glossary or the VMware Technical Publications Glossary.

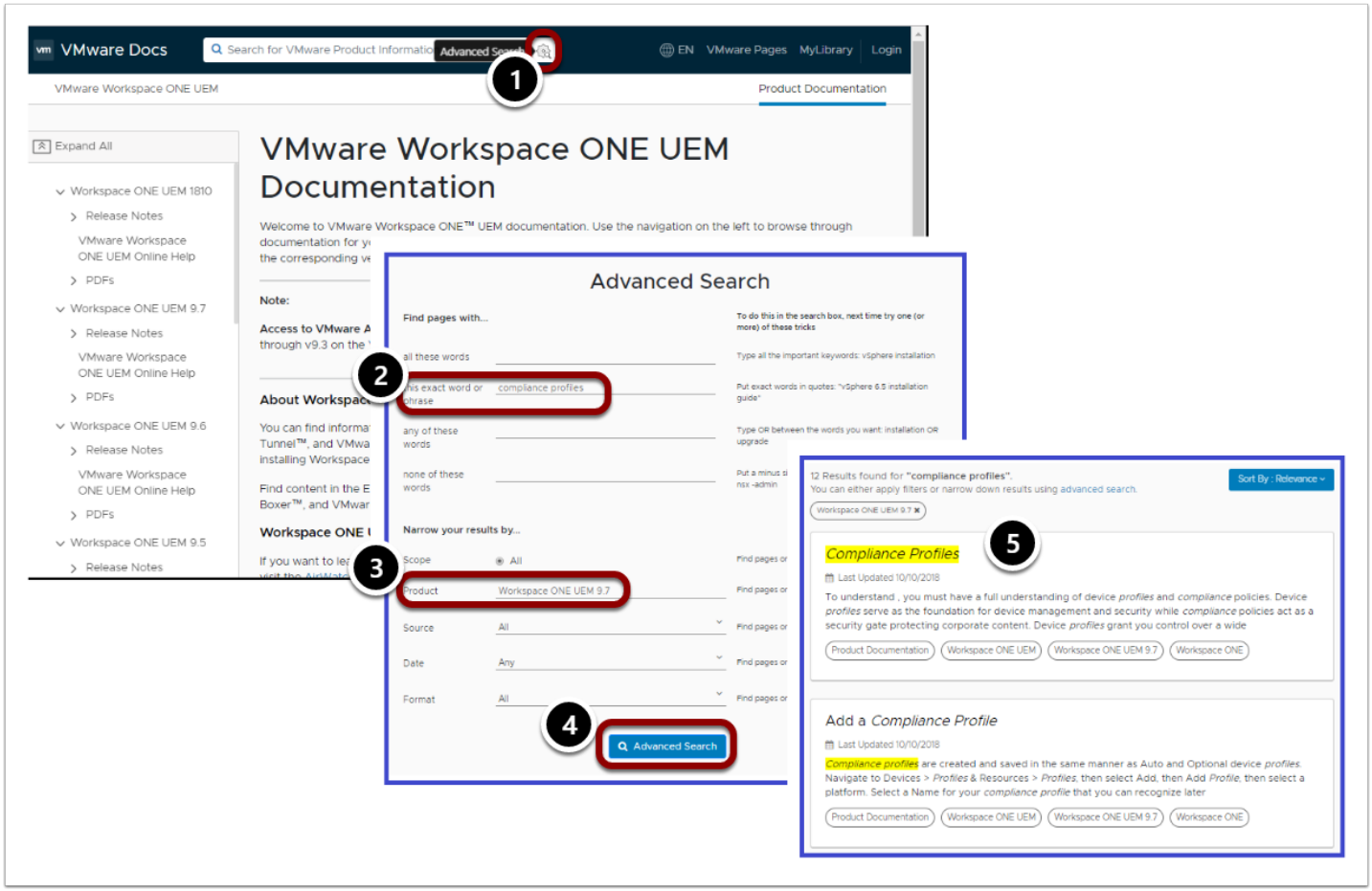
Additional Resources

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

Advanced Search.

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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com