# Table of Contents

Lab Overview - HOL-1957-04-UEM - Workspace ONE UEM - Windows 10 Management .... 4

Lab Guidance ....................................................................................................................... 5

**Module 1 - Introduction to Windows 10 Management** ...................................................... 11
  Introduction ......................................................................................................................... 12
  Login to the Workspace ONE UEM Console ................................................................. 13
  Create Test User Account .............................................................................................. 19
  Connect to the Windows 10 Virtual Machine ............................................................... 21
  Modifying Internet Options for Windows Enrollment .................................................... 22
  Enrolling Your Windows 10 Device with a Basic Account ............................................. 27
  Return to the Main Console ............................................................................................ 39
  Configuring a Device Profile for Windows 10 ............................................................... 40
  Delivering Apps on Windows 10 .................................................................................... 48
  Connect to the Windows 10 Virtual Machine ............................................................... 62
  Validate Device Enrollment .......................................................................................... 63
  Un-enrolling your Windows 10 Device ........................................................................... 67
  Conclusion ......................................................................................................................... 72

**Module 2 - Windows 10 Software Distribution and Troubleshooting** ........................ 73
  Introduction ......................................................................................................................... 74
  Connect to Windows 10 VM ............................................................................................ 76
  Login to the Workspace ONE UEM Console ................................................................. 77
  Modifying Internet Options for Windows Enrollment ..................................................... 83
  Enrolling Your Windows 10 Device ............................................................................... 88
  Deploying Notepad++ ......................................................................................................... 100
  Confirm the aduser Certificate Has Installed ............................................................... 118
  Login to the Workspace ONE Application ................................................................. 124
  Verify Notepad++ Deployment ........................................................................................ 128
  Deploying Office 365 ProPlus ....................................................................................... 145
  Verifying Office 365 Pro Plus Deployment .................................................................... 168
  Un-enrolling your Windows 10 Device ......................................................................... 181
  Sign Out of the Workspace ONE Application ............................................................. 186
  Close Chrome to Clear Session Cookies ........................................................................ 188
  Conclusion ......................................................................................................................... 189

**Module 3 - Windows 10 Real-Time and Automated Security Protection and Compliance** .................................................................................................................. 190
  Introduction ......................................................................................................................... 191
  Connect to Windows 10 VM ............................................................................................ 192
  Login to the Workspace ONE UEM Console ................................................................. 193
  Device Posture and Real-Time Compliance .................................................................. 199
  Conditional Access ........................................................................................................ 203
  Modifying Internet Options for Windows Enrollment ..................................................... 209
  Enrolling Your Windows 10 Device ............................................................................... 214
  Confirm the aduser Certificate Has Installed ............................................................... 226
Compliance with Workspace ONE ................................................................. 232
Login to the Workspace ONE Application .............................................. 233
Confirm Successful Login to the Workspace ONE App.................... 237
Sign Out of the Workspace ONE Application ....................................... 238
Create a Compliance Rule .................................................................... 240
Data Loss Prevention ............................................................................ 254
Un-enrolling your Windows 10 Device .................................................. 256
Remove the Compliance Policy ............................................................... 261
Close Chrome to Clear Session Cookies ............................................... 262
Conclusion ............................................................................................ 263

Module 4 - Manage Windows 10 Policy with Workspace ONE ............ 264
  Introduction .......................................................................................... 265
  Moving Policy to Modern Management ............................................. 266
  Policy Builder Overview .................................................................... 269
  Login to the Workspace ONE UEM Console ..................................... 271
  Connect to the Windows 10 VM ......................................................... 277
  Modifying Internet Options for Windows Enrollment ....................... 278
  Enrolling Your Windows 10 Device ..................................................... 283
  Return to the Main Console ................................................................. 295
  Review the Enrolled Device ................................................................. 296
  Review the VMware Policy Builder .................................................... 297
  Set a CSP with the VMware Policy Builder ....................................... 311
  Update an Existing CSP with VMware Policy Builder ....................... 322
  Return to the Main Console ................................................................. 335
  Un-enrolling your Windows 10 Device ................................................ 336
  Conclusion ............................................................................................ 342

Module 5 - Migrating Devices from SCCM .......................................... 343
  Introduction .......................................................................................... 344
  Introduction to Workspace ONE AirLift ............................................. 345
  Connect to the SCCM Server .............................................................. 347
  Login to the Workspace ONE UEM Console .................................... 348
  Setup Workspace ONE AirLift ............................................................ 354
  Review and Enable Co-Management in Workspace ONE AirLift ....... 358
  Review Workspace ONE AirLift .......................................................... 367
  Setup a Profile in Workspace ONE UEM ......................................... 376
  Enroll SCCM Devices in Workspace ONE UEM with AirLift ............ 383
  Login to the Workspace ONE UEM Console .................................... 403
  Review and Validate the Enrolled Windows 10 Device ...................... 409
  Conclusion ............................................................................................ 416

Module 6 - Migrating Applications from SCCM .................................. 417
  Introduction .......................................................................................... 418
  Enrolling Your Windows 10 Device (Optional) .................................... 419
  Connect to the SCCM Server .............................................................. 434
  Login to the Workspace ONE UEM Console .................................... 435
  Setup Workspace ONE AirLift ............................................................ 441
  Review and Enable Co-Management in Workspace ONE AirLift ....... 445
  Migrate Application from SCCM to Workspace ONE UEM with AirLift 454
  Connect to the Windows 10 Virtual Machine .................................... 463
  Confirm Application Install on Windows 10 Device ......................... 464
Login to the Workspace ONE UEM Console ......................................................... 466
Un-enrolling your Windows 10 Device................................................................. 472
Conclusion........................................................................................................ 477
Module 7 - Migrating Group Policy Objects to Workspace ONE UEM ............ 478
Introduction........................................................................................................ 479
Connect to the SCCM Server ......................................................................... 480
Login to the Workspace ONE UEM Console .................................................. 481
Execute the AirWatch GPO Migration Tool ....................................................... 487
Upload GPO Package to Workspace ONE UEM.............................................. 501
Assign GPO Package........................................................................................ 508
Remote Desktop to your Windows 10 Device for Enrollment ......................... 513
Modifying Internet Options for Windows Enrollment ....................................... 514
Enrolling Your Windows 10 Device ................................................................. 519
Login to the Workspace ONE UEM Console (IF NEEDED) ............................. 531
Verify GPO App Package Installed ................................................................. 534
Un-enrolling your Windows 10 Device............................................................... 546
Conclusion........................................................................................................ 551
Lab Overview -
HOL-1957-04-UEM -
Workspace ONE UEM -
Windows 10 Management
Lab Guidance

Note: It may take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

Discover how Workspace ONE UEM with Windows 10 enables Policy Configuration, OS Patch Management, Software Distribution and Security. Also, learn about new SCCM co-management capabilities in order to ease the transition from traditional to modern management for Windows 10.

Lab Module List:

- **Module 1 - Introduction to Windows 10 Management** (30 minutes) (Beginner) Explore how Unified Endpoint Management for Windows 10 enables you to configure restrictions and deploy applications to your managed devices.
- **Module 2 - Windows 10 Software Distribution and Troubleshooting** (30 minutes) (Beginner) 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. Today's sophisticated user requires control over apps on both personal and corporate-owned devices. VMware AirWatch on Windows 10 introduces features and tools to simplify application integration and management.
- **Module 3 - Windows 10 Real-Time and Automated Security Protection and Compliance** (30 minutes) (Beginner) 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. Combining traditional client requirements with modern enterprise management capabilities creates a simplified, cost-effective management solution. Use Workspace ONE UEM to establish user trust, assess the device posture, enforce conditional access, and enable data loss prevention.
- **Module 4 - Manage Windows 10 Policy with Workspace ONE** (30 minutes) (Intermediate) One of the biggest challenges with migration to Modern Management is moving from traditional GPO to Configuration Service Providers (CSPs). In this module you will configure and deploy CSPs for common policy settings.
- **Module 5 - Migrating Devices from SCCM** (45 minutes) (Intermediate) This module, you will use existing tools to migrate devices from SCCM into Workspace ONE to enable co-management. This allows moving selected workloads from traditional to modern management.
• **Module 6 - Migrating Applications from SCCM** (45 minutes) (Intermediate) In this module you will migrate existing applications from SCCM to Workspace ONE. This eases the transition from legacy PCLM to modern management. The applications can be delivered over the air leveraging CDN instead of traditional delivery methods.

• **Module 7 - Migrating Group Policy Objects to Workspace ONE UEM** (45 minutes) (Intermediate) In this module you will download and run the GPO migration tool in order to move local and group policy settings from domain managed to over the air delivery with Workspace ONE.

**Lab Captains:**

• Roger Deane, Sr. Manager, Technical Marketing, USA
• Shardul Navare, Sr. Technical Marketing Architect, USA
• Chris Halstead, EUC Staff Architect, USA
• Andreano Lanusse, EUC Staff Architect, USA
• Justin Sheets, Sr. Technical Marketing Architect, USA

**Subject Matter Experts:**

• Josue Negron, Sr. Technical Marketing Architect, USA

This lab manual can be downloaded from the Hands-on Labs Document site found here:

[http://docs.hol.vmware.com](http://docs.hol.vmware.com)

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.

2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.

3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

### Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

**Click and Drag Lab Manual Content Into Console Active Window**
You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

**Accessing the Online International Keyboard**

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.

**Click once in active console window**

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.
Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.
Look at the lower right portion of the screen

Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.
Module 1 - Introduction to Windows 10 Management
Introduction

In this lab module, you will learn how to enroll a Windows 10 device into Workspace ONE UEM and how to configure and deploy restriction profiles and applications to your enroll device.

Pre-Requisites

To successfully complete this Hands-On Lab, you'll need to ensure you have the following pre-requisites:

- A virtual machine or spare Windows device running Windows 10 (non Home edition) with the latest updates installed. DO NOT access the Hands-On Lab from the same machine you will be managing.
  NOTE - We have provided a Windows 10 VM for you which has all the pre-requisites setup for this lab. We recommend you using that by following the instructions in the manual for this lab.
- Administrative rights to the virtual machine or spare Windows device which you will be using to perform the Hands-On Lab.
- A Windows 10 Desktop app (*.msi), such as 7-Zip. A sample Windows 10 app has been provided in the lab machine for your use.

As a reminder, DO NOT access the Hands-On lab from the same machine you plan to enroll & manage as part of the HOL exercise. As part of the HOL, you will be rebooting this machine and will temporarily lose access to the lab documentation if you run the lab from the machine you enroll.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your Username. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter VMware1! for the Password field.
3. Click the Login button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

Confirm Security PIN *

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Create Test User Account

Basic accounts are the accounts which are created locally in the AirWatch admin console, as opposed to the accounts which are imported from an active directory. In this section, we will create a Basic User account which we will use for enrollment in the following section.

Click on Add / User

In the top right corner of the AirWatch console,

1. Click Add.
2. Click User.
Add User information

In the pop-up window,

1. Ensure that security type is **Basic**
2. Enter the username as **testuser**
3. Enter the password as **VMware1!**
4. Confirm the password as **VMware1!**
5. Enter the first name as **Test**
6. Enter the last name as **User**
7. Enter the e-mail address as **testuser@corp.local**
8. Click on **Save**

**NOTE - Use the scroll bar if you don't see the option to enter email address**

You should see a confirmation that user is created successfully. If the user is already created with the same username then you can use the existing user in the following section.
Connect to the Windows 10 Virtual Machine

Double-click the **Win10-01a.rdp** shortcut from the Main Console Desktop to connect to the Windows 10 virtual machine.
Modifying Internet Options for Windows Enrollment

Before enrolling the Windows 10 Virtual Machine, we will make modifications to the Windows 10 device to reduce network traffic to expedite enrollment.

Open Settings

1. Click the **Windows** button.
2. Click the **Settings (Gear)** icon.
Open Internet Options

1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.
Modify the Certificate Revocation Options

1. Click the **Advanced** tab.
2. Scroll down to find the **Security** section.
3. **Uncheck** the **Check for publisher's certificate revocation** option.
4. **Uncheck** the **Check for server certificate revocation** option.
5. Click **Apply**.
6. Click **OK**.
1. Right-Click the Windows button.
2. Click Windows PowerShell (Admin).
Allow Windows PowerShell to Make Changes

Click **Yes** when prompted to allow Windows PowerShell to make changes to your device.

**Enter Commands to Stop Windows Update Service**

Enter the following commands (remember that you can highlight then drag-and-drop the text from the manual into PowerShell!)

1. Enter `Set-Service wuauserv -startup disabled` then press **ENTER**.
2. Enter `Stop-Service wuauserv` then press **ENTER**.
3. Click the **Close** button to exit PowerShell.
Enrolling Your Windows 10 Device with a Basic Account

We will now enroll our Windows 10 device in Workspace ONE UEM. First, we will need to download the Workspace ONE Intelligent Hub.

Download the Workspace ONE Intelligent Hub on the Windows 10 VM

From a new tab in the browser, if not opened already,
2. Click **Download Hub for Windows 10**.
   **NOTE:** Please wait while the Workspace ONE Intelligent Hub installer finishes downloading.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

   **NOTE - If you do not see the warning about the AirWatchAgent.msi file, skip this and continue to the next step.**

### Launch the Workspace ONE Intelligent Hub Installer

![AirWatchAgent.msi file](image)

Click the **AirWatchAgent.msi** file in your download bar.

**NOTE - The installer may take a few seconds to launch, please be patient after clicking the AirWatchAgent.msi file.**

### Click Run

![Security Warning dialog](image)

Click **Run** to proceed with the installation.
Accept the Default Install Location

Leave the default install location and click **Next**.

*NOTE - The Next button may take several seconds to enable while the required additional features are installed.*
Accept the License Agreement

1. Select **I accept the terms of the license agreement**.
2. Click **Next**.
Start the Workspace ONE Intelligent Hub Install

Click **Install** to start the installer.
Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

If prompted to allow the app to make changes to your device, click Yes.
Complete the Workspace ONE Intelligent Hub Installer

Click Finish to complete the Workspace ONE Intelligent Hub installer.

**NOTE** - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.
Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

Click **Server Detail**.

Find your Group ID from Workspace ONE UEM Console
The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**Enter the Server Details**

1. Enter **labs.awmdm.com** for the **Server Name** field.
2. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
1. Enter **testuser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Click **Next**

**NOTE - Wait while the server checks your enrollment details.**
Since our Workspace ONE UEM and VMware Identity Manager environments are linked for this environment, the Workspace ONE Application will automatically open after enrollment is complete. You will not need it for this exercise, so click **Close**.
Finish the Workspace ONE UEM Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM.
Return to the Main Console

Click **Close (X)** on the Remote Desktop Connection bar at the top of the screen to return to the Main Console to finish making configurations within the Workspace ONE UEM Console.
Configuring a Device Profile for Windows 10

Profiles allow you to modify how the enrolled devices behave. This exercise helps you to configure and deploy a restrictions profile that we can verify has applied to the device later in the section.

Add a Profile

In the upper-right corner of Workspace ONE UEM Console:

1. Select Add.
2. Select Profile.
Add a Windows Profile

Select the Windows icon.

**Note:** Make sure that you select **Windows** and *not* Windows Rugged.

Add a Windows Desktop Profile

Select Device Type

- Windows Phone
- Windows Desktop
- Windows 7
Select **Windows Desktop**.

**Select Context - Device Profile**

Select **Device Profile**.
Define the General Settings

1. Select **General** if it is not already selected.
2. Enter a profile name such as **Windows Restrictions** in the Name text box.
3. Copy the profile name into the Description field.
4. Click in the **Assigned Groups** field. This will pop-up the list of created Assignment Groups. Select the **All Devices** Assignment Group.

**Note:** You may need to scroll down to view the Assigned Groups field.

**Note:** You do not need to click **Save & Publish** at this point. This interface allows you to move around to different payload configuration screens before saving.
Select the Restrictions Payload

![Image of Add a New Windows Desktop Profile](image)

**Note**: When initially setting a payload, a **Configure** button will show to reduce the risk of accidentally setting a payload configuration.

1. Select the **Restrictions** payload in the Payload section on the left.
2. Click the **Configure** button to continue setting the Restrictions payload.
Adding a Restriction - Disable Cortana

1. Using the scroll bar on the right, scroll down to the **Device Functionality** section.
2. Select **Don't Allow** for Cortana.
3. Notice the **10** on the right side of the Restrictions window. These are all the restrictions that Workspace ONE UEM can apply to a Windows 10 computer.
4. Click **Save & Publish**.
Publish the Restrictions Profile

Click Publish.
Navigate to Profiles List View

1. Select Devices.
2. Select Profiles & Resources.
3. Select Profiles.

Verify the Restrictions Profile Now Exists

You should now see your Restrictions Profile within the List View of the Devices Profiles window.

Note: If you need to edit the Restrictions Profile, this is where you would do so. To edit the profile, click the profile name, then select Add Version. Update the profile and click Save & Publish to push the new settings to the assigned devices.
Delivering Apps on Windows 10

You can distribute applications to Windows 10 devices, allowing for a seamless user experience. This exercise helps you to create and distribute an application to your Windows 10 device.

This exercise uses the 7-Zip installation program downloaded and stored in the **Documents** folder.

### Add Internal Application

In the upper-right corner of Workspace ONE UEM Console:

1. Select **Add**.
2. Select **Internal Application**.
Upload Application

Add Application

Organization Group ID*

Application File*

Click **Upload**.

Find the Application MSI

Add

Type

- Local File
- Link

Browse... No file selected.

You have used 0 MB of 25000 MB

Click the **Browse...** button.
Upload the EXE File

Navigate to your installation file. The 7-zip installation file has been downloaded to the server and placed in the Documents folder.

1. Select **Documents**.
2. Expand **HOL**.
3. Select the **Windows 10** folder.
4. Select your installation file, for example, **7z1604-x64.exe**.
5. Click **Open**.
Save the EXE File

Add

Type  ☐ Local File  ☐ Link

Browse...  7z1604-x64.exe

You have used 0 MB of 25000 MB

SAVE  CANCEL

Click Save.

Continue to the App Settings

Add Application

Organization Group ID*  your.email@shown here

Application File*  7z1604-x64.exe

Is this a dependency app?  YES  NO

CONTINUE  CANCEL
1. Select No for Is this a dependency app?
2. Click Continue.

**Configure App Details**

1. Enter a name for your application, for example, 7-Zip.
2. Select 64-bit for the Supported Processor Architecture.
Configure Application Files

1. Select the **Files** tab.
2. Scroll down to find the **App Uninstall Process** section.
3. Select **Input** for the **Custom Script Type**.
4. Enter the following for **Uninstall Command**:

   7z1604-x64.exe /Uninstall

**Note**: For information about copying text from the manual, see the Guidance section.
Select Deployment Options

1. Select Deployment Options.
2. Scroll down until you see the option for Install Command.
3. Enter Install Command as:

```
7z1604-x64.exe /S
```

Note: For information about copying text from the manual, see the Guidance section.
1. Scroll down to find the When To Call Install Complete section.
2. Select Defining Criteria for Identity Application By.
3. Click Add.
Configure the Install Complete Defining Criteria

1. Select **File Exists** for the **Criteria Type**.
2. Enter `C:\Program Files\7-Zip\7zFM.exe` for the **Path**.
3. Click **Add**.

**Note:** For information about copying text from the manual, see the Guidance section.
Save and Assign the Application

Click **Save & Assign**.
**Add an Assignment**

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

Click **Add Assignment**.
Add Assignment Group and Push Mode

1. Click the **Select Assignment Groups** search box and select **All Devices (your.email@shown.here)**.
2. Select **Auto** for the **App Delivery Method**.
3. Click **Add**.
Save and Publish the Application

7-Zip - Update Assignment

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Devices</td>
<td>0</td>
<td>Auto</td>
<td></td>
</tr>
</tbody>
</table>

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

Click **Save & Publish**.
Preview the Assigned Devices

No Records Found

Click **Publish**.
Connect to the Windows 10 Virtual Machine

Double-click the **Win10-01a.rdp** shortcut from the Main Console Desktop to connect to the Windows 10 virtual machine.
Validate Device Enrollment

Once your Windows 10 device is enrolled, the restriction profile and application you created earlier will be installed on the device. Continue to confirm enrollment was successful and that the profile installed correctly by verifying that the restrictions took place on your device.

Confirm Profile

1. Click on **Start** logo.
2. Click on **Cortana** in the apps list.
Cortana Disabled

Notice now you are not greeted by Cortana, you only have basic search capabilities now that Workspace ONE UEM has disabled Cortana.
Confirming Cortana is Disabled

For further confirmation, click on the Gear icon and you will see that all of the Cortana settings which were present before have now disappeared. You should only see settings regarding searching and indexing.

Confirm Application

Click Explorer from the bottom toolbar.
Open 7-Zip

1. Click **Local Disk (C:)**.
2. Click **Program Files**.
3. Click **7-Zip**.
4. Double-click **7zFM.exe** to launch the **7-Zip File Manager**.

**NOTE - If you do not see the 7-Zip Folder, your application may still be downloading. Due to lab scalability and network resources, this may take several minutes to finish.**
Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from Workspace ONE UEM console, also known as managed content.

Delete Device from Workspace ONE UEM Console

From the Workspace ONE UEM Console,

1. Click on Devices
2. Click on List View
3. Select the check box next to your device friendly name.
4. Click on More Actions
5. Click on Delete Device
1. Enter the reason as **lab completed**.
2. Click on **Delete**.
Validate DELETE IN PROGRESS...

List View

1. You may see device friendly name changing to **DELETE IN PROGRESS...**
2. Click on the **Refresh Icon** to validate if the device deletion is successful.

Ensure that device record is deleted

List View

1. Use the **Refresh Button** if needed.
2. Ensure that the device record is now deleted from the Workspace ONE UEM console and you see the message **No Records Found.**
Navigate to Windows 10 Settings

1. Click on the Windows Icon
2. Click on the gear icon to access Windows 10 Settings

Access Accounts Settings

From the Settings Menu, access Accounts
Validate That No Management Account Exists

1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to **AirWatchMDM**.

**NOTE** - The CORP AD domain is the local domain in this lab and is not controlled by AirWatch Enrollment, so you will see this connection if your device is enrolled or unenrolled.
Conclusion

In addition to managing mobile devices, Workspace ONE UEM can also manage your Windows 10 applications as well. This quick look into Windows 10 management should provide a clearer picture on how you can manage your Windows 10 devices by configuring restrictions and profiles and deploying applications alongside your mobile workforce. For a deeper dive into Windows 10 Management, consider taking the following Windows 10 modules.

This concludes the Basic Windows 10 Management module.
Introduction

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. Today’s sophisticated user requires control over apps on both personal and corporate-owned devices. Workspace ONE UEM on Windows 10 introduces features and tools to simplify application integration and management.

Software Distribution and Lifecycle Flow with Workspace ONE UEM

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.
You can use the Workspace ONE UEM software distribution feature to deliver Win32 applications, track installation statuses, keep application versions current, and delete old applications.
Connect to Windows 10 VM

We have provided you a Windows 10 VM to complete the necessary steps for this lab. Let's connect to it to complete the steps in the following section.

Connect to the Windows 10 VM

Double-click the Win10-01a.rdp shortcut on the lab desktop.

If prompted, the login credentials for the Windows 10 VM are:

- Username: corp\holuser
- Password: VMware1!
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your **Username**. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Password Recovery Question

Password Recovery Answer

Password Recovery Answer

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

Confirm Security PIN *

Security PIN

Confirm Security PIN

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Modifying Internet Options for Windows Enrollment

Before enrolling the Windows 10 Virtual Machine, we will make modifications to the Windows 10 device to reduce network traffic to expedite enrollment.

Open Settings

1. Click the Windows button.
2. Click the Settings (Gear) icon.
Open Internet Options

1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.
Modify the Certificate Revocation Options

1. Click the **Advanced** tab.
2. Scroll down to find the **Security** section.
3. **Uncheck** the **Check for publisher's certificate revocation** option.
4. **Uncheck** the **Check for server certificate revocation** option.
5. Click **Apply**.
6. Click **OK**.
Open PowerShell as Administrator

1. Right-Click the Windows button.
2. Click Windows PowerShell (Admin).
Allow Windows PowerShell to Make Changes

Click Yes when prompted to allow Windows PowerShell to make changes to your device.

Enter Commands to Stop Windows Update Service

Enter the following commands (remember that you can highlight then drag-and-drop the text from the manual into PowerShell!)

1. Enter `Set-Service wuauserv -startup disabled` then press ENTER.
2. Enter `Stop-Service wuauserv` then press ENTER.
3. Click the Close button to exit PowerShell.
Enrolling Your Windows 10 Device

We will now enroll our Windows 10 device in Workspace ONE UEM. First, we will need to download the Workspace ONE Intelligent Hub.

Download the Workspace ONE Intelligent Hub on the Windows 10 VM

From a new tab in the browser, if not opened already,

2. Click **Download Hub for Windows 10**.
   **NOTE:** Please wait while the Workspace ONE Intelligent Hub installer finishes downloading.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

   **NOTE - If you do not see the warning about the AirWatchAgent.msi file, skip this and continue to the next step.**

### Launch the Workspace ONE Intelligent Hub Installer

Click the **AirWatchAgent.msi** file in your download bar.

**NOTE - The installer may take a few seconds to launch, please be patient after clicking the AirWatchAgent.msi file.**

### Click Run

Click **Run** to proceed with the installation.
Accept the Default Install Location

Leave the default install location and click Next.

NOTE - The Next button may take several seconds to enable while the required additional features are installed.
Accept the License Agreement

1. Select **I accept the terms of the license agreement**.
2. Click **Next**.
Click **Install** to start the installer.
Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

If prompted to allow the app to make changes to your device, click **Yes**.
Complete the Workspace ONE Intelligent Hub Installer

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

**NOTE** - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.
Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

Click **Server Detail**.

**Find your Group ID from Workspace ONE UEM Console**
The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**Enter the Server Details**

1. Enter **labs.awmdm.com** for the **Server Name** field.
2. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
Enter Your User Credentials

1. Enter **aduser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Click **Next**

*NOTE - Wait while the server checks your enrollment details.*
Workspace ONE Application Launch

Since our Workspace ONE UEM and VMware Identity Manager environments are linked for this environment, the Workspace ONE Application will automatically open after enrollment is complete. You will not need it for this exercise, so click **Close**.
Finish the Workspace ONE UEM Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM.
Deploying Notepad++

In this exercise, we will deploy Notepad++ to our Windows 10 device to see how to configure and deploy an application to your end users and what the end user experience is like for interacting with these applications.

Deploying Notepad++ In Workspace ONE UEM

1. Click Apps & Books.
2. Click Add Application.

Upload Application File

Add Application

Organization Group ID*

Application File*
Click **Upload**.

**Choose Application File to Upload**

Click **Choose File**.

Click **Choose File**.
Select the Notepad++ Installer

1. Click Documents.
2. Click HOL.
3. Click Notepad++ Installer.exe.
4. Click Open.
Save the Application File

Click **Save**.

**Configure Notepad++ Application**
1. Select **No** for Is this a dependency file.
2. Click **Continue**.

**Configure Application Details**

1. Enter **Notepad++** for the Name.
2. Select **64-bit** for the Supported Processor Architecture.
Configure Application Files

1. Click **Files**.
2. Scroll down to the App Uninstall Process section.
3. Select **Input** for Custom Script Type.
4. Enter `"%ProgramFiles%\Notepad++\Uninstall.exe" /S` for the uninstall command.
Configure Deployment Options

1. Click the **Deployment Options** tab.
2. Enter **5** for Disk Space Required.
3. Select **MB** for the Disk Space Required Units.
4. Enter **50** for Device Power Required.
5. Enter **1** for RAM Required.
6. Select **GB** for the RAM Required Units.
Configure Install Options

Edit Application - Notepad++ Installer.exe v 1.0.0

1. Scroll down to the How To Install section.
2. Select **Device** for Install Context.
3. Enter `Notepad++ Installer.exe /S` for the Install Command.
4. Select **No** for Admin Privileges.
5. Enter **3** for Retry Count.
6. Enter **5** for Retry Interval.
7. Enter **15** for the Install Timeout.
Configure When To Call Install Complete

1. Scroll down to the When To Call Install Complete section.
2. Enter 1 for the Installer Reboot Exit Code.
3. Enter 0 for the Install Success Exit Code.
5. Click Add.
Add Defining Criteria

1. Select **File Exists** for the Criteria Type.
2. Enter `%ProgramFiles%\NotePad++` for the Path.
3. Click **Add**.
Configure Application Images

1. Click the **Images** tab.
2. Click the **Icon** tab.
3. Click the **Click or drag files here** button.
Select the Notepad++.png file

1. Click **Documents**.
2. Click **HOL**.
3. Click **Notepad++.png**.
4. Click **Open**.
Configure Terms of Use

1. Click the Terms of Use tab.
2. If you wanted to configure a terms of use policy for this application, you would do so here. For this lab, we will leave the Required Terms of Use as None.
3. Click Save & Assign.
Add Assignment

Notepad++ - Update Assignment

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Exclusions</th>
</tr>
</thead>
</table>

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive highest priority (0 being highest priority).

Click **Add Assignment**.
Configure Assignment

1. Select All Devices (your.email@shown.here) for Select Assignment Groups.
2. Select Auto for the App Delivery Method.
3. Click Add.
Save & Publish Notepad++ Application

Notepad++ - Update Assignment

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Exclusions</th>
</tr>
</thead>
</table>

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

[Add Assignment]

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Devices</td>
<td>0</td>
<td>Auto</td>
<td>Now</td>
</tr>
</tbody>
</table>

Click **Save & Publish**.
### Preview Assigned Devices and Publish

#### Preview Assigned Devices

<table>
<thead>
<tr>
<th>Assignment Status</th>
<th>Friendly Name</th>
<th>User</th>
<th>Platform/OS/Model</th>
<th>Organization Group</th>
</tr>
</thead>
</table>

No Records Found

Click **Publish**
Confirm the Notepad++ Application Was Added

1. Click Apps & Books.
2. Ensure the Notepad++ application was added successfully.
Confirm the aduser Certificate Has Installed

We have configured few device profiles for you to automatically install the user certificate you will need for this lab. In this section, we are going to validate if that user certificate is installed on your Windows 10 device or not before proceeding.

Check the Device Details for the Certificate Profile Status

In the Workspace ONE UEM Console,

1. Click **Devices**
2. Click **List View**
3. Click the **device link** for the enrolled device.
Install the Win10 - User Cert Profile (IF NEEDED)

1. Click the Profiles tab.
2. Mouse over the status of the Win10 - User Cert profile.
   - If the status shows as Install Failed, follow the below steps to install it.
   - If the status shows as Pending Information, refresh the page and re-check the status.
   - If the status is a green checkmark, continue to the Check the aduser Certificate on the Windows 10 Device step.
3. Select the Win10 - User Cert
4. Click Install.

Confirm the Install Action (IF NEEDED)

Click OK to confirm the Install action.
**Ensure the Win10 - User Cert Profile Installs (IF NEEDED)**

If you needed to install the Win10 - User Cert profile, follow these steps. Otherwise, continue to the next step.

1. Click **Refresh**.
2. Check the status of the **Win10 - User Cert profile**, it should update about every 1-2 minutes. If the Status is not a green checkmark, refresh until the install completes.

   **NOTE** - Mouse over the icon in the Status column to see the current status. If you see the Yellow Warning sign respond with "Install Failed", select the **Win10 - User Cert** and click Install again to restart the install process.
Check the aduser Certificate on the Windows 10 Device

1. Click the **Windows** button.
2. Type **user certificates** and the Search bar will populate.
3. Click the **Manage user certificates** option.
Allow the Microsoft Management Console to make changes

Click **Yes** when asked if you want to allow this app to make changes to your device.

Confirm the aduser Certificate Has Installed

1. Click the **Personal** folder to expand it.
2. Click the **Certificates** folder.
3. Check if the **aduser** certificate exists.
4. If the **aduser** certificate does NOT exist, wait a minute or two and click the **Refresh** button to check again. Continue to **refresh** until you see that the **aduser certificate exists**.

**Do not continue** to the next step until you've confirm that the **aduser certificate has been installed**.

*NOTE - Due to lab scalability and limitations, the aduser certificate may take a few minutes to download from the CA.*
Login to the Workspace ONE Application

1. Click the Windows button.
2. Click the Workspace ONE app icon from the start menu.
Enter the Workspace ONE Server Address (IF NEEDED)

1. Enter https://cn1193-2057-ws1win.vidmpreview.com for the Server Address field.
2. Click Continue.
Enter Your Username for Workspace ONE

1. Enter **aduser** for the username.
2. Click **Next**.

Allow Access to Credentials

Click **Allow** to allow access to your private key.

*NOTE - The user will only be prompted once for this permission.*
NOTE - If you receive the "Access Denied. Certificate login failure." screen, please wait a few minutes and try to login again. The device may take several minutes to receive the certificate due to scalability and lab network limitations.

Enter the Workspace

Your workspace is ready.

Enter

Once the workspace is ready, click Enter.
Verify Notepad++ Deployment

Now that you have published Notepad++ to your Windows 10 Devices and logged into the Workspace ONE catalog, let's review how to verify that your application was deployed successfully.

Confirm Deployment in the Workspace ONE Catalog

1. Ensure the Notepad++ app displays and shows as Installed.
2. If the Notepad++ app is not installed yet, you may need to wait a few minutes for it to complete. Click the Refresh button to reload the page as needed.

As an end user, you will have access to the Notepad++ application once it is installed. If you are able to see the Notepad++ application in the Catalog and the status displays as Installed, then the deployment was successful and our parameters for determining a successful install were correct.

INFO: The Notepad++ application began to install automatically because you set the App Delivery Method as Auto in the Workspace ONE UEM Console. If you had applications that you did not want to deploy automatically that users could download when needed, you could set the App Delivery Method to On Demand and allow end users to initiate the Notepad++ download from the Workspace ONE catalog.
Confirm Application Installed

1. Click the **Windows** button.
2. Confirm Notepad++ displays in the **Recently Added** section, confirming the install.

Deployment Details and Troubleshooting

In most cases, a successfully deployment is easily verified by inspecting if the app was installed or deployed to your device through either the Workspace ONE Catalog or by inspecting files that you are expecting to install. Continue through this section to see how you can inspect other details for further troubleshooting and for additional details on Software Distribution on Windows 10.
Inspecting Application Details

You can view additional details about the application, the deployment status, and potential errors in the Workspace ONE UEM Console. You can also find the Build Version here, which we will cover shortly to demo how to check the AppDeploymentCache and Registry on your devices for further debugging.

In the Workspace ONE UEM Console,

1. Click **Apps & Books**.
2. Click **Notepad++**.
Additional Information and Troubleshooting in the Workspace ONE UEM Console

1. Click the **Devices** tab.
2. Check the **Install Status** of the application. Note that ours already shows as **Installed**. If an install was pending or had failed, this would be reflected here.
3. Click the link to the enrolled device.
Inspecting Device Apps

In addition to our previous method, we can also check the status through the Device Details View.

1. Click the Apps tab.
2. Scroll through the list and find the Notepad++ application. Notice that our shows as installed, and other statuses would be reflected here as well.
Navigate to the Device Troubleshooting Section

1. Click the **More** tab dropdown.
2. Click **Troubleshooting**.
View the Event Logs for Application Events

1. Click **Event Log**.
2. Enter **Application** into the search and press enter. Since we may have several records to search through, we want to inspect only those pertaining to our Application events.
3. You may need to scroll to the right to view the Event Data column.
4. Notice the **Event Data** column associated with each Event. You can click any of these links to retrieve additional details about the event, inspecting potential issues and errors for why the deployment failed.

Feel free to inspect the Event Data links as desired, then continue to the next step.
Obtaining the Application Build Version

The Application Build Version is used to find your application details within the Registry and AppDeploymentCache. Before investigating those areas, we will first obtain the Build Version from the Workspace ONE UEM Console.

In the Workspace ONE UEM Console,

1. Click Apps & Books.
2. Click Notepad++.
Note the Build Version for the Notepad++ Application

1. Click the Details tab.
2. Note the Build Version value for this application.

In the following steps, we will check the Registry and App Deployment Cache on the Windows 10 device for additional troubleshooting. In our lab, we've only deployed one application so finding the correct folder will be easy. However, in a production environment, there could be multiple applications being deployed and the folder names will match the Build Version found above, so it is important to know where to retrieve this to debug the correct application deployment.
Inspecting the AppDeploymentCache

1. Click the File Explorer icon from the task bar.
2. Enter %programdata%\AirWatchMDM\AppDeploymentCache into the search bar and press enter.
Obtain Access to the AppDeploymentCache folder

Click **Continue**.

Open the Notepad++ Folder (Noted by Build Version)

Double-click the folder in the AppDeploymentCache. Note that the name matches the Build Version we previewed in the Workspace ONE UEM Console for the Notepad++ application previously.

In a production scenario, you could have multiple application caches here, each notated by their own Build Version. Retrieving this value from the Workspace ONE UEM Console to find the correct cache is an important step in debugging the correct deployment.
Obtain Access to the Application Cache Folder

Click **Continue**.

Inspect App Deployment Cache for Notepad++

1. Notice that our only file for this deployment is the Notepad++ Installer.exe, which we uploaded to the Workspace ONE UEM Console in our previous steps. If we had uploaded a .zip containing multiple files, those would be displayed here.
NOTE - This app cache allows you to confirm if the application contents are reaching the device, and if so, what their file names are.

2. Notice that the deployed filename matches our Install Command under Deployment Options > How To Install when we setup the application in the AirWatch Console.

NOTE - If your application is not installing, it is useful to compare the deployed contents and ensure your Install Command is setup correctly to reference the correct filenames and paths.

Inspecting the AppDeploymentAgent Registry Entries

You can also inspect the Registry for additional information on the deployment. To get started, we need to launch regedit.
1. Click the **Windows Start** button.
2. Enter `regedit`.
3. Click the `regedit` result.

**Allow Access to RegEdit**

Click **Yes** to allow User Account Control to **Registry Editor**.

**Inspect the AppDeploymentAgent Contents**
1. Expand Computer.
2. Expand HKEY_LOCAL_MACHINE.
3. Expand SOFTWARE.
4. Expand AirWatchMDM.
5. Expand AppDeploymentAgent.
6. Inspect the contents of the AppManifests, ContentManifests, Queue and S-1-#### sections.

Notice that the folder name matches the Build Version of our Notepad++ application, same as the AppDeploymentCache.

- **AppManifests** contains information about the options set in the Workspace ONE UEM Console from the Deployment Options tab of your application.
- **ContentManifests** contains information about the options set in the Workspace ONE UEM Console from the Files tab of your application.
- **Queue** will contain information the applications that are currently pending installation. In our example, the Notepad++ application has finished and so it’s entry is no longer available in the Queue. As files complete or error and the install stops, they will be moved to the S-1-#### section.
- **S-1-####** will contain information about the install process for applications that completed successfully or with errors. In our example, the Notepad++ application has finished and has moved to this section.

There can be two S-1-#### entries under AppDeploymentAgent. The names of these entries refer to the SID (Security Identifier), which will be based on the Install Context we configured when deploying the application previously in the AirWatch Console.

- **S-1-5-18** contains applications pushed to the Device Install Context, and refers to the service account that is used by the operating system.
- **S-1-5-21-####** contains applications pushed to the User Install Context, and refers to the SID (Security Identifier) of the user account.

Application Status Codes

1. Click the entry under **S-1-####**.
2. Inspect the **LastDeploymentLog** entry.
3. Inspect the **LastStatusCode** entry.

The Queue and S-1-#### entries will contain the **LastStatusCode** and **LastDeploymentLog** entries you can inspect to see additional details about the process and discern why the install finished or failed. When evaluating the logs (LastDeploymentLogs) provided in these entries, it is important to also reference the Status Codes (LastStatusCode) to help determine what occurred and why.

For reference, a list of Status Codes are included below:

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPLOYMENT_OPERATION_QUEUED</td>
<td>0x000</td>
</tr>
<tr>
<td>FIRST_DETECTION_INPROGRESS</td>
<td>0x100</td>
</tr>
<tr>
<td>FIRST_DETECTION_FAILED</td>
<td></td>
</tr>
<tr>
<td>FIRST_DETECTION_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>CHECK_REFERENCE_COUNT_INPROGRESS</td>
<td>0x200</td>
</tr>
<tr>
<td>CHECK_REFERENCE_COUNT_FAILED</td>
<td></td>
</tr>
<tr>
<td>CHECK_REFERENCE_COUNT_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>REQUIREMENTS_EVALUATION_INPROGRESS</td>
<td>0x300</td>
</tr>
<tr>
<td>REQUIREMENTS_EVALUATION_FAILED</td>
<td></td>
</tr>
<tr>
<td>REQUIREMENTS_EVALUATION_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>DEPENDENCIES_INPROGRESS</td>
<td>0x400</td>
</tr>
<tr>
<td>DEPENDENCIES_FAILED</td>
<td></td>
</tr>
<tr>
<td>Status Description</td>
<td>Code</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>DEPENDENCIES_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>SANITIZE_CACHE_INPROGRESS</td>
<td>0x500</td>
</tr>
<tr>
<td>SANITIZE_CACHE_FAILED</td>
<td></td>
</tr>
<tr>
<td>SANITIZE_CACHE_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>PENDING_NETWORK_CONNECTIVITY</td>
<td>0x600</td>
</tr>
<tr>
<td>DOWNLOAD_CONTENT_INPROGRESS</td>
<td></td>
</tr>
<tr>
<td>PENDING_DOWNLOAD_RETRY</td>
<td></td>
</tr>
<tr>
<td>DOWNLOAD_CONTENT_FAILED</td>
<td></td>
</tr>
<tr>
<td>DOWNLOAD_CONTENT_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>TRANSFORM_CACHE_INPROGRESS</td>
<td>0x700</td>
</tr>
<tr>
<td>TRANSFORM_CACHE_FAILED</td>
<td></td>
</tr>
<tr>
<td>TRANSFORM_CACHE_SUCCESSFUL</td>
<td></td>
</tr>
<tr>
<td>PENDING_USER_SESSION</td>
<td>0x800</td>
</tr>
<tr>
<td>EXEC_DEPLOYMENT_INPROGRESS</td>
<td>0x801</td>
</tr>
<tr>
<td>PENDING_EXEC_DEPLOYMENT_RETRY</td>
<td>0x802</td>
</tr>
<tr>
<td>EXEC_DEPLOYMENT_FAILED</td>
<td>0x803</td>
</tr>
<tr>
<td>EXEC_DEPLOYMENT_SUCCESSFUL</td>
<td>0x804</td>
</tr>
<tr>
<td>PENDING_REBOOT</td>
<td>0x805</td>
</tr>
<tr>
<td>FINAL_DETECTION_INPROGRESS</td>
<td>0x900</td>
</tr>
<tr>
<td>FINAL_DETECTION_FAILED</td>
<td>0x901</td>
</tr>
<tr>
<td>FINAL_DETECTION_SUCCESSFUL</td>
<td>0x902</td>
</tr>
<tr>
<td>DEPLOYMENT_OPERATION_FAILED</td>
<td>0x40000000</td>
</tr>
<tr>
<td>DEPLOYMENT_OPERATION_SUCCEEDED</td>
<td>0x80000000</td>
</tr>
<tr>
<td>DEPLOYMENT_OPERATION_SUSPENDED</td>
<td>0xC0000000</td>
</tr>
</tbody>
</table>

**Conclusion**

There are several ways to debug a failed or erroneous Software Distribution deployment, as we have reviewed. The Workspace ONE UEM Console is a good first step for determining what is occurring, but digging into the AppDeploymentCache and AppDeploymentAgent registry files will assist in deeper troubleshooting to determine any issues.

With this knowledge in mind, we will move onto deploying Office 365. Continue to the next step.
Deploying Office 365 ProPlus

In this hands on lab, you will package Office 2016 with a configuration file for click-to-run delivery to remote and enterprise worker devices. You will configure and assign the application to smart groups with the flexible deployment feature.

We have provided you with all of the files needed to complete the steps; however, in your organization you will have a customized configuration file to embed with your Office installation.

Preparing the Office 365 ProPlus Files

Before we can upload the ProPlus app to the Workspace ONE UEM Console, we need to prepare and zip the files.

Package the Office 365 Files as a Zip

![Image of file preparation process]

1. Open Windows Explorer.
2. Navigate to the Documents folder.
3. Create a new folder named HOL.
4. Create a folder named configuration.
5. Right-click on the configuration folder and select Send to > Compressed (zipped) folder.
6. Name the compressed file as required.
1. Click the **File Explorer** icon from the task bar.
2. Click **Documents**.
3. Click **HOL**.
4. CTRL+Click to select both the `configuration.xml` and `setup.exe` files.
5. Right-click either of the selected files and hover over **Send to**.
6. Click **Compressed (zipped) folder**.

**Rename the Zipped Folder**

![Renaming zipped folder](image)

Rename the zipped folder to **Office365ProPlus**.

*NOTE - If you accidentally canceled the rename after the zipped folder was created, you can rename it by right-clicking the zipped folder and selecting **Rename from the list**.*
Inspect the Configuration.xml File (Optional)

1. Select **configuration.xml** and right-click the file.
2. Select **Edit**.

For this lab, we are using the default **configuration.xml** file that is provided with the Office 365 ProPlus deployment. Your organization, if it has deployed Office 365, will have a configuration.xml file already that contains organization specifics for install and licensing options. For your knowledge, know that the **configuration.xml** file contains organization specific details that the **setup.exe** process uses to configure the Office 365 installation for your users.

Feel free to explore the **configuration.xml** file before continuing.
3. Click the **Close (X)** button to exit Notepad.
Deploying Office 365 Pro Plus in Workspace ONE UEM

Now that you've zipped the setup.exe and configuration.xml files for your Office 365 deployment, the next step is to upload and deploy this application through the Workspace ONE UEM Console.

Add an Internal Application

Back in the Workspace ONE UEM Console,

1. Click **Apps & Books**.
2. Click **Add Application**.

Upload the Application File

Add Application

- Organization Group ID*
  - your.email@shown.here
- Application File*

Click **Upload**.
Choose the File to Upload

Click **Choose File**.
Choose the Office365ProPlus.zip File

1. Click Documents.
2. Click HOL.
3. Click to select the Office365ProPlus.zip file.
4. Click Open.
Save the Uploaded File

Click Save.

Continue after Saving the File

1. Select No for Is this a dependency app?
2. Click Continue.
Selecting Yes for marking a file as a dependency file associates a dependency to Win32 applications. Dependency files are libraries and frameworks that the app requires to function, such as Java, Silverlight, or .NET libraries.

**Configure the Details Information**

1. Ensure the Details tab is selected.
2. Enter **Office 365 Pro Plus** for the Name.
3. Select **64-bit** for the Supported Processor Architecture. The Windows 10 device we are using for this lab is 64-bit, but you should verify which processor architecture is relevant for your devices during your organization's deployments.
NOTE - When uploading MSI files all possible fields are automatically pre-populated with all of the metadata, however for ZIP packages you will have to generate a Name as well as some of the Deployment options.

Files App Information

1. Click the **Files** tab.
2. Here you can configure additional details and requirements about your application.
   - **App Dependencies:** This is where you would select dependency files and enable the system to apply dependencies.
   - **App Transforms:** Allows you to apply MSI Transform (MST) files.
   - **App Patches:** Allows you to apply MSI Patch (MSP) files.

Continue to the next step.
Configure the App Uninstall Process

1. Scroll down to find the **App Uninstall Process** section.
2. Select **Input** for the **Custom Script Type**.
3. Enter `setup.exe /uninstall ProPlus` into the **Uninstall Command**
Configure the When to Install Details

1. Click the **Deployment Options** tab.
   The When To Install section allows to configure details about what requirements must be met in order to install the application.

2. Enter **3** for the **Disk Space Required** which specifies the amount of disk space the device must have available to install the application.

3. Select **GB** for the **Units** of the Disk Space Required.

4. Enter **50** for the **Device Power Required** which specifies the battery power, in percentage, that the device must have to install the application.

5. Enter **500** for the **RAM Required** which specifies the amount of RAM the device must have to install the application.

6. Enter **MB** for the **Units** of the RAM Required.
Configure the Deployment Options

1. Scroll down to find the **How To Install** section.
2. Enter `setup.exe /configure configuration.xml` for the **Install Command**
1. Scroll down further to find the Retry and Installer fields described below.
2. Enter 3 for the **Retry Count**, which specifies the number of times the system attempts to install the application after an unsuccessful attempt.
3. Enter 5 for the **Retry Interval**, which specifies the time (in minutes) the system waits when it tries to install the application after an unsuccessful attempt.
4. Enter 30 for the **Install Timeout**, which specifies the time (in minutes) the system allows the installation process to run without success.
5. Enter 1614 for the **Installer Reboot Exit Code**, which specifies the code the installer outputs to identify a reboot action.
6. Enter 0 for the **Installer Success Exit Code**, which specifies the code the installer outputs to identify a successful installation.
NOTE - The Installer Reboot Exit Code is not guaranteed to be 1614 for every application, but this is the usual default value that is commonly used. You should verify this code for any application you decide to deploy to verify it is correct.

Configure the When To Call Install Complete Section

1. Scroll down to the When To Call Install Complete section.
2. Select Defining Criteria for Identify Application By.
3. Click + Add.
1. Select **Registry Exists** for the **Criteria Type**.
2. Enter `HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\0365ProPlusRetail - en-us` for the **Path**.
3. Enter **DisplayName** for the **Value Name**.
4. Select **String** for the **Value Type**.
5. Enter `Microsoft Office Professional Plus 2016` for the **Value Data**.
6. Click **Add**.

**NOTE - There are multiple Criteria Types to choose from, allowing you to be flexible in determining if your deployment was successful. You can also add multiple Criteria configurations and link them together logically to cover complex deployments.**
1. Click the **Images** tab.
2. Click the **Icon** tab.
3. Click the area labeled **Click or drag files here**.

---

**Configure Images**

"Edit Application - Office365ProPlus.zip v 1.0.0"

- Internal | Managed By: your.email@shown.here | Application ID: (7bfc8e75-477-44c6-9d9...)

<table>
<thead>
<tr>
<th>Details</th>
<th>Files</th>
<th>Deployment Options</th>
<th>Images</th>
<th>Terms of Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Images</td>
<td>Tablet Images</td>
<td>Icon</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Click or drag files here
Select the O365 Logo for the Icon

1. Click **Documents**.
2. Click **HOL**.
3. Click the **o365-logo.jpg** file to select it.
4. Click **Open**.
View the Terms of Use and Assign

1. Click the **Terms of Use** tab.
2. If you decide to have a Terms of Use that your users must accept before installing applications, you can configure that here. For the purposes of this lab, we will leave this as **None**.
3. Click **Save & Assign**.
Add Assignments

Office 365 Pro Plus - Update Assignment

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Exclusions</th>
</tr>
</thead>
</table>

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive per highest priority (0 being highest priority).

Click + Add Assignment.
Configure the Application Assignment

1. Select **All Devices (your.email@shown.here)** for the Assignment Groups.
2. Select **Auto** for App Delivery Method.
3. Click **Add**.
Save and Publish

Office 365 Pro Plus - Update Assignment

Assignments

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>App Delivery Method</th>
<th>Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Devices</td>
<td>0</td>
<td>Auto</td>
<td>Now</td>
</tr>
</tbody>
</table>

Click **Save & Publish**.
Click Publish.
Confirm the Office 365 ProPlus Application Was Added

Back at the Internal Applications List View, confirm that the Office 365 Pro Plus application is displayed.

You have successfully added the Office 365 ProPlus app to Workspace ONE UEM for deployment. Remember that Workspace ONE UEM supports uploading and deploying MSIs, EXEs, as well as packaged apps like the zipped file we uploaded in this lab.

**Workshop ONE UEM Tip** - When deploying numerous apps to end-user devices, it can take some time to install all the device applications. After device on-boarding completes, apps queue up in a random order for the device to install per Windows operating system specifications, configured timeout values, and retry logic. Dependency files are installed prior to the main application.
Verifying Office 365 Pro Plus Deployment

Due to the scalability of this lab, time constraints, and the size of the install size, the Office 365 Pro Plus installer WILL NOT complete on your Windows 10 device before the lab session expires. This section will guide you through verifying that the install command was completed and how you can verify your software distribution process for scenarios outside of this lab.

Verify App Availability in Workspace ONE

You can confirm that the Office 365 Pro Plus application was assigned to your device and is installing within the Workspace ONE application.
View the Office 365 ProPlus app in the Catalog

1. Click the **Workspace ONE App** icon from the task bar.
2. Click **Refresh** icon
3. Notice that the **Office 365 ProPlus** application you configured within Workspace ONE UEM displays as **Installing**.

Because our Office 365 ProPlus app was deployed as Auto install, the application is already installing on our device. On Demand apps would also display here in the catalog, and users would need to manually begin the installation process from this view if they desired to download those apps.
NOTE - If you don't see the Office 365 Pro Plus application, you may need to wait several minutes and try refreshing the Catalog by closing the Workspace ONE application and re-opening it.

NOTE - The "Installing" status will update appropriately once the installation is finished. Due to limited network resources and limited lab time, we suggest continuing to the next steps to see how else you could verify and troubleshoot app deployments.

Verify Install Command Was Sent

You can retrieve details about the current install status of an application on the assigned devices. This can be used to monitor if devices are installing the application appropriately.

Navigate to the Details View of the Internal Application

Back in the Workspace ONE UEM Console,

1. Click **Apps & Books**
2. Click the **Office 365 Pro Plus** application you deployed.
1. Notice that the Install Status is currently showing **Not Installed** for 1 device. This verifies that 1 device is currently assigned to receive the application and the application is still reporting as Not Installed.

2. You can also verify your **Deployment Progress** to ensure that the number of devices receiving this application is correct and that your Deployment Mode (Auto or On Demand) is correct.
1. Click the **Devices** tab. This will show the current list of Devices that are assigned to receive this application.

2. Notice that our enrolled Windows 10 Device is marked as Not Installed, but the Reason is listed as **Install Command Dispatched**. Since we are installing a few GB over a network with limited resources, this is expected as the install can take some time.

**NOTE** - Once the Install Command is processed, the Install Status and Reason fields will update to show either that the install was successful or that there were errors.

**Using Device Details to Track Applications & Troubleshooting**

In addition to the applications details view, you can view Apps information and Troubleshooting logs, which can aid in tracking application deployments and debugging why deployments may fail.
Navigate to the Device Details View

Click your **Device Name** from the Devices view.
1. Click the Apps tab.
2. Scroll down until you see the **Office 365 Pro Plus** app in the list.
3. Here you can see a list of applications that are installed on the device and additional information about each of them. Successful, pending, and failed installations will all appear here. You can see here that the **Office 365 Pro Plus** application is pending due to the grey checkmark.
1. Click the **More** dropdown.
2. Click **Troubleshooting**.
View Device Events

1. Ensure the Event Log tab is selected. Under Event Log, you can view the full list of events sent to the device. You can use this information to verify that the Install Command was received, and details around why the install succeeded or failed.

2. Enter Application in the search box.

3. Scroll to the right.

4. Find the Install Application Requested action for the Office 365 Pro Plus application to verify that the device received the command. You may need to scroll to the right to find the necessary columns, which are:

   • Event: Install Application Confirmed
   • Event Data: Application: Office 365 Pro Plus

Verify Install Was Completed (follow along)

The following steps are for instructional purposes only, as the Office 365 Pro Plus installer WILL NOT complete before the lab expires due to limited network resources and lab! Please follow along to see how you can verify that software distribution installs are completed and successful.

**NOTE** - As mentioned before, the Office 365 Pro Plus install will likely not complete before your lab expires due to limited network resources and the lab time limit! This section will demonstrate what a successful install would look like in the Workspace ONE UEM Console in a real deployment.
Navigate to the Details View of the Internal Application (follow along)

1. Click **Apps & Books**.
2. Click the **Office 365 Pro Plus** application you deployed.

**NOTE** - As mentioned before, the Office 365 Pro Plus installment will likely not complete before your lab expires due to limited network resources and the lab time limit! This section will demonstrate what a successful install would look like in the Workspace ONE UEM Console in a real deployment.
Notice that the Install Status now shows **Installed** for the Windows 10 device.

**NOTE - As mentioned before, the Office 365 Pro Plus installment will likely not complete before your lab expires due to limited network resources and the lab time limit! This section will demonstrate what a successful install would look like in the Workspace ONE UEM Console in a real deployment.**
Notice that the **Install Status** has been updated to show **Installed**, and that the **Reason** is listed as **Managed**.

*NOTE - As mentioned before, the Office 365 Pro Plus installment will likely not complete before your lab expires due to limited network resources and the lab time limit! This section will demonstrate what a successful install would look like in the Workspace ONE UEM Console in a real deployment.*
Verify Installation on the Windows 10 Device (follow along)

1. Click the Windows button.
2. Once the install completes, you will notice that the Recently Added section now displays the Office 2016 suite.

NOTE - As mentioned before, the Office 365 Pro Plus installment will likely not complete before your lab expires due to limited network resources and the lab time limit! This section will demonstrate what a successful install would look like in the Workspace ONE UEM Console in a real deployment.
Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from Workspace ONE UEM console, also known as managed content.

Delete Device from Workspace ONE UEM Console

From the Workspace ONE UEM Console,

1. Click on Devices
2. Click on List View
3. Select the check box next to your device friendly name.
4. Click on More Actions
5. Click on Delete Device
Enter Reason and Delete

Delete Device

1. Enter the reason as **lab completed**.
2. Click on **Delete**.
Validate DELETE IN PROGRESS...

List View

1. You may see device friendly name changing to DELETE IN PROGRESS...
2. Click on the Refresh Icon to validate if the device deletion is successful.

Ensure that device record is deleted

List View

1. Use the Refresh Button if needed.
2. Ensure that the device record is now deleted from the Workspace ONE UEM console and you see the message No Records Found.
Navigate to Windows 10 Settings

1. Click on the **Windows Icon**
2. Click on the gear icon to access **Windows 10 Settings**

Access Accounts Settings

From the Settings Menu, access **Accounts**
Validate That No Management Account Exists

1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to **AirWatchMDM**.

**NOTE** - The CORP AD domain is the local domain in this lab and is not controlled by AirWatch Enrollment, so you will see this connection if your device is enrolled or unenrolled.
Sign Out of the Workspace ONE Application

1. Click the Workspace ONE App icon from the task bar.
2. Click the User icon.
3. Click Sign Out.
Confirm Sign Out

Click **Sign Out**

Close the Workspace ONE App

Click the **Close** button.
Close Chrome to Clear Session Cookies

1. Return to your Chrome browser.
2. Click the Close (X) button.

Workspace ONE saves your OAuth session details in cookies. Closing your browser ensures your previous session cookies will be deleted and won't interfere with any additional modules you take.
Conclusion

Software Distribution in AirWatch allows you to deliver Windows applications and adhere to the application life-cycle. Software Distribution enables your organization to deploy applications, track the installation statuses, debug and troubleshoot installation issues, and maintain applications with ease.
Module 3 - Windows 10
Real-Time and Automated Security Protection and Compliance
Introduction

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 Unified Endpoint Management’s (UEM) capabilities, you can fold the Windows 10 functionality into an existing VMware AirWatch management solution. Combining traditional client requirements with modern enterprise management capabilities creates a simplified, cost-effective management solution. Use Workspace ONE UEM to establish user trust, assess the device posture, enforce conditional access, and enable data loss prevention.

In this hands on lab, we will explore how to configure many of the end-to-end security features, however, due to using VMs we will not be able to fully test all of our security configurations.

*NOTE - You may need to scroll to the right to view the full screen button on the video above.*
Connect to Windows 10 VM

We have provided you a Windows 10 VM to complete the necessary steps for this lab. Let's connect to it to complete the steps in the following section.

Connect to the Windows 10 VM

Double-click the Win10-01a.rdp shortcut on the lab desktop.

If prompted, the login credentials for the Windows 10 VM are:

- Username: corp\holuser
- Password: VMware1!
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your **Username**. This is your **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

What was your childhood nickname?  

Password Recovery Answer *

VMware1!  

Confirm Password Recovery Answer *

VMware1!

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

1234

Confirm Security PIN *

1234

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter **VMware1!** in the Password Recovery Answer field.
4. Enter **VMware1!** in the Confirm Password Recovery Answer field.
5. Enter **1234** in the Security PIN field.
6. Enter **1234** in the Confirm Security PIN field.
7. Click the **Save** button when finished.

**Close the Welcome Message**

**Workspace ONE UEM Console Highlights**

**Powered by VMware AirWatch!**

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE

[Don't show this message on login]
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Device Posture and Real-Time Compliance

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.

Navigate to All Settings
1. Click **Groups & Settings**.
2. Click **All Settings**.

### Navigate to Windows Health Attestation

1. Click **Devices & Users**
2. Click **Windows**
3. Click **Windows Desktop**
4. Click **Windows Health Attestation**
5. Select **Override** for the Current Setting
6. Uncheck **BitLocker Disabled** under the Compromised Status Definition section.
Configure Health Attestation

1. Scroll down to the bottom of the page.
2. Click **Save**
Close Settings

1. Ensure the **Saved Successfully** prompt is displayed.
2. Click the **Close (X)** button to close the Setting window.
Conditional Access

For this lab we will be using the VMware Workspace ONE app to demonstrate the conditional access and Single Sign-On functions instead of a public 3rd party application such as the native SalesForce app.

Introduction

Conditional access to corporate resources through Workspace ONE combines Workspace ONE UEM (VMware AirWatch) management capabilities with VMware Identity Manager™. Available across all platforms and device types, conditional access provides the intelligence necessary for comprehensive unified endpoint management. While Workspace ONE UEM automatically denies access to unmanaged devices, conditional access enables a more nuanced approach by allowing managed devices to access corporate resources if they report a healthy compliance status.

For this lab several items such as Identity Manager integration and Certificate Profiles have been pre-configured for your Organization Group.
View Conditional Access Flow

We will now launch the Workspace ONE App to see how our access is affected when logging in from a device that is not enrolled.

Launch the Workspace ONE App

1. Click the Windows button.
2. Click the Workspace ONE app icon from the start menu.
Enter the Workspace ONE Server Address (IF NEEDED)

1. Enter **https://cn1193-2057-ws1win.vidmpreview.com** for the Server Address field.
2. Click **Continue**.
Enter Your Username for Workspace ONE

1. Enter **aduser** for the username.
2. Click **Next**.
Confirm Authentication Failure

The environment has been configured to use certificate authentication into the application. The certificate is installed on the device only after the device has been enrolled into Workspace ONE UEM thus preventing any unauthorized users from accessing the application's information.
Close the Workspace ONE application by clicking on the **Close (X)** in the upper right corner.
Modifying Internet Options for Windows Enrollment

Before enrolling the Windows 10 Virtual Machine, we will make modifications to the Windows 10 device to reduce network traffic to expedite enrollment.

Open Settings

1. Click the Windows button.
2. Click the Settings (Gear) icon.
Open Internet Options

1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.
Modify the Certificate Revocation Options

1. Click the **Advanced** tab.
2. Scroll down to find the **Security** section.
3. **Uncheck** the **Check for publisher's certificate revocation** option.
4. **Uncheck** the **Check for server certificate revocation** option.
5. Click **Apply**.
6. Click **OK**.
Open PowerShell as Administrator

1. Right-Click the Windows button.
2. Click Windows PowerShell (Admin).
Allow WindowsPowerShell to Make Changes

Click **Yes** when prompted to allow Windows PowerShell to make changes to your device.

**Enter Commands to Stop Windows Update Service**

Enter the following commands (remember that you can highlight then drag-and-drop the text from the manual into PowerShell!)

1. Enter `Set-Service wuauserv -startup disabled` then press **ENTER**.
2. Enter `Stop-Service wuauserv` then press **ENTER**.
3. Click the **Close** button to exit PowerShell.
Enrolling Your Windows 10 Device

We will now enroll our Windows 10 device in Workspace ONE UEM. First, we will need to download the Workspace ONE Intelligent Hub.

Download the Workspace ONE Intelligent Hub on the Windows 10 VM

From a new tab in the browser, if not opened already,

1. Enter [https://www.getwsone.com](https://www.getwsone.com) in the navigation bar and press Enter.
2. Click **Download Hub for Windows 10**.  
   **NOTE:** Please wait while the Workspace ONE Intelligent Hub installer finishes downloading.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

**NOTE - If you do not see the warning about the AirWatchAgent.msi file, skip this and continue to the next step.**

### Launch the Workspace ONE Intelligent Hub Installer

![Image of AirWatchAgent.msi file]

Click the **AirWatchAgent.msi** file in your download bar.

**NOTE - The installer may take a few seconds to launch, please be patient after clicking the AirWatchAgent.msi file.**

### Click Run

![Image of Open File - Security Warning]

Click **Run** to proceed with the installation.
Accept the Default Install Location

Leave the default install location and click **Next**.

**NOTE** - *The Next button may take several seconds to enable while the required additional features are installed.*
Accept the License Agreement

1. Select **I accept the terms of the license agreement**.
2. Click **Next**.
Start the Workspace ONE Intelligent Hub Install

Click **Install** to start the installer.
Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

If prompted to allow the app to make changes on your device, click **Yes**.
Complete the Workspace ONE Intelligent Hub Installer

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

**NOTE - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.**
Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

Click **Server Detail**.

**Find your Group ID from Workspace ONE UEM Console**
The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**Enter the Server Details**

1. Enter `labs.awmdm.com` for the **Server Name** field.
2. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
Enter Your User Credentials

1. Enter aduser in the Username field.
2. Enter VMware1! in the Password field.
3. Click Next

*NOTE - Wait while the server checks your enrollment details.*
Since our Workspace ONE UEM and VMware Identity Manager environments are linked for this environment, the Workspace ONE Application will automatically open after enrollment is complete. You will not need it for this exercise, so click **Close**.
Finish the Workspace ONE UEM Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM.
Confirm the aduser Certificate Has Installed

We have configured few device profiles for you to automatically install the user certificate you will need for this lab. In this section, we are going to validate if that user certificate is installed on your Windows 10 device or not before proceeding.

Check the Device Details for the Certificate Profile Status

In the Workspace ONE UEM Console,

1. Click Devices
2. Click List View
3. Click the device link for the enrolled device.
Install the Win10 - User Cert Profile (IF NEEDED)

1. Click the Profiles tab.
2. Mouse over the status of the Win10 - User Cert profile.
   - If the status shows as Install Failed, follow the below steps to install it.
   - If the status shows as Pending Information, refresh the page and re-check the status.
   - If the status is a green checkmark, continue to the Check the aduser Certificate on the Windows 10 Device step.
3. Select the Win10 - User Cert
4. Click Install.

Confirm the Install Action (IF NEEDED)

Click OK to confirm the Install action.
Ensure the Win10 - User Cert Profile Installs (IF NEEDED)

If you needed to install the Win10 - User Cert profile, follow these steps. Otherwise, continue to the next step.

1. Click **Refresh**.
2. Check the status of the **Win10 - User Cert profile**, it should update about every 1-2 minutes. If the Status is not a green checkmark, refresh until the install completes.

**NOTE - Mouse over the icon in the Status column to see the current status. If you see the Yellow Warning sign respond with “Install Failed”, select the Win10 - User Cert and click Install again to restart the install process.**
Check the aduser Certificate on the Windows 10 Device

1. Click the **Windows** button.
2. Type **user certificates** and the Search bar will populate.
3. Click the **Manage user certificates** option.
Allow the Microsoft Management Console to make changes

Click **Yes** when asked if you want to allow this app to make changes to your device.

Confirm the aduser Certificate Has Installed

1. Click the **Personal** folder to expand it.
2. Click the **Certificates** folder.
3. Check if the **aduser** certificate exists.
4. If the aduser certificate does NOT exist, wait a minute or two and click the Refresh button to check again. Continue to refresh until you see that the aduser certificate exists.

Do not continue to the next step until you've confirm that the aduser certificate has been installed.

NOTE - Due to lab scalability and limitations, the aduser certificate may take a few minutes to download from the CA.
Compliance with Workspace ONE

In this section, we are going to create a Compliance Policy and validate both the compliant and non-compliant states on our Windows 10 device to show how you can control access to apps and services by requiring devices to remain within compliance.

View Conditional Access Flow After Enrollment

Now that our Windows 10 device is enrolled, let's sign in to Workspace ONE again and see how the authentication flow has changed. We will validate that the Windows 10 device is able to login to the Workspace ONE app after enrollment but prior to adding in a Compliance Policy.
Login to the Workspace ONE Application

1. Click the Windows button.
2. Click the Workspace ONE app icon from the start menu.
Enter the Workspace ONE Server Address (IF NEEDED)

1. Enter **https://cn1193-2057-ws1win.vidmpreview.com** for the Server Address field.
2. Click **Continue**.
Enter Your Username for Workspace ONE

1. Enter \texttt{aduser} for the username.
2. Click \texttt{Next}.

Allow Access to Credentials

Click \texttt{Allow} to allow access to your private key.

\textit{NOTE - The user will only be prompted once for this permission.}
NOTE - If you receive the "Access Denied. Certificate login failure." screen, please wait a few minutes and try to login again. The device may take several minutes to receive the certificate due to scalability and lab network limitations.

Enter the Workspace

Your workspace is ready.

Enter

Once the workspace is ready, click Enter.
Confirm Successful Login to the Workspace ONE App

Upon successfully logging in, you will see the app catalog page of the Workspace ONE app. For this exercise, no applications have been assigned to your user, so you will not see any available applications.

Continue to the next step after confirming your login was successful.
1. Click the Workspace ONE App icon from the task bar.
2. Click the User icon.
3. Click Sign Out.
Confirm Sign Out

Click **Sign Out**

Close the Workspace ONE App

Click the **Close** button.
Create a Compliance Rule

We will now create another Compliance rule to cause our device to become non-compliant. This way, we can validate the flow in the scenario where device becomes non-compliant.

Add a Compliance Policy

Back to the Workspace ONE UEM console in Chrome,

1. Click Devices.
2. Click Compliance Policies.
3. Click List View.
4. Click Add.

No
Select Compliance Platform Type

Add Compliance Policy

Select a platform to start:

- Android
- iOS
- macOS
- Windows
- Windows Rugged

Click on the **Windows** icon.

**NOTE - Do NOT select Windows Rugged icon.**

Select Compliance Device Type

Select Device Type

Select a platform to start:

- Windows Phone
- Windows Desktop
- Windows 7
Click on the **Windows Desktop** icon.

**Select Encryption**

1. Click the **Rules** dropdown and select **Encryption**.
2. Select **is not encrypted**.
3. Click **Next**.

---

1. Click the **Rules** dropdown and select **Encryption**.
2. Select **is not encrypted**.
3. Click **Next**.
Configure Additional Compliance Action

1. Select Profile from the Actions dropdown.
2. Ensure Block/Remove All Profiles is selected.
3. Click Next.

This Action will remove all profiles from the device immediately upon becoming non-compliant. However, it will leave the device enrolled so that all of the Profiles will be re-installed when the device comes back into compliance.
Create Compliance Assignment

1. Select **All Devices (your.email@shown.here)** for the Assigned Groups.
2. Click **Next**.
Activate the Compliance Rule

Click **Finish & Activate**.

Confirm Device is Non-Compliant

With the new Compliance Policy in place, we will now confirm that our device is showing as non-compliant. Because our enrolled Windows 10 device is not encrypted, and our Compliance Policy requires devices to be encrypted, it will be marked as non-compliant once the policy applies.
Navigate to Device List View

1. Click Devices
2. Click List View
Confirm the Device Shows as Non-Compliant

1. You may need to scroll right to view the Compliance Status for your Windows 10 device.
2. Confirm the Windows 10 device shows Non-Compliant for your enrolled device. This may take a few minutes as the compliance check runs every 5 minutes.
3. If the device does not show Non-Compliant, click on the Refresh icon to refresh the page.

**NOTE - You may need to wait several minutes for the Compliance Check to complete since it runs every 5 minutes. Please continue to refresh every few minutes until you see the device marked as Non-Compliant before proceeding.**
Open the Microsoft Management Console

1. Click the **Windows** button.
2. Enter **user certificates** and the Search bar will populate.
3. Click the **Manage user certificates** option.
Allow the Microsoft Management Console to make changes

Click **Yes** when asked if you want to allow this app to make changes to your device.

**Confirm the aduser Certificate is Removed**

1. Click the **Personal** folder to expand it.
2. Click the **Certificates** folder.
3. Check if the **aduser** certificate still exists.
4. If the **aduser** certificate exists, wait a few minutes and click the **Refresh** button to check again. Continue to **refresh** until you see that the **aduser certificate is no longer shown**.

**Do not continue** to the next step until you've confirm that the **aduser certificate has been removed**.
NOTE - Due to lab scalability and limitations, the aduser certificate may take a few minutes to be removed.

Launch the Workspace ONE App

Now that our Windows 10 device is showing as non-compliant, let us return to the Workspace ONE app on the Windows 10 VM and see how the authentication flow has changed for our non-compliant device.

Launch the Workspace ONE App

1. Click the Windows button.
2. Click the Workspace ONE app icon from the start menu.
Enter the Workspace ONE Server Address (IF NEEDED)

Your Workspace ONE app may have already validated the workspace server URL. If you are prompted to enter a username rather than a workspace server URL, you can skip this step.

1. The server address [https://cn1193-2057-ws1win.vidmpreview.com](https://cn1193-2057-ws1win.vidmpreview.com) should already be set when launching the Workspace ONE app, enter the value in the Server Address field if it is not already set.
2. Click **Continue**.
Enter Your Username for Workspace ONE

1. Enter **aduser** for the username.
2. Click **Next**.
1. Confirm that authentication into the Workspace ONE app now fails.

The authentication fails because our encryption Compliance Policy was setup to remove all Profiles should the device become non-compliant. Since the Windows 10 device we are testing from is not encrypted, the device became non-compliant once the Compliance Check completed and so the Profile containing the certificate used to login to the Workspace ONE portal was revoked. Without the certificate, the user can no longer login to the Workspace ONE app.

2. Click the **Close** button to exit the Workspace ONE app.
Data Loss Prevention

Let's take a look at how Workspace ONE UEM can help with Data Loss Prevention with your Windows 10 devices. To limit the scope of this lab, we will be going through videos, rather than actual configurations.

Windows Information Protection (WIP), App Control, & Per-App VPN

Workspace ONE UEM can configure the Windows Information Protection, App Control, and Per-App VPN feature that is built into Windows 10. Please watch the video for a demonstration on configuration and it working on a device.

NOTE - You may need to scroll to the right to view the full screen button on the video above.

BitLocker Encryption

With Workspace ONE UEM you able to configure BitLocker settings, please watch the video for a demonstration on configuration and it working on a device.
NOTE - You may need to scroll to the right to view the full screen button on the video above.
Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from Workspace ONE UEM console, also known as managed content.

Delete Device from Workspace ONE UEM Console

From the Workspace ONE UEM Console,

1. Click on **Devices**
2. Click on **List View**
3. Select the check box next to your device friendly name.
4. Click on **More Actions**
5. Click on **Delete Device**
Enter Reason and Delete

Delete Device

You are about to delete 1 device. This action cannot be undone. To continue, please review the details below and click Delete.

1. Enter the reason as **lab completed**.
2. Click on **Delete**.
Validate DELETE IN PROGRESS...

1. You may see device friendly name changing to DELETE IN PROGRESS...
2. Click on the Refresh Icon to validate if the device deletion is successful.

Ensure that device record is deleted

1. Use the Refresh Button if needed.
2. Ensure that the device record is now deleted from the Workspace ONE UEM console and you see the message No Records Found.
Navigate to Windows 10 Settings

1. Click on the **Windows Icon**
2. Click on the gear icon to access **Windows 10 Settings**

Access Accounts Settings

From the Settings Menu, access **Accounts**
1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to **AirWatchMDM**.

**NOTE** - The CORP AD domain is the local domain in this lab and is not controlled by AirWatch Enrollment, so you will see this connection if your device is enrolled or unenrolled.
Remove the Compliance Policy

In the Workspace ONE UEM Console in Chrome,

1. Click **Devices**.
2. Expand **Compliance Policies**.
3. Click **List View**.
4. Find the **Encryption** Compliance Policy and click the **X** button to remove it.

Confirm the Compliance Policy Removal

Click **OK** to delete the Compliance Policy.
Close Chrome to Clear Session Cookies

1. Return to your Chrome browser.
2. Click the Close (X) button.

Workspace ONE saves your OAuth session details in cookies. Closing your browser ensures your previous session cookies will be deleted and won't interfere with the any additional modules you take.
Conclusion

In this hands on lab, we explored how to configure many of the end-to-end security features, however, due to using VMs we were not able to fully test all of our security configurations. Thus, below you will find an end-to-end demo of Windows 10 management using Workspace ONE UEM many of the same security features we configured.

NOTE - You may need to scroll to the right to view the full screen button on the video above.
Module 4 - Manage Windows 10 Policy with Workspace ONE
**Introduction**

In this module, you will learn about why you should start migrating from traditional policy management to modern management of policies.

You will do the following in this module:

- Learn about challenges with traditional policy management and why Windows 10 is different
- Learn about Configuration Service Providers (CSPs)
- Learn about the VMware Policy Builder tool
- Use the VMware Policy Builder tool to set CSPs on a Windows 10 device
Moving Policy to Modern Management

Windows 10 is essentially a mobile operating system and should be managed in a modern way. Users are no longer tethered to physical office locations with domain joined, always on corporate network systems. We need to be able to manage these systems over the air from anywhere, much like we do with our other mobile devices today. We will now review how Windows was managed traditionally, and how we can manage policy in a modern way with Configuration Service Providers (CSPs).

Traditional Policy Management

Traditional policy management methodologies are based on Domain Joined, corporate network tethered systems. This does not provide a lot of flexibility for the way that the mobile workforce operates today. Microsoft Policy management has been around for over 25 years and has the following management methodologies today:

**Group Policy (GPO)**

- Centrally managed domain based policies
- Over 4000 GPOs available, many very obscure
- Can lead to long log in times
- Can’t be easily retrieved unless logging in on corporate network
- Must be domain members to receive group policy

**Local Policy (LGPO)**

- Distributed GPO management for non-domain joined machines
- Can emulate GPO settings
- Difficult to control as there is no centralized management

Modern Policy Management

Windows 10 is essentially a mobile operating system and can be managed over the air in the same way as your other mobile devices are. It has interfaces that allow settings which affect the registry and file system to be pushed over the air. These
What is a CSP and why is it important?

Configuration Service Providers (CSP) are the interfaces used to read or set policies on the Windows device.

CSP capabilities have continued to grow with each release of the Windows 10 operating system. More capabilities can now be managed over the air using modern methods reducing the dependency on traditional methods like the requirement to log on to the domain network to get updated policies or the need to a desk at a branch location. Configuration on devices can be updated in real time ensuring security and compliance at all times.

How can I use a CSP?

The Workspace ONE UEM console allows admin to configure policies through Profiles. Those policies that are used often and across industries and provide easy configuration through the GUI. The admin can simply toggle switches or use the text fields to set up these policies. The Workspace ONE UEM console also provides a Custom Settings profile that is extensible to any custom xml that can be sent to the device leveraging the
existing infrastructure to securely communicate with the device. Admins can leverage the Custom Settings profile to configure any CSP and publish those settings to devices. The xml used to configure a CSP which the Open Mobile Alliance Device Management (OMA DM) client in the operating system can understand parse to apply the appropriate settings is called SyncML.
Policy Builder Overview

We will be using the VMware Policy Builder in this lab to set custom policy on a Windows 10 machine. Please read about the VMware Policy Builder and watch the video demo below to understand more about how the tool works and why you should use it.

VMware Policy Builder

The Policy Builder is an easy to use tool that will save time and effort throughout your journey to modernize management of Windows 10 devices.

- The Policy Builder reduces the complexity to hand rolling xml that is difficult and error-prone. Admins can use the easy form-based UI to generate or modify xml.
- The tool supports the configuration by operating system version reducing the chances of error if a specific node is not supported in the operating system version of the device receiving the xml.
- Support for configuring or modifying multiple CSPs at a time for your convenience.
- Policy Builder dynamically generates SyncML for nodes that you populate. Which makes it easy to edit as you go or delete whole nodes if they are no longer necessary. The corresponding block of SyncML is removed if a node has no value.
- The ability to generate GUIDs if needed to populate SyncML is included in the tool.
- An easy to use Filter helps avoid the need to scroll through the list to find the CSP required
- The tool is cloud-hosted and can be updated quickly and easily with new features and bug fixes greatly reducing turn around time.

Please watch the video demo below to understand more about the VMware Policy Builder
Why should I use Policy Builder?

The Policy Builder is an easy to use tool that will save time and effort throughout your journey to modernize management of Windows 10 devices.

- The Policy Builder reduces the complexity to hand rolling xml that is difficult and error-prone. Admins can use the easy form-based UI to generate or modify xml.
- The tool supports the configuration by operating system version reducing the chances of error if a specific node is not supported in the operating system version of the device receiving the xml.
- Support for configuring or modifying multiple CSPs at a time for your convenience.
- Policy Builder dynamically generates SyncML for nodes that you populate. Which makes it easy to edit as you go or delete whole nodes if they are no longer necessary. The corresponding block of SyncML is removed if a node has no value.
- The ability to generate GUIDs if needed to populate SyncML is included in the tool.
- An easy to use Filter helps avoid the need to scroll through the list to find the CSP required.
- The tool is cloud-hosted and can be updated quickly and easily with new features and bug fixes greatly reducing turn around time.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your Username. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter VMware1! for the Password field.
3. Click the Login button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *
What was your childhood nick?  

Password Recovery Answer *
VMware!

Confirm Password Recovery Answer *
VMware!

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *
1234

Confirm Security PIN *
1234

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE

Don't show this message on login
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Connect to the Windows 10 VM

We have provided you a Windows 10 VM to complete necessary steps for this lab.

Connect to the Windows 10 VM

Double-click the Win10-01a.rdp shortcut on the lab desktop.

If prompted, the login credentials for the Windows 10 VM are:

- Username: corp\holuser
- Password: VMware1!
Modifying Internet Options for Windows Enrollment

Before enrolling the Windows 10 Virtual Machine, we will make modifications to the Windows 10 device to reduce network traffic to expedite enrollment.

Open Settings

1. Click the Windows button.
2. Click the Settings (Gear) icon.
Open Internet Options

1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.
Modify the Certificate Revocation Options

1. Click the Advanced tab.
2. Scroll down to find the Security section.
3. Uncheck the Check for publisher's certificate revocation option.
4. Uncheck the Check for server certificate revocation option.
5. Click Apply.
6. Click OK.
Open PowerShell as Administrator

1. Right-Click the Windows button.
2. Click Windows PowerShell (Admin).
Allow Windows PowerShell to Make Changes

Click Yes when prompted to allow Windows PowerShell to make changes to your device.

Enter Commands to Stop Windows Update Service

Enter the following commands (remember that you can highlight then drag-and-drop the text from the manual into PowerShell!)

1. Enter `Set-Service wuauserv -startup disabled` then press ENTER.
2. Enter `Stop-Service wuauserv` then press ENTER.
3. Click the Close button to exit PowerShell.
Enrolling Your Windows 10 Device

We will now enroll our Windows 10 device in Workspace ONE UEM. First, we will need to download the Workspace ONE Intelligent Hub.

Download the Workspace ONE Intelligent Hub on the Windows 10 VM

From a new tab in the browser, if not opened already,

2. Click **Download Hub for Windows 10**.  
   **NOTE:** Please wait while the Workspace ONE Intelligent Hub installer finishes downloading.

3. Click **Keep** when warned about the AirWatchAgent.msi download.

   **NOTE - If you do not see the warning about the AirWatchAgent.msi file, skip this and continue to the next step.**

**Launch the Workspace ONE Intelligent Hub Installer**

Click the **AirWatchAgent.msi** file in your download bar.

**NOTE - The installer may take a few seconds to launch, please be patient after clicking the AirWatchAgent.msi file.**

**Click Run**

Click **Run** to proceed with the installation.
Accept the Default Install Location

Leave the default install location and click **Next**.

*NOTE - The Next button may take several seconds to enable while the required additional features are installed.*
Accept the License Agreement

1. Select **I accept the terms of the license agreement**.
2. Click **Next**.
Start the Workspace ONE Intelligent Hub Install

Click **Install** to start the installer.
Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

If prompted to allow the app to make changes to your device, click Yes.
Complete the Workspace ONE Intelligent Hub Installer

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

**NOTE - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.**
Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

Click **Server Detail**.

**Find your Group ID from Workspace ONE UEM Console**
The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.  
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**Enter the Server Details**

1. Enter **labs.awmdm.com** for the **Server Name** field.  
2. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
Enter Your User Credentials

1. Enter `aduser` in the **Username** field.
2. Enter `VMware1!` in the **Password** field.
3. Click **Next**

**NOTE - Wait while the server checks your enrollment details.**
Workspace ONE Application Launch

Since our Workspace ONE UEM and VMware Identity Manager environments are linked for this environment, the Workspace ONE Application will automatically open after enrollment is complete. You will not need it for this exercise, so click Close.
Finish the Workspace ONE UEM Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM.
Return to the Main Console

Click the Close (X) button to return to the Main Console to complete the upcoming steps.
Review the Enrolled Device

Back in the Workspace ONE UEM Console,

1. Click on **Devices**.
2. Click **List View**.
3. Confirm that the recently enrolled Windows 10 device is present.
Review the VMware Policy Builder

We will now open and review the VMware Policy Builder.

Open the link to VMware Policy Builder

On the desktop of the Main Console, double-click the Policy Builder shortcut to open the VMware Policy Builder

Sign up for a My VMware Account (Optional)

If you already have a My VMware account, please skip ahead to the Log into the VMware Policy Builder step.

If you currently don't have a My VMware account, you will need to sign up for one in order to access the Policy Builder.

You need to sign in with a My VMware account in order to access the Policy Builder!

If you don't currently have a My VMware account, follow the next steps to sign up for one. https://my.vmware.com/web/vmware/registration

If you believe you have a VMware account, but you are not sure of the password, go to the following link to reset your password: https://my.vmware.com/web/vmware/forgot-password

Both of these options will be detailed in following optional steps.
Click the Sign up for an account link or go to https://my.vmware.com/web/vmware/registration

Register for My VMware Account

Enter the following required information:

1. Email Address you want to use - you will need access to this email address during the lab to retrieve the activation code
2. Verify the Email Address
3. Enter a Password with at least 6 characters
4. Verify the Password
5. Enter your First Name
6. Enter your Last Name
7. Select if you are a VMware Partner or not on the radio button
Register for My VMware Account (continued)

Continue entering in the required information:

1. Select a Department
2. Select a Job Role
3. Enter a Business Phone Number
4. Select a Preferred Language
5. Enter your Company Name
6. Select your Industry
7. Enter your Company Address
8. Enter the City of your Company
9. Enter the zip or postal code of your Company
Enter the Captcha Code

Join VMware Communities

As a member, you may post content like discussions, documents, and blogs to the VMware Community site.

Preferred community username

A-Z, a-z, 0-9 only and no spaces.

☐ Yes, I wish to join VMware Communities and I agree to the VMware Communities Terms of Use.

Enter the Captcha code shown in the box.

NOTE - Please match the captcha visible on your screen and not the manual.

Accept the My VMware Terms of Use

My VMware Terms of Use

Effective Date: 18 September 2017

My VMware Terms of Use

The My VMware Terms of Use is available in the following languages: English, German, French, Japanese, Simplified Chinese, and Korean.

General

Please read these terms of use (the “Terms of Use”) carefully before using the My VMware website. These terms govern your use of the

☐ I agree to the terms and conditions outlined in the My VMware Terms of Use Agreement.

☐ Yes, I would like to receive email communications related to VMware including newsletters and invitation-only events. I understand that any information I provide will be treated in accordance with the VMware Privacy Policy.

Continue entering in the required information:
1. Review the My VMware Terms of Use
2. Check the box indicating you agree to the Terms of Use
3. Uncheck the box indicating you would like to receive email communications
4. Click the Continue button

Check your Email Account

You will receive an activation email next. If you don't receive it in a few minutes, you can click the Resend Email button
Activate your new My VMware Account

When you get the activation email, click the **Activate Now** button, you will now be redirected to an activation webpage.
Enter your My VMware Account Password

1. Enter the password you entered when setting up your My VMware Account
2. Click the **Continue** button
Confirm Your Login Was Successful
Account Activated
If you are not automatically redirected within 15 seconds, click continue.

Continue to My VMware  Continue to my AirWatch

About My VMware
Top 10 things to know
My VMware FAQ
Index of My VMware Articles

VMware Technology
End-User Computing
Hybrid Cloud
Software-Defined Data Center
Virtualization

Try & Purchase
VMware Hardware
Virtual Appliances
Marketplace
VMware Partner Programs
Partner Locator
Online Store

Copyright © 2017 VMware. All rights reserved.
Your My VMware account is now verified and you can use it to log in to the VMware Policy Builder. We will log in to Policy Builder in the next step.
Log into the VMware Policy Builder

![Login screen for VMware Policy Builder](image)

1. Username: `user@company.com`
2. Password: `*******`
3. Login button

Login with your My VMware account

Sign up for an account
If you have a My VMware account do the following to log in.

1. Enter the **email address** you use for My VMware
2. Enter the **password** for your My VMware account
3. Click the **Login** button to log into the Policy Builder

**Review the VMware Policy Builder**

One you are logged in, take a few minutes to review the features of the VMware Policy Builder.

1. This link takes you back to the list of Configuration Service Providers which can be configured via the tool.
2. One a CSP is selected, this link allows you to enter configuration parameters and have the SyncML generated automatically.
3. When this link is clicked, you are taken to a page which allows you to paste in existing SyncML which can be modified graphically.
4. This link allows you to generate a unique GUID and copy it to the clipboard. Some CSP configurations require a GUID to be passed in.
5. This is the list of supported Windows 10 operating systems. The CSPs are unique and specific to the OS version you are targeting.
6. This is the list of CSPs and associated DDF files. Device Description Framework (DDF) files contain the configuration details of a CSP in XML format.

We will use the VMware Policy Builder to create custom SyncML for Windows 10 profiles in Workspace ONE UEM in the next section.
Set a CSP with the VMware Policy Builder

We will now use the VMware Policy Builder to create and push custom policy to our Windows 10 device.

Create a custom CSP for Desktop Background

We will now use the Personalization CSP in order to set the desktop background on your Windows 10 system over the air. This is something that is routinely done through traditional group policy management.

Do the following to find and create a policy from the Personalization CSP

1. Click the **CSPs** tab.
2. Make sure the CSP Baseline is set to **Windows 10, 1709**. This is the operating system of our Windows 10 virtual machine in this lab.
3. Enter **person** in the filter box, to filter on the Personalization CSP.
4. Click the Check-Box next to Personalization to select this CSP for configuration.
5. Click the **Configure** button to start the process of creating a custom policy from this CSP.
Review the Configure Page

1. Click the **Expand All** button to expand all of the settings as defined in the DDF file for the CSP.
2. Click the **Collapse All** button to collapse all of the settings as defined in the DDF file for the CSP.
3. Click the **Reset Form** button to reset any settings you have made on the page.
4. This is where you enter the configuration parameters.
5. The SyncML is dynamically generated here when you enter configuration data.
6. The **Copy** button will save any generated SyncML to the clipboard so it can be pasted into a profile in the Workspace ONE UEM Console.
Configure CSP and copy the generated SyncML

1. Click **Expand All** if the options are collapsed.
2. Enter `\hol\vmware.jpg` in the Desktop Image Url section.
3. Notice the SyncML is generated for you dynamically including the configuration data you entered.
4. Click the **Copy** button to copy the SyncML. We will paste this into the Workspace ONE UEM Console in the following steps.

Create Windows 10 Profile in Workspace ONE UEM

We will now create a custom device profile for Windows 10 containing the SyncML we just generated. We will push it down to our Windows 10 system and then verify the settings applied on the device.
In the Workspace ONE UEM console,

1. Click **Devices**.
2. Select **Profiles**.
3. Select **Add**.
4. Select **Add Profile**.
Select the Windows Platform

Click Windows.

Select the Windows Desktop Device Type

Click Windows Desktop.
Select the Context

Click **Device Profile**.
Enter the General Payload Details

1. Click the **General** payload tab.
2. Enter **Background Image** as the name of the Profile.
3. Select the **All Devices (your@email.shown.here)** group for the Assigned Groups.
Add the Custom Settings Payload

1. Scroll down to the bottom on the left pane.
2. Click the Custom Settings payload tab.
3. Click Configure
Configure the Custom Settings Payload

1. Right-click within the Custom Settings textbox and click **Paste** to paste the SyncML you copied earlier.
2. Ensure the SyncML pasted successfully.
3. Click **Save & Publish**.
Confirm Device Assignment and Publish

1. Review the device assignment. Your Windows 10 device you recently enrolled into Workspace ONE should be listed.
2. Click **Publish** to push the CSP down to your Windows 10 device.

Validate the CSP Profile was Installed

Double-Click the **Win10-01a.rdp** file on the desktop to reconnect to the Windows 10 virtual machine to validate the CSP Profile.
Notice that the desktop background is now set to a VMware logo. This was configured via the Personalization CSP and pushed to your Windows 10 device with Workspace ONE UEM.

**NOTE** - You will see this change as soon as the device checks in with Workspace ONE UEM and the profile is installed. If you do not see the change immediately, try closing the Remote Desktop Connection session to the win10-01a virtual machine and re-connecting.
Update an Existing CSP with VMware Policy Builder

In this exercise, you will modify an existing SyncML which enables or disables Cortana. We will paste the SyncML into the VMware Policy Builder, modify the setting and then create a Workspace ONE Device profile to disable Cortana on your Windows 10 system.
Review current search settings

1. Click the **Search Bar**.
2. Validate that Cortana is enabled on the device.

Return to the Main Console
Click the **Close (X)** button on the remote desktop connection bar to end the session to the Windows 10 device and return to the Main Console.

**Return to the VMware Policy Builder**
1. Click the **Google Chrome** icon from the Task Bar.
2. Click the tab you previously opened to the VMware Policy Builder.

**Modify Existing SyncML**

1. Click the **Modify** tab.
2. Drag-and-drop the below SynML into the SyncML pane. The VMware Policy Builder will read the SyncML and show configuration information in the left pane.
3. Expand **Policy**.
4. Expand **Device**.
5. Expand **Config**.

```xml
<Replace>
  <CmdID>4bfee036-2523-413e-aba3-40102dbca0f5</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/Experience/AllowCortana</LocURI>
    </Target>
    <Meta>
      <Type xmlns="syncml:metinf">int</Type>
      <Format xmlns="syncml:metinf">text/plain</Format>
    </Meta>
    <Data>1</Data>
  </Item>
</Replace>
```
Modify the Allow Cortana Setting

1. Expand Experience
2. Under Allow Cortana notice it is set to 1. That means Cortana is currently enabled.
Disable Cortana and copy SyncML

1. Enter 0 under **Allow Cortana**
2. Notice that the SyncML dynamically updated, and it now shows a 0 for the Data attribute.
3. Click the **Copy** button to copy the SyncML.
Create Profile in Workspace ONE to Disable Cortana

In the Workspace ONE UEM Console,

1. Click Devices.
2. Expand Profiles & Resources.
3. Click Profiles.
4. Click Add.
5. Click Add Profile.

Select the Windows Platform
Click **Windows**.

**Select the Device Type**

Click **Windows Desktop**.

**Select the Context**

Click **Device Profile**.
Setup the General Payload Details

1. Click the **General** payload tab.
2. Enter **Disable Cortana** as the name.
3. Select **All Devices (your@email.shown.here)** for the Assigned Groups.
Enable the Custom Settings Payload

1. Scroll down to find the Custom Settings payload tab.
2. Click the **Custom Settings** payload tab.
3. Click **Configure**.
Configure the Custom Settings Payload

1. Right-click within the the Custom Settings textbox and click **Paste** to paste the copied SyncML.
2. Confirm the SyncML pasted.
3. Click **Save & Publish**.
View the Device Assignment and Publish

1. Review the device assignment. Your Windows 10 desktop which you recently enrolled into Workspace ONE should be listed.
2. Click the **Publish** button to push the CSP down to your Windows 10 device.

**Validate the Search Settings CSP**
Double-click the Win10-01a.rdp file on the desktop of the Main Console to log back in to our Windows 10 device.

**Review Search Settings**

1. Click the **Search Bar**.
2. Confirm that Cortana is disabled.

Cortana is now **disabled** and the system is using standard search. This exercise shows how you can modify and push down existing SyncML with the VMware Policy Builder.
Return to the Main Console

Click the Close (X) button to return to the Main Console to complete the upcoming steps.
Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from Workspace ONE UEM console, also known as managed content.

Delete Device from Workspace ONE UEM Console

From the Workspace ONE UEM Console,

1. Click on **Devices**
2. Click on **List View**
3. Select the check box next to your device friendly name.
4. Click on **More Actions**
5. Click on **Delete Device**
Enter Reason and Delete

1. Enter the reason as "lab completed"
2. Click on Delete
Validate DELETE IN PROGRESS...

List View

1. You may see device friendly name changing to **DELETE IN PROGRESS...**
2. Click on the **Refresh Icon** to validate if the device deletion is successful.

Ensure that device record is deleted

List View

1. Use the **Refresh Button** if needed.
2. Ensure that the device record is now deleted from the Workspace ONE UEM console and you see the message **No Records Found.**
Navigate to Windows 10 VM

If you are not on Windows 10 VM, double-Click the **Win10-01a.rdp** file on the desktop to reconnect to the Windows 10 virtual machine

Navigate to Windows 10 Settings

1. Click on the **Windows Icon**
2. Click on the gear icon to access **Windows 10 Settings**
Access Accounts Settings

From the Settings Menu, access **Accounts**
Validate That No Management Account Exists

1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to device management or other types.
Conclusion

In this module you have learned about why you should start moving from Traditional to Modern Management and how you can use the VMware Policy Builder to generate custom CSPs and you pushed them to your Windows 10 device.
Introduction

In this module, you will migrate devices from Microsoft System Center Configuration Manager (SCCM) to VMware Workspace ONE using Workspace ONE AirLift.
Introduction to Workspace ONE AirLift

VMware Workspace ONE AirLift is a fully supported tool to help ease the migration from traditional PCLM (PC Lifecycle Management) management with SCCM to modern management with Workspace ONE UEM.

Why Co-Management?

- As customers move to Modern Management, traditional PCLM tools are challenging
- Not every customer is 100% at Windows 10, and cannot take advantage of Modern Management
- Legacy Windows desktop Operating Systems (OS's) and Server OS’s need to be managed
- Most companies have had SCCM in place for over 20 years and it is deeply embedded into business systems
- Not easy to just “rip off the band-aid”
- May need SCCM to get to Windows 10
- May need SCCM to upgrade Windows 7 to Windows 10
- Can enroll devices into Workspace ONE with SCCM
- Typical hardware refresh cycle is 3-5 years

Workspace ONE AirLift
Workspace ONE AirLift has the following features:

- Has detailed monitoring information on progress of enrollment and modern management
- Runs as a web service and keeps SCCM and Workspace ONE in sync
- Allows mapping between SCCM device collections and Workspace ONE UEM Smart Groups
  - Uses Tags in Workspace ONE UEM to map devices and groups to SCCM Collections
- Allows migration of applications from SCCM to Workspace ONE
- Allows enrollment of devices into Workspace ONE by creating SCCM deployments
- Has detailed logging information

Pre-Requisites for AirLift

- Clean Windows operating systems which is Domain joined to the same Domain as the SCCM server
  - Windows 10 and Windows Server tested
  - 2 CPU and 4 GB RAM
- SCCM 2012R2 or later
- SCCM permissions required
  - Read Only Analyst for basic functionality
  - Privilege to create and deploy SCCM applications in order to build and deploy a custom enrollment application
  - At least one SCCM Device Collection with at least one Windows 10 client
- Workspace ONE 9.5 or later
Connect to the SCCM Server

We will be doing all of the AirLift configuration on the SCCM server.

Launch `sccm-01a.rdp` from the main desktop.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the **Chrome** Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your **Username**. This is your **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

IF YOU HAVE PURCHASED VMWARE IDENTITY MANAGER AS A SERVICE, YOUR USE OF VMWARE IDENTITY MANAGER IS SUBJECT TO THE VMWARE IDENTITY MANAGER TERMS OF SERVICE AVAILABLE AT: HTTP://WWW.VMWARE.COM/DOWNLOAD/EULA.HTML. IF YOU HAVE PURCHASED WORKSPACE ONE AS A SERVICE, YOUR USE OF VMWARE IDENTITY MANAGER IS SUBJECT TO THE WORKSPACE ONE TERMS OF SERVICE AVAILABLE AT: HTTP://WWW.VMWARE.COM/DOWNLOAD/EULA.HTML.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 “Affiliate” means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls.

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

Confirm Security PIN *

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE

Don't show this message on login
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Setup Workspace ONE AirLift

You will now setup Workspace ONE AirLift, connecting it to both Workspace ONE UEM and Microsoft SCCM in order to support Co-Management of Windows 10 devices.

Retrieve the Workspace ONE UEM API Key

We now need to retrieve the admin REST API key from the Workspace ONE UEM Console. This key will be required by AirLift in order to connect to Workspace ONE UEM.
In the Workspace ONE UEM Console,

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

**Copy the REST API Key**

1. Expand **System**.
2. Expand **Advanced**.
3. Expand **API**.
4. Select **REST API**.
5. Select the **API Key** value for the AirWatchAPI service.
6. Right-click and click **Copy**.

You will need this key in the upcoming steps for configuring AirLift.
Launch Workspace ONE AirLift

Double click the **AirLift** shortcut on the desktop of the SCCM server.

This will be the first time we are launching AirLift, so we will be asked to configure connectivity to Workspace ONE UEM and SCCM.

**Configure AirLift**

We will now configure AirLift to connect to both Workspace ONE UEM and SCCM.

**Configure AirLift for Workspace ONE**

![Workspace ONE AirLift configuration interface]

**Connect Workspace ONE**

Enter Workspace ONE connection information

1. **API URL**: [https://labs.awmdm.com](https://labs.awmdm.com)
2. **Console Address**: Same as API
3. **API Key**: [Your API Key]
4. **Username**: [Your VLP Email Address]
5. **Password**: [VMware]
6. **CONTINUE**
1. Enter [https://labs.awmdm.com](https://labs.awmdm.com) for the API URL.
2. Select Same as API for the Console Address.
3. Paste the API Key from your Workspace ONE tenant that you captured in the previous step.
4. Enter your email address that you have associated with your VMware Learning Platform (VLP) account.
5. Enter VMware1! for the Password field.
6. Click the Continue button.

**Configure AirLift for SCCM**

1. Enter **sccm-01a.corp.local** for the SCCM Server
2. Enter **HOL** for the Site Code
3. Enter **CORP** as the Domain
4. Enter **Administrator** as the Account
5. Enter **VMware1!** as the Password
6. Click the Submit button

Congratulations - you have successfully configured AirLift!
The first time you launch AirLift, you will be taken to a getting started page with direct links to different phases of Co-Management.

Click on **Plan** to start using AirLift. This will take us to the **Collections** screen.
Review Device Collections in AirLift and compare to SCCM

When AirLift connects to SCCM, it imports Device Collections from SCCM. Let’s take a look at the information which AirLift has imported and compare it to what is in our SCCM server.

1. Click the eye symbol to the right of Getting Started so that a \ is through it. This will prevent Getting Started from coming up each time we refresh the page.
2. Click on Collections, if you are not already there.
3. Review the Collections that have already been imported into AirLift from SCCM. Notice all of the Device Collections which are imported have at least one device assigned.

Open the SCCM Console

Click the SCCM Console icon from the taskbar to return to the SCCM Console.
Navigate to SCCM Device Collections

1. Click on **Assets and Compliance**.
2. Click on **Device Collections**.
3. Review and compare the list of collections in SCCM to what is in AirLift. Notice they DO NOT match. This is because AirLift only imports Device Collections from SCCM which contain Windows 10 devices.
Review Management of Collections in AirLift

Back in the AirLift Console in Chrome,

1. Click the checkbox next to the Win10 collection.
2. You can Map, Enroll, and Manage devices in collections from these buttons. DO NOT interface with these yet, you will be using them in upcoming steps to view the functionality.
   - **Map** allows you to determine a Workspace ONE UEM Smart Group for this collection to belong to in order to enable Co-Management.
   - **Enroll** is enabled once Co-Management is enabled for a Collection, and allows you to enroll devices into Workspace ONE UEM.
   - **Manage** is enabled once Co-Management is enabled for a Collection, and allows you to view and manage the Smart Group that your collection is mapped to in Workspace ONE UEM.
3. Data is refreshed from SCCM and Workspace ONE UEM on a schedule. You can click this button to initiate an immediate refresh of Collection and Smart Group data.
4. Click the number (1) in the Devices column for the Win10 collection. This will open a page with details on the devices in this collection.
Review your Windows 10 Machine

1. Review the machine in the Win10 collection. This is the Win10-01a Virtual Machine that is available to you for this lab.
2. Click the Collections link to return to the collections page.

Map the Win10 Collection

1. Click the checkbox for the Win10 collection to select it.
2. Click Map.

When you click the Map button on a Collection, a list of available Workspace ONE UEM Smart Groups will be displayed, which you can choose from to map your device collections to enable Co-Management.
Map SCCM Collection to Workspace ONE Group

1. Enter **AirLift** for Workspace ONE Group. Notice that the AirLift group does not exist in the dropdown list of available Workspace ONE UEM Smart Groups. Entering in the name manually will have the AirLift Smart Group automatically created and mapped for Co-Management in the Workspace ONE UEM Console. **NOTE:** If you had an existing Smart Group you wanted to use to map and enable Co-Management for, you could select that from the Workspace ONE Group dropdown instead.

2. Click **Save** to have the Win10 Device Collection mapped to the AirLift Smart Group in Workspace ONE UEM.
Confirming AirLift Smart Group Creation

1. After clicking save, a message from AirLift will confirm that the Smart Group creation and mapping is **In Progress**. This will update to a clickable link once it is completed.

2. Once completed, the Workspace Mapping will update to the AirLift Smart Group and the Management column will reflect that the devices in this collection are now Co-managed. Click the **AirLift** hyperlink, this will take you directly to the Smart Group in the Workspace ONE UEM Console.

**NOTE** - This process may take a few minutes to complete. If the page does not refresh automatically, you can click the **Refresh** button on the browser or the **Refresh** button in AirLift to check if the task has completed after a few minutes!
AirLift Smart Group in Workspace ONE UEM Console

Notice that clicking the AirLift hyperlink in AirLift will automatically take you to the AirLift Smart Group mapping in the Workspace ONE UEM Console.

Click the **Edit** icon next to the AirLift Smart Group.
View Smart Group

1. Scroll down to find the Tags section.
2. Notice that a new custom tag is created with the format `Co_Mgmt:site_<SCCM_Site_Code>:<Device_Collection_ID>`. This was generated automatically from AirLift.
3. Click on the X to close this popup.
Review Workspace ONE AirLift

You will now review additional features and settings of AirLift to familiarize yourself with the console before upcoming exercises.

Review Devices in AirLift and Compare to SCCM

AirLift imports Windows 10 devices that are active SCCM Clients. Let's take a look at what AirLift has imported and compare it to SCCM.

In the AirLift Console in Chrome,

1. Click on Devices in AirLift.
2. Review details on the device imported into AirLift.
1. Click the **SCCM Console icon** from the taskbar to return to the SCCM Console.
2. Click on **Assets and Compliance**.
3. Click on **Devices**.
4. Review the list of devices in SCCM. Notice there is only one active SCCM client that is running Windows 10. This is the system that was imported into AirLift.
Review Applications in AirLift and compare to SCCM

AirLift imports metadata on SCCM Applications and allows these applications to be imported via APIs to Workspace ONE UEM. This greatly simplifies the process of migrating applications to Workspace ONE without the need for repackaging.

Back in the AirLift Console in Chrome,

1. Click on Applications.
2. Review the list of applications that have already been imported into AirLift.
Review Applications in SCCM

1. Click the **SCCM Console icon** from the task bar.
2. Click on **Software Library**.
3. Expand **Application Management**.
4. Click **Applications**.
5. Review the applications in SCCM - notice they match what was imported into AirLift.
This module will not cover managing and migrating applications using AirLift in detail. If you wish to learn more on this subject, refer to [Module 6 - Migrating Applications from SCCM](#).

**Review the AirLift Activity Log**

The activity logs show details of actions such as exporting applications, or setting Workspace ONE or SCCM connection information.

In the AirLift Console in Chrome,

1. Click on **Activity Log**.
2. Review the Activity Log details. Notice that the actions you have taken during this exercise have been logged here for review. This section can be useful for recalling past actions and troubleshooting.
Review the AirLift Settings

All of the account settings that were set during the initial launch of AirLift can be modified in the Settings section. In addition, Enrollment settings are managed here. The enrollment section lets you build a custom enrollment package in SCCM or select an existing one.

1. Click on **Settings** in AirLift.
2. Review the **Workspace ONE** settings. These settings can be updated from here if required.
3. Scroll down to **Enter connection information for System Center Configuration Manager**.

![Workspace ONE AirLift settings](image)

HOL-1957-04-UEM
1. Review the SCCM settings. These settings can be updated from here if required.
2. Scroll back up to the very top.
Review Enrollment Application

1. Click the Enrollment tab to manage enrollment settings.
2. Select Yes for Use Existing Enrollment Application.
3. You can select an existing SCCM application to use for enrollment.

DO NOT select anything for now, you will return to these settings when enrolling a device in upcoming steps.
Review the AirLift Dashboard

The AirLift dashboard provides real-time information on your workloads which are managed by AirLift.

1. Click **Dashboard**.
2. The **Devices** section shows the number of devices managed by Workspace ONE UEM.
3. The **Applications** section shows the number of applications managed by Workspace ONE UEM.
4. The **Top Workloads** section shows the highest workloads on enrolled systems.
5. The **Co-Management by Collection** section shows the breakdown of SCCM and Co-Management by collection.

Now that you are familiar with the overview of AirLift, the upcoming exercises will show how to use AirLift to manage and enroll a device.
Setup a Profile in Workspace ONE UEM

In this exercise, you will create a profile in the Workspace ONE UEM Console to configure BitLocker. These policies will be deployed to our AirLift Co-Managed devices and will be reported to our AirLift Dashboard. This allows us to co-manage the devices in this SCCM collection with AirLift and Workspace ONE UEM.

Create Windows 10 Profile for Devices

In the Workspace ONE UEM Console,

1. Click **Devices**.
2. Expand **Profiles & Resources**.
3. Click **Profiles**.
4. Click **Add**.
5. Click **Add Profile**.

![Diagram of Workspace ONE UEM Console](image)
Select the Windows Platform

Select Windows.

Select the Device Type

Select Windows Desktop.
Select the Context

Select Device Profile.

Configure the Profile General Payload

Add a New Windows Desktop Profile

**General**

- **Name**: BitLocker
- **Version**: 1
- **Description**: 
- **Deployment**: Managed
- **Assignment Type**: Auto
- **Allow Removal**: Always
- **Managed By**: chalstead
- **Assigned Groups**: 
  - Airlift
  - Start typing to add a group
1. Enter **BitLocker** as the name of the profile.
2. Select **AirLift (your@email.shown.here)** for the Assigned Groups.

**Enable the Encryption Payload**

1. Select **Encryption**.
2. Click **Configure**.
Configure the Encryption Payload

BitLocker Encryption:

- **Encrypted Volume**: Select **System Partition**
- **Encryption Method**: Select **System Default**
- **Only encrypt used space during initial encryption**: Click the checkbox
- **Custom URL for Recovery Screen**: Enter your device services host name
- **BitLocker Authentication Settings**
  - **Authentication Mode**: Select **Password**
  - **Minimum Password Length**: Enter 8
- **BitLocker Static Recovery Key Settings**: Copy and paste

1. Select **System Partition** for Encrypted Volume.
2. Select **System Default** for Encrypted Method.
3. Click the checkbox next to Only encrypt used space during initial encryption.
4. Select **Password** for the Authentication Mode.
5. Enter 8 for the Minimum Password Length.
6. Click **Save & Publish**.
Publish the Encryption Profile

Click **Publish**.

Confirm the BitLocker Profile

<table>
<thead>
<tr>
<th>Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>Profile Details</td>
</tr>
<tr>
<td>BitLocker</td>
</tr>
<tr>
<td>Windows Desktop - Encryption</td>
</tr>
</tbody>
</table>
View the BitLocker profile you just created, and make sure it is assigned to the AirLift group.
Enroll SCCM Devices in Workspace ONE UEM with AirLift

In this exercise, you will configure a SCCM Enrollment application for your Workspace ONE UEM tenant and then deploy the application to the AirLift Collection that you have enabled for Co-Management.

Create Enrollment Application in AirLift

1. Click **Settings**.
2. Click **Enrollment**.
3. Select **No** for Use Exiting Enrollment Application.

In the AirLift Console in Chrome,

1. Click **Settings**.
2. Click **Enrollment**.
3. Select **No** for Use Exiting Enrollment Application.
4. Enter **Workspace ONE Enrollment**.
5. Select your VLP email address from the Organization Group dropdown.
6. Enter **StagingUser**
7. Enter **VMware1!**
8. Enter **labs.awmdm.com**
9. Check the **Include Workspace ONE App** option. This option will automatically install the Workspace ONE app if it is not present on the device.
10. Un-check the **Include SCCM Integration Client** option, this client is only needed when using pre-1709 Windows 10 and pre-1710 SCCM.
11. Click **Show**.

**Copy the Agent Install Command Line**

1. Click and drag and highlight the Agent Install Command Line.
2. Right-click the highlighted text and click **Copy**.

You will modify and use this copied text in an upcoming step.
Enter the Enrollment Application Content Location

Agent Install Command Line

```
msiexec.exe /i AirwatchAgent.msi /qn ENROLL=Y IMAGE=N SERVER= labs.awmdm.com
LGNAME=your@email.shown.here
USERNAME=StagingUser PASSWORD=VMware1!
DOWNLOADWSBUNDLE=true
ASSIGMENTLOGGEDINUSER=Y /log
%TEMP%\AAgent.log
```

Content Location

```
\SCCM-01\SCCMPackages\WS1
```

Distribution Selection

- Auto
- Manual

1. Enter \SCCM-01\SCCMPackages\WS1 for Content Location. The needed files have been pre-staged at this location for your convenience.
2. Click Create.

Confirm Application Creation

Create Application

Ensure you have copied the enrollment application files to the specified path before proceeding.

Click Proceed.
Review and Modify Workspace ONE Enrollment Application

The following steps involving modifying the Workspace ONE Enrollment app are not needed in production. However, you will need to update the install command-line for this lab.

Update Install Command Line

1. Right-Click the Windows button.
2. Click Search.
3. Enter `Notepad` for the search.
4. Click the **Notepad** application.
Paste the Copied Install Command Line Text

1. Click **Edit**.
2. Click **Paste**.
3. Click **Format**.
4. Click **Word Wrap** to enable wrapping.

Locate the LGName property

You will need to update the LGNAME value in our copied install command line to match your Group ID from the Workspace ONE UEM Console. Continue to the next step to find the Group ID value to use here.
Obtain your Group ID from the Workspace ONE UEM Console

In the Workspace ONE UEM Console,

1. Click on your Organization Group name.
2. Copy your Group ID value. In this example, the Group ID is yourid1234.

Update the LGNAME Value

Update the LGNAME value with your Group ID from the Workspace ONE UEM Console. **DO NOT** use yourid1234 as shown, be sure to use your own Group ID.
Copy the Updated Install Command Line Text

1. Click **Edit**.
2. Click **Select All**.
3. Click **Edit**.
4. Click **Copy**.
Review and Modify Properties of Workspace ONE Enrollment Application

1. Click the **SCCM Console icon** from the task bar.
2. Click **Software Library**.
3. Expand **Application Management**.
4. Click **Applications**.
5. If you do not see the Workspace ONE Enrollment application in the list, you may need to click the **Refresh** button.
6. Right-Click the **Workspace ONE Enrollment** application.
7. Click **Properties**.
Edit the Workspace ONE Enrollment Windows Installer

1. Click the **Deployment Types** tab.
2. Select the **Workspace ONE Enrollment - Windows Installer x64 (*.msi file)**.
3. Click the **Edit** button.
Replace the Installation Program Command

1. Click the **Programs** tab.
2. In the Installation program text box, remove ALL existing text and paste your copied install command.
3. Click **OK**.
Save the Deployment Types Changes

Click **OK** again to save your changes.

**Enroll Members of the Win10 Collection into Workspace ONE UEM**

Now that we have create the Workspace ONE Enrollment app using AirLift and mapped our Win10 device collection to the AirLift Smart Group, we will leverage AirLift to automatically onboard our Win10 collection devices into Workspace ONE UEM.
Enroll the Win10 Collection into Workspace ONE UEM

In the AirLift Console in Chrome,

1. Click **Collections**.
2. Click the **checkbox** next to the **Win10** collection.
3. Click the **Enroll** button.

Confirm Devices Affected

Are you sure you want to begin Workspace ONE enrollment?

1 Devices will be affected.

Click the **Enroll** button to confirm the enrollment - notice 1 Device will be affected.
Review Enrollment Confirmation

Review enrollment confirmation, the devices in the Win10 collection have begun enrollment.

Review Enrollment Application Deployment in SCCM

Back in the SCCM Console, ensure the **Workspace ONE Enrollment** app is selected.
1. Click on the SCCM Console icon on the task bar.
2. Ensure the Workspace ONE Enrollment app is still selected.
3. Click on the Deployments tab.
4. Notice there is a deployment which was created by AirLift. This deployment is mandatory and automatic and targets the Win10 collection.

**Return to the Main Console**

Click the Close (X) button to return to the Main Console.

**Connect to Windows 10 Device**

Double-click the Win10-01a.rdp shortcut on the desktop of the Main Console.

**Modify Internet Options for Windows Enrollment**

Before enrolling the Windows 10 Virtual Machine, we will make a modification to prevent issues with the Hands on Labs firewall causing a delay in the enrollment process.
Open Settings

1. Click the Windows button.
2. Click the Settings (Gear) icon.

Open Internet Options
1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.

**Modify the Certificate Revocation Options**

1. Click the **Advanced** tab.
2. Scroll down to find the **Security** section.
3. **Uncheck** the **Check for publisher's certificate revocation** option.
4. **Uncheck** the **Check for server certificate revocation** option.
5. Click **Apply**.
6. Click **OK**.
Launch Configuration Manager

Double-click the **Configuration Manager shortcut** on the desktop of the Windows 10 device.

Force policy update on SCCM Client

We will now force a policy retrieval cycle on the SCCM client in order to speed up the process of receiving the deployment and enrolling the device into Workspace ONE UEM.

1. Click the **Actions** tab.
2. Select **Machine Policy Retrieval & Evaluation Cycle**.
3. Click the **Run Now** button.

### Confirm the Cycle Prompt

![Machine Policy Retrieval & Evaluation Cycle]

Click **OK** to confirm the cycle may take several minutes to complete.

### Monitor Enrollment into Workspace ONE

![AirWatch Enrollment icon]

Watch for the **AirWatch Enrollment icon** on the desktop of the Windows 10 system.

The deployment will run automatically and should happen fairly quickly. If you watch the desktop of the Windows 10 client, you will see the AirWatch Enrollment icon appear on the desktop. This means the enrollment process is running. This process should only take a few minutes at most to complete.

### Verify via Software Center

![SCCM Software Center]

Click the icon shortcut on the taskbar of the Windows 10 device to launch the SCCM Software Center.
We can also verify that the deployment has been received on the Windows 10 client by reviewing the SCCM Software Center

1. Click the **Applications** tab.
2. Notice the **Workspace ONE Enrollment** deployment has been received on the Windows 10 client.

You don't need to run the deployment manually. It will execute automatically.
Enter Agent User Credentials

Since the install command line was setup to use a staging user account (named StagingUser), you will now need to provide your user credentials as part of the enrollment.

1. Enter aduser for the Username.
2. Enter VMware1! for the Password.
3. Click Submit.

NOTE: The user is only prompted for credentials due to the architecture of this lab. In real deployments where the VMware Enterprise Systems Connector is installed at the Customer organization group and has access to the domain controller, the user would not need to enter credentials.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

NOTE - If you see a Captcha, please be aware that it is case sensitive!

1. Enter your Username. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter VMware1! for the Password field.
3. Click the Login button.

NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls,

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

Confirm Security PIN *

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the Don't show this message on login check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Review and Validate the Enrolled Windows 10 Device

You will now review the enrolled Windows 10 device in the Workspace ONE UEM Console and AirLift Console to see how to confirm that the enrollment was successful. You will also verify that the BitLocker profile you configured was delivered to the device.

Return to the Main Console

Click the Close (X) button on the Remote Desktop Connection to return to the Main Console.

Connect to the SCCM Server

Launch `sccm-01a.rdp` from the main desktop.
Initiate Full Sync for AirLift

We will want to perform a real-time sync between AirLift and Workspace ONE UEM to see an updated dashboard.

In the AirLift Console in Chrome,

1. Click **Settings**.
2. Scroll down to the bottom of the Account tab.
3. Click **Sync**.
Review AirLift Dashboard

1. Click on the **Dashboard** link on the left pane of AirLift.
2. Notice on the **Top Workloads** section, you see there is a client with Encryption and Compliance Enabled.

Return to the Main Console

Click the **Close (X)** button to return to the Main Console.
Connect to Windows 10 Device

Double-click the Win10-01a.rdp shortcut on the desktop of the Main Console.

Review Enrolled Client in Workspace ONE UEM Console

In the Workspace ONE UEM Console,

1. Click **Devices**.
2. Click **List View**.
3. If you navigate to the Workspace ONE UEM Console quickly enough, you may see that the device is enrolled to the StagingUser account. Shortly after enrolling your user credentials for aduser, the device will show it is enrolled for aduser instead. Click the device link to view the **Device Details View**.
Review Device Details

1. Notice the device is a member of the AirLift Workspace ONE Smart Group, due to enabling Co-Management.
2. Review the computer name, this matches what we seen earlier in the SCCM and AirLift console.
3. Notice the device has had the Co-Management tag added to it. This is the same tag that was added to the Workspace ONE AirLift Smart Group. This is what enables synchronization between SCCM and Workspace ONE during Co-Management.
Verify BitLocker Profile is Pushed via AirLift Co-Management

The BitLocker Encryption dialog will pop up, indicating the device was enrolled into Workspace ONE UEM and that it is properly enabled for Co-Management.

1. Enter **VMware1!** for the password.
2. Enter **VMware1!** for the password confirmation.
3. Click the **Encrypt** button to start BitLocker encryption.
Close the VMware Workspace ONE App

The Workspace ONE Application will open automatically after enrollment.

Click the X to close the application. We don't use it during this exercise.

Validation Completed

Congratulations! You have successfully enrolled your Windows 10 device into Workspace ONE UEM using AirLift and validated a successful enrollment after pushing a BitLocker profile to the device!
Conclusion

In this module you have learned how to setup and use VMware Workspace ONE AirLift to setup Co-Management between SCCM and Workspace ONE. You have also learned how to automatically enroll SCCM devices into Workspace ONE using AirLift.
Module 6 - Migrating Applications from SCCM
Introduction

In this module, you will migrate an application from Microsoft System Center Configuration Manager (SCCM) to Workspace ONE UEM using Workspace ONE AirLift
Enrolling Your Windows 10 Device (Optional)

NOTE: You only need to perform the following steps if you did not complete the previous module (Module 5 - Migrating Devices from SCCM). Skip to the next exercise if your Windows 10 system is already enrolled.

You will now enroll a Windows 10 device in Workspace ONE UEM. You will need to connect to the Windows 10 virtual machine made available as part of the lab and download and run the Workspace ONE Intelligent Hub.

Connect to the Windows 10 Virtual Machine

Double-click the Win10-01a.rdp shortcut from the Main Console Desktop to connect to the Windows 10 virtual machine.

Modify Internet Options for Windows Enrollment

Before enrolling the Windows 10 Virtual Machine, we will make a modification to prevent issues with the Hands on Labs firewall causing a delay in the enrollment process.
Open Settings

1. Click the Windows button.
2. Click the Settings (Gear) icon.

Open Internet Options
1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.

**Modify the Certificate Revocation Options**

1. Click the **Advanced** tab.
2. Scroll down to find the **Security** section.
3. **Uncheck** the **Check for publisher’s certificate revocation** option.
4. **Uncheck** the **Check for server certificate revocation** option.
5. Click **Apply**.
6. Click **OK**.
Download the Workspace ONE Intelligent Hub on the Windows 10 VM

From a new tab in the browser, if not opened already,

2. Click Download.
   **NOTE:** Please wait while the Workspace ONE Intelligent Hub installer finishes downloading.
3. Click Keep when warned about the AirWatchAgent.msi file download.

**NOTE - If you do not see the warning about the AirWatchAgent.msi file, skip this and continue to the next step.**
Launch the Workspace ONE Intelligent Hub Installer

Click the **AirWatchAgent.msi** file in your download bar.

**NOTE** - The installer may take a few seconds to launch, please be patient after clicking the **AirWatchAgent.msi** file.

Click **Run** to proceed with the installation.
Accept the Default Install Location

Leave the default install location and click **Next**.

*NOTE - The Next button may take several seconds to enable while the required additional features are installed.*
Accept the License Agreement

1. Select **I accept the terms of the license agreement**.
2. Click **Next**.
Start the Workspace ONE Intelligent Hub Install

Click **Install** to start the installer.
Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

If prompted to allow the app to make changes on your device, click **Yes**.
Complete the Workspace ONE Intelligent Hub Installer

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

*NOTE - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.*
Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

Click Server Detail.

Find your Group ID from Workspace ONE UEM Console
The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

### Enter the Server Details

1. Enter **labs.awmdm.com** for the **Server Name** field.
2. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
Enter Your User Credentials

1. Enter **aduser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Click **Next**

*NOTE - Wait while the server checks your enrollment details.*
Since our Workspace ONE UEM and VMware Identity Manager environments are linked for this environment, the Workspace ONE Application will automatically open after enrollment is complete. You will not need it for this exercise, so click **Close**.
Finish the Workspace ONE UEM Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM.

Return to the Main Console

Click the **Close (X)** button on the Remote Desktop Connection bar to return to the Main Console.
Connect to the SCCM Server

Double-click the `sccm-01a.rdp` shortcut from the Main Console Desktop to connect to the SCCM Server.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your **Username**. This is your email address that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

IF YOU HAVE PURCHASED VMWARE IDENTITY MANAGER AS A SERVICE, YOUR USE OF VMWARE IDENTITY MANAGER IS SUBJECT TO THE VMWARE IDENTITY MANAGER TERMS OF SERVICE AVAILABLE AT: HTTP://WWW.VMWARE.COM/DOWNLOAD/EULA.HTML. IF YOU HAVE PURCHASED WORKSPACE ONE AS A SERVICE, YOUR USE OF VMWARE IDENTITY MANAGER IS SUBJECT TO THE WORKSPACE ONE TERMS OF SERVICE AVAILABLE AT: HTTP://WWW.VMWARE.COM/DOWNLOAD/EULA.HTML.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE: If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

What was your childhood nickname?  

Password Recovery Answer *

VMware1!  

Confirm Password Recovery Answer *

VMware1!  

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

1234  

Confirm Security PIN *

1234  

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Setup Workspace ONE AirLift

You will now setup Workspace ONE AirLift, connecting it to both Workspace ONE UEM and Microsoft SCCM in order to support Co-Management of Windows 10 devices.

Retrieve the Workspace ONE UEM API Key

We now need to retrieve the admin REST API key from the Workspace ONE UEM Console. This key will be required by AirLift in order to connect to Workspace ONE UEM.
In the Workspace ONE UEM Console,

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

**Copy the REST API Key**

1. Expand **System**.
2. Expand **Advanced**.
3. Expand **API**.
4. Select **REST API**.
5. Select the **API Key** value for the AirWatchAPI service.
6. Right-click and click **Copy**.

You will need this key in the upcoming steps for configuring AirLift.
Launch Workspace ONE AirLift

Double click the AirLift shortcut on the desktop of the SCCM server.

This will be the first time we are launching AirLift, so we will be asked to configure connectivity to Workspace ONE UEM and SCCM.

Configure AirLift

We will now configure AirLift to connect to both Workspace ONE UEM and SCCM.

Configure AirLift for Workspace ONE

Connect Workspace ONE

Enter Workspace ONE connection information

1. API URL: https://labs.awmelm.com
2. Console Address: Same as API (Yes)
3. API Key: [Redacted]
4. Username: [Redacted]
5. Password: [Redacted]
6. Continue
1. Enter [https://labs.awmdm.com](https://labs.awmdm.com) for the API URL.
2. Select Same as API for the Console Address.
3. Paste the API Key from your Workspace ONE tenant that you captured in the previous step.
4. Enter your email address that you have associated with your VMware Learning Platform (VLP) account.
5. Enter VMware1! for the Password field.
6. Click the Continue button.

**Configure AirLift for SCCM**

![Workspace ONE AirLift](image)

**Connect System Center Configuration Manager**

- SCCM Server: sccm-01a.corp.local
- Site Code: HOL
- Domain: CORP
- Username: Administrator
- Password: VMware1!

1. Enter **sccm-01a.corp.local** for the SCCM Server
2. Enter **HOL** for the Site Code
3. Enter **CORP** as the Domain
4. Enter **Administrator** as the Account
5. Enter **VMware1!** as the Password
6. Click the **Submit** button

Congratulations - you have successfully configured AirLift!
Review and Enable Co-Management in Workspace ONE AirLift

The first time you launch AirLift, you will be taken to a getting started page with direct links to different phases of Co-Management.

Click on Plan to start using AirLift. This will take us to the Collections screen.
Review Device Collections in AirLift and compare to SCCM

When AirLift connects to SCCM, it imports Device Collections from SCCM. Let's take a look at the information which AirLift has imported and compare it to what is in our SCCM server.

1. Click the eye symbol to the right of Getting Started so that a \ is through it. This will prevent Getting Started from coming up each time we refresh the page.
2. Click on Collections, if you are not already there.
3. Review the Collections that have already been imported into AirLift from SCCM. Notice all of the Device Collections which are imported have at least one device assigned.

Open the SCCM Console

Click the SCCM Console icon from the taskbar to return to the SCCM Console.
Navigate to SCCM Device Collections

1. Click on **Assets and Compliance**.
2. Click on **Device Collections**.
3. Review and compare the list of collections in SCCM to what is in AirLift. Notice they DO NOT match. This is because AirLift only imports Device Collections from SCCM which contain Windows 10 devices.
Review Management of Collections in AirLift

Back in the AirLift Console in Chrome,

1. Click the **checkbox** next to the Win10 collection.
2. You can Map, Enroll, and Manage devices in collections from these buttons. DO NOT interface with these yet, you will be using them in upcoming steps to view the functionality.
   - **Map** allows you to determine a Workspace ONE UEM Smart Group for this collection to belong to in order to enable Co-Management.
   - **Enroll** is enabled once Co-Management is enabled for a Collection, and allows you to enroll devices into Workspace ONE UEM.
   - **Manage** is enabled once Co-Management is enabled for a Collection, and allows you to view and manage the Smart Group that your collection is mapped to in Workspace ONE UEM.
3. Data is refreshed from SCCM and Workspace ONE UEM on a schedule. You can click this button to initiate an immediate refresh of Collection and Smart Group data.
4. Click the number (1) in the Devices column for the Win10 collection. This will open a page with details on the devices in this collection.
Review your Windows 10 Machine

1. Review the machine in the Win10 collection. This is the Win10-01a Virtual Machine that is available to you for this lab.
2. Click the Collections link to return to the collections page.

Map the Win10 Collection

1. Click the checkbox for the Win10 collection to select it.
2. Click Map.

When you click the Map button on a Collection, a list of available Workspace ONE UEM Smart Groups will be displayed, which you can choose from to map your device collections to enable Co-Management.
Map SCCM Collection to Workspace ONE Group

1. Enter **AirLift** for Workspace ONE Group. Notice that the AirLift group does not exist in the dropdown list of available Workspace ONE UEM Smart Groups. Entering in the name manually will have the AirLift Smart Group automatically created and mapped for Co-Management in the Workspace ONE UEM Console. **NOTE:** If you had an existing Smart Group you wanted to use to map and enable Co-Management for, you could select that from the Workspace ONE Group dropdown instead.

2. Click **Save** to have the Win10 Device Collection mapped to the AirLift Smart Group in Workspace ONE UEM.
Confirming AirLift Smart Group Creation

1. After clicking save, a message from AirLift will confirm that the Smart Group creation and mapping is **In Progress**. This will update to a clickable link once it is completed.

2. Once completed, the Workspace Mapping will update to the AirLift Smart Group and the Management column will reflect that the devices in this collection are now Co-managed. Click the **AirLift** hyperlink, this will take you directly to the Smart Group in the Workspace ONE UEM Console.

**NOTE** - This process may take a few minutes to complete. If the page does not refresh automatically, you can click the **Refresh** button on the browser or the **Refresh** button in AirLift to check if the task has completed after a few minutes!
AirLift Smart Group in Workspace ONE UEM Console

Notice that clicking the AirLift hyperlink in AirLift will automatically take you to the AirLift Smart Group mapping in the Workspace ONE UEM Console.

Click the **Edit** icon next to the AirLift Smart Group.
1. Scroll down to find the **Tags** section.
2. Notice that a new custom tag is created with the format **Co_Mgmt:site_**<SCCM_Site_Code>**: <Device_Collection_ID>. This was generated automatically from AirLift.
3. Click on the X to close this popup.
Migrate Application from SCCM to Workspace ONE UEM with AirLift

Review Applications in AirLift

AirLift imports metadata on SCCM Applications and allows these applications to be imported via APIs to Workspace ONE UEM. This greatly simplifies the process of migrating applications to Workspace ONE without the need for repackaging.

Back in the AirLift Console in Chrome,

1. Click on Applications.
2. Review the list of applications that have already been imported into AirLift.
Review Applications in SCCM

1. Click the **SCCM Console icon** from the task bar.
2. Click on **Software Library**.
3. Expand **Application Management**.
4. Click **Applications**.
5. Review the applications in SCCM - notice they match what was imported into AirLift.
Confirm Apps in SCCM are not available in Workspace ONE UEM

In the Workspace ONE UEM Console,

1. Click **Apps & Books**.
2. Expand **Applications**.
3. Click **Native**.
4. Click the **Internal** tab.
5. Confirm that the applications seen in AirLift and SCCM are currently unavailable in the Workspace ONE UEM Console.

Managing Applications in AirLift

In the AirLift Console in Chrome,

1. Click the **checkbox** next to 7-Zip 17.01 (x64 edition).
2. Click on the informational tooltip. Notice we receive a validation warning since our app in SCCM is set for both system/user install context. AirLift tells us it will default to using Device context when exporting to Workspace ONE UEM.

3. Click the **Export** button to export an application from SCCM to Workspace ONE UEM.

### Export Applications Confirmation

![Export Applications Confirmation](image)

Click **Export** to confirm.

### Viewing Exported App in Workspace ONE UEM Console

![Applications](image)

AirLift indicates when an application has been exported, then displays a link under the Workspace Application column.

1. After the Application has been exported, the Status will change from Exporting to **Exported**.
2. To manually check the status of the export, click the **Refresh** button.

**NOTE:** The application may take several minutes to finish exporting.

3. Click the **7-Zip 17.01 (x64 edition)** hyperlink, which takes you directly to the app in the Workspace ONE UEM console.
Assign 7-Zip

Once we export the app to the Workspace ONE UEM console, all you have to do is assign the app to devices. In this case, we will assign the app to our AirLift smart group which we mapped to our Win10 SCCM device collection.

Click **Assign**.

**Assign and Publish the Application**

Once we export the app to the Workspace ONE UEM console, all you have to do is assign the app to devices. In this case, we will assign the app to our AirLift smart group which we mapped to our Win10 SCCM device collection.

Click **Add Assignment**.
Add Assignment

1. Select the **AirLift** smart group for the Assignment Group.
2. Select **Auto** for the App Delivery Method.
**Configure Assignment Policies**

1. Scroll down to the Policies section.
2. Select **Enabled** for Make App MDM Managed if User Installed. **NOTE:** This option allows Workspace ONE UEM to assume management of an application that the user has already installed, allowing you to check for installation status and manage the application as necessary.
3. Click **Add**.

---

Would you like to enable Data Loss Prevention (DLP)?
DLP policies provide controlled exchange of data between managed and unmanaged applications on the device.
To prevent data loss on this application, make it "Managed Access" and create "Restriction" profile policies for desired device types.
Update Assignment

Click **Save & Publish**.
Click **Publish**.
Connect to the Windows 10 Virtual Machine

Click the Close (X) button to return to the Main Console.

Connect to Windows 10 Virtual Machine

Double-click the **Win10-01a.rdp** shortcut on the desktop of the Main Console.
Confirm Application Install on Windows 10 Device

1. Click the **Windows** button.
2. Click the **dropdown** next to the 7-Zip folder.
3. Confirm the **7-Zip File Manager.exe** has installed on the device.
4. You may also notice that the **7-Zip File Manager.exe** has been added to the Recently Added list at the top of the start menu.
This confirms that you were able to successfully export the application details from SCCM, import the application into Workspace ONE UEM and then assign and install the application to your devices.
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your **Username**. This is your **email address** that you have associated with your **VMware Learning Platform (VLP) account**.
2. Enter **VMware1!** for the **Password** field.
3. Click the **Login** button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If you are licensing the Software for evaluation purposes, your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

Security Settings

Password Recovery Question 1

Password Recovery Question *

Password Recovery Answer *

Confirm Password Recovery Answer *

Password Recovery Question

What was your childhood nickname? 2

Password Recovery Answer

VMware1! 3

Confirm Password Recovery Answer

VMware1! 4

Security PIN

A four-digit Security PIN must be entered. It is required in the console for some restricted actions (configured by authorized administrators in System Security settings).

Security PIN *

1234 5

Confirm Security PIN *

1234 6

Save

After accepting the Terms of Use, you will be presented with a Security Settings popup. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter **VMware1!** in the Password Recovery Answer field.
4. Enter **VMware1!** in the Confirm Password Recovery Answer field.
5. Enter **1234** in the Security PIN field.
6. Enter **1234** in the Confirm Security PIN field.
7. Click the Save button when finished.

**Close the Welcome Message**

**Workspace ONE UEM Console Highlights**

**Powered by VMware AirWatch!**

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from Workspace ONE UEM console, also known as managed content.

Delete Device from Workspace ONE UEM Console

From the Workspace ONE UEM Console,

1. Click on Devices
2. Click on List View
3. Select the check box next to your device friendly name.
4. Click on More Actions
5. Click on Delete Device
Enter Reason and Delete

1. Enter the reason as **lab completed**.
2. Click on **Delete**.
Validate DELETE IN PROGRESS...

List View

1. You may see device friendly name changing to DELETE IN PROGRESS...
2. Click on the Refresh Icon to validate if the device deletion is successful.

Ensure that device record is deleted

List View

1. Use the Refresh Button if needed.
2. Ensure that the device record is now deleted from the Workspace ONE UEM console and you see the message No Records Found.
Navigate to Windows 10 Settings

1. Click on the Windows Icon
2. Click on the gear icon to access Windows 10 Settings

Access Accounts Settings

From the Settings Menu, access Accounts
Validate That No Management Account Exists

1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to **AirWatchMDM**.

**NOTE** - The CORP AD domain is the local domain in this lab and is not controlled by AirWatch Enrollment, so you will see this connection if your device is enrolled or unenrolled.
Conclusion

This module reviewed how to utilize AirLift to quickly migrate your desired application from SCCM to Workspace ONE UEM and how to deploy this application to your devices and users.
Introduction

In this module, you will migrate your Group Policy Objects (GPOs) to VMware AirWatch and assign those GPOs to users and devices.

This module contains the following lessons:

• Download and Run AirWatch GPO Migration Tool
• Upload GPOs to AirWatch
• Assign and Test GPO App Package
• Enroll Windows 10 Device
• Verify GPO App Package Installation
Connect to the SCCM Server

Double-click **sccm-01a.rdp** from the Main Console desktop.

*NOTE - The files and resources required to complete this lab are on the sccm-01a server! Please ensure you connect and remain connected until instructed to change servers to complete the lab!*
Login to the Workspace ONE UEM Console

To perform most of the lab, you will need to login to the Workspace ONE UEM Admin Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Admin Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your Username. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter VMware1! for the Password field.
3. Click the Login button.

**NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.**
Accept the End User License Agreement

Terms of Use

You must accept the following VMware End User License Agreement to use Workspace ONE UEM.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls

NOTE - The following steps of logging into the Administration Console will only need to be done during the initial login to the console.

You will be presented with the Workspace ONE UEM Terms of Use. Click the Accept button.
Address the Initial Security Settings

After accepting the Terms of Use, you will be presented with a Security Settings pop-up. The Password Recovery Question is in case you forget your admin password and the Security PIN is to protect certain administrative functionality in the console.
1. You may need to scroll down to see the Password Recovery Questions and Security PIN sections.
2. Select a question from the Password Recovery Question drop-down (default selected question is ok here).
3. Enter VMware1! in the Password Recovery Answer field.
4. Enter VMware1! in the Confirm Password Recovery Answer field.
5. Enter 1234 in the Security PIN field.
6. Enter 1234 in the Confirm Security PIN field.
7. Click the Save button when finished.

Close the Welcome Message

Workspace ONE UEM Console Highlights

Powered by VMware AirWatch!

Workspace ONE is powered by VMware AirWatch Unified Endpoint Management (UEM) technology, a unified digital workspace platform delivering a single, secure experience for app management, single sign-on (SSO), and conditional access.

Workspace ONE UEM transforms your business so you can:

- Configure, manage and support devices from any endpoint
- Increase productivity with seamless access to any app
- Safeguard company data at every layer
- Access identity and access management tools with ease
- Enjoy a simplified, consistent look and feel across Workspace ONE

Don't show this message on login
After completing the Security Settings, you will be presented with the Workspace ONE UEM Console Highlights pop-up.

1. Click on the **Don't show this message on login** check box.
2. Close the pop-up by clicking on the X in the upper-right corner.
Execute the AirWatch GPO Migration Tool

The bulk of this exercise will be completed from the SCCM Server, where we will utilize the AirWatch GPO Migration Tool to deploy our modified local policies to other devices.

We will now execute the GPO Migration script to deploy our modified local policies to other devices via AirWatch.

The GPO Migration script has already been downloaded and included for you on the Desktop of your SCCM Server under the GPO Migration folder. Outside of the lab, this script is available for download at https://code.vmware.com/samples.

Setup the GPO Migration PowerShell Script
1. Click the **File Explorer** icon from the task bar.
2. Click **Documents**.
3. Click **HOL**.
4. Click **GPO Migration**.
5. Right-click the **Migrate-GPO-AirWatch.ps1** file.
6. Click **Run with Powershell**.

**Note the LGPO.exe Requirement**

1. Notice that the PowerShell terminal outputs a warning stating that the LGPO.exe file is required. LGPO.exe will be utilized to capture and package your local policies, so our first step will be to download the LGPO.exe from the provided link.
2. The link to the Microsoft Security Compliance Toolkit is available in the output for easy reference.
3. Click **Close** for the Windows PowerShell window.

For the purposes of this exercise, the LGPO.exe file has already been downloaded for you. You will now move the LGPO.exe file into the project folder as you would need to do when downloading the tool to meet the dependency requirements.
Copy the LGPO.exe File to the GPO Tool Folder

NOTE - The LGPO.exe file is only available on the sccm-01a server! If you are not connected to the sccm-01a server, please refer to the instructions at the beginning of the lab for how to connect and continue with these steps once you have connected!

1. Click the **File Explorer** icon from the task bar.
2. Click **Documents**.
3. Click **HOL**.
4. Click **LGPO**.
5. Right-click the **LGPO.exe** file.
6. Click **Copy**.

```markdown
NOTE - The LGPO.exe file is only available on the sccm-01a server! If you are not connected to the sccm-01a server, please refer to the instructions at the beginning of the lab for how to connect and continue with these steps once you have connected!

1. Click the **File Explorer** icon from the task bar.
2. Click **Documents**.
3. Click **HOL**.
4. Click **LGPO**.
5. Right-click the **LGPO.exe** file.
6. Click **Copy**.
```
Paste the LGPO.exe file in the GPO Migration Folder

1. Click the GPO Migration folder.
2. Right-click within the folder and click **Paste**.
Execute the GPO Migration PowerShell Script After Setup

1. Confirm that the **LGPO.exe** file exists in the GPO Migration folder now alongside Migrate-GPO-AirWatch.ps1.
2. Right-click the **Migrate-GPO-AirWatch.ps1** file.
3. Click **Run with PowerShell**.

Confirm GPO Migration PowerShell Script Starts Successfully

Once the LGPO.exe file is included, the GPO Migration script will initialize and present the Task selection input for further use. Confirm that you no longer see output.
prompting for the LGPO.exe file to be included in the folder and then continue to the next step.

Modify Local GPO Settings

Before proceeding, we will modify our local GPO so that we can capture and distribute these changes to other devices to confirm that our deploy was successful.

1. Right-click the Windows icon.
2. Click Run.

Launch Local Group Policy Editor
You will launch the Local Group Policy Editor to make the policy changes.

1. Enter `gpedit.msc`.
2. Click OK

**Navigate to the Active Power Plan Settings**

1. Click **Computer Configuration**.
2. Click **Administrative Templates**.
3. Click **System**.
4. Click **Power Management**.
5. Double-click the **Select an Active Power Plan** policy.
Select Active Power Plan

1. Select **Enabled**.
2. Select **High Performance** as the Active Power Plan.
3. Click **OK**.

We will use this local GPO as a reference on our enrolled devices to ensure that our captured policies applied correctly.
Capture GPO Backups

1. Return to the PowerShell Terminal by clicking **PowerShell** icon on the task bar.
2. At the Task prompt, enter `2` and press **ENTER**.
3. Confirm that the output shows that the local GPO was captured after task finishes.

View GPO Backups

From the PowerShell prompt, enter `1` and press **ENTER** to view the list of GPO backups.
Confirm Captured GPO Backup Displays

1. Any captured or copied GPO backups placed in the expected directory (\GPO Backups) are displayed here. Notice that the GPO backup you just took is available in this list.
2. Click OK to close the window.

Using External GPO Backups

If you have previously captured GPO backups that you want to use with this tool, you can include these in the \GPO Backups folder of the root directory of the GPO Migration tool. Any GPO backups available in the \GPO Backups folder will display as selectable GPOs for Option 1 (Viewing GPOs) and option 3 (Uploading GPOs to AirWatch).
Copy the Existing Security GPO Backups

1. Click the File Explorer icon from the task bar.
2. Click Documents.
3. Click HOL.
5. Select all of the folders within the Security GPO Backups folder and right-click.
6. Click Copy.
Paste the Security GPO Backups in the GPO Backups folder

1. Click **GPO Migration**.
2. Click **GPO Backups**.
3. **Right-click** within the GPO Backups folder.
4. Click **Paste** to insert the Security GPO Backup folders that were previously copied.
View GPO Backups from the Tool

1. Return to the PowerShell Terminal by clicking **PowerShell** icon on the task bar.
2. At the Task prompt, enter **1** and press **ENTER** to view the list of available GPO Backups again.

Confirm the Security GPO Backups Are Listed
1. Confirm that the 4 Security GPO Backups that were copied into the GPO Backups folder now display alongside the local GPO capture that was taken previously for a total of 5 GPO Backups.
2. Click **OK** to close the dialog.
Upload GPO Package to Workspace ONE UEM

With a range of GPO backups now available, we can use the GPO migration tool to upload the package to Workspace ONE UEM for distribution. This exercise will cover selecting a GPO package to upload to the Workspace ONE UEM Console that we can distribute to our devices.

**Uploading GPOs to Workspace ONE UEM**

1. Return to the PowerShell terminal by clicking the PowerShell icon from the task bar.
2. For the Task selection, enter `3` to Upload the GPO to AirWatch and press **ENTER**.
3. Enter `https://labs.awmdm.com` for the awServer and press **ENTER**.
4. Enter your email address for the awUsername and press **ENTER**. This is the same username you used to login to the Workspace ONE UEM Console in previous steps.
5. Enter `VMware1!` for the awPassword and press **ENTER**.

Continue to the next step for instructions on obtaining the remaining parameter values from the Workspace ONE UEM Console (awTenantAPIKey and awGroupId).
Navigate to the Workspace ONE UEM Administration Console

1. Click Chrome icon from the task bar.
2. From the Workspace ONE UEM Console, click Groups & Settings.
3. Click All Settings.
Retrieve the REST API Key

1. Click System.
2. Click Advanced.
3. Click API.
4. Click REST API.
5. Click and drag or double-click to highlight the API Key text for the AirWatchAPI service.
6. Right-click and select Copy.
7. Click Close to exit the REST API menu.

Paste the Copied API Key

HOL-1957-04-UEM
1. Return to the PowerShell Terminal by clicking the **PowerShell** icon from the task bar.
2. Paste the copied API Key for the `awTenantAPIKey` parameter by **right-clicking**, then press **ENTER**.

**Retrieve the Organization Group Numerical ID**

1. Click **Groups & Settings**.
2. Click **Groups**.
3. Click **Organization Groups**.
4. Click **Details**.

Return to the Workspace ONE UEM Console.

1. Click **Groups & Settings**.
2. Click **Groups**.
3. Click **Organization Groups**.
4. Click **Details**.
5. The numerical ID at the end of the URL is your **Organization Group Numerical ID**. Highlight this text and **right-click**.

6. Click **Copy**.

**Paste the Copied Organization Group Numerical ID**

![Image showing the copied Organization Group Numerical ID]

1. Return to the PowerShell Terminal by clicking the **PowerShell** icon from the task bar.
2. Paste the copied Organization Group Numerical ID for the awGroupId parameter by **right-clicking**, then press **ENTER**.

**Wait for API Authentication**

![Image showing the API authentication status]

After inputting the connection details, a prompt will be displayed stating **Confirming AirWatch API authentication... this may take a few moments**. This process will check that the API Authentication was successful and that the Group ID provided exists and can be accessed with the provided API Key.

Once this completes, you will be presented with a popup to select the GPO Backup for Upload. Continue to the next step.
Select GPO to Upload

1. Select the GPO you captured in the previous steps. This GPO is in the format `GPO <machinename> <date> <time>`.

2. Click **OK**.

A series of loading tasks will begin to run, notated by the progress bars at the top of the PowerShell terminal. These will inform you what step the process is currently on.
Confirm the GPO Package App was uploaded to the Workspace ONE UEM Console Successfully

When the process has completed successfully, you should see the following text:

```
Successfully saved GPO package app to the AirWatch Console!

----- IMPORTANT ----- 
Be sure to navigate to the AirWatch Console and assign the application '{filename}' to the appropriate users and devices!
----- IMPORTANT ----- 
```

The app is now uploaded to the Workspace ONE UEM Console and is ready for assignment. You will assign this package to a device in an upcoming exercise.

NOTE: If you are uploading multiple GPOs in a single package, they will be applied to enrolled devices in the order in which they are selected from the Select GPO Backups to Upload prompt. If the order of the GPOs matters for your deployment, ensure you select them in the intended order!
Assign GPO Package

After the GPO app package is uploaded using the tool, the final step is to add assignments to deploy to the users and/or devices that you designate.

Assign GPO App Package

Return to the Workspace ONE UEM Console,

1. Click **Apps & Books**.
2. Click **Applications**.
3. Click **Native**.
4. Click the **Internal** tab.
5. Select the GPO package uploaded in the previous exercise. The name format will be `GPO <machinename> <date> <time>.zip`.
6. Click **Assign**.
Click **Add Assignment**.

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the group with highest priority (0 being highest priority).
Update the App Assignment Details

1. Select All Devices (your@email.shown.here) for the Select Assignment Groups field.
2. Select Auto for the App Delivery Method.
3. Click Add.
Save & Publish

Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

Click **Save & Publish**.
Publish the GPO App Package

Click Publish.

After the GPO app package has been assigned to all devices, the next step is to enroll your Windows 10 device. Proceed to the next exercise to enroll your Windows 10 device.
Remote Desktop to your Windows 10 Device for Enrollment

Close the RDP session to the SCCM Server by clicking the **Close** button (X) on the Remote Desktop Connection tab at the top of your screen.

**NOTE:** If this blue tab does not appear, you may have unpinned this from displaying at the top. Hover your mouse near the top of the screen to show the tab.

Connect to the Windows 10 VM

From the Desktop of the Main Console, double-click the **Win10-01a.rdp** shortcut.

This Windows 10 device will be used to enroll and test our uploaded GPO package.

Open Google Chrome

Double-click the **Google Chrome** shortcut on the desktop.
Modifying Internet Options for Windows Enrollment

Before enrolling the Windows 10 Virtual Machine, we will make modifications to the Windows 10 device to reduce network traffic to expedite enrollment.

Open Settings

1. Click the **Windows** button.
2. Click the **Settings (Gear)** icon.
Open Internet Options

1. Type **Internet Options** in the search bar.
2. Click **Internet Options** from the results list.
Modify the Certificate Revocation Options

1. Click the **Advanced** tab.
2. Scroll down to find the **Security** section.
3. **Uncheck** the **Check for publisher's certificate revocation** option.
4. **Uncheck** the **Check for server certificate revocation** option.
5. Click **Apply**.
6. Click **OK**.
Open PowerShell as Administrator

1. Right-Click the Windows button.
2. Click Windows PowerShell (Admin).
Allow WindowsPowerShell to Make Changes

Click Yes when prompted to allow Windows PowerShell to make changes to your device.

Enter Commands to Stop Windows Update Service

1. Enter `Set-Service wuauserv -startup disabled` then press ENTER.
2. Enter `Stop-Service wuauserv` then press ENTER.
3. Click the Close button to exit PowerShell.
Enrolling Your Windows 10 Device

We will now enroll our Windows 10 device in Workspace ONE UEM. First, we will need to download the Workspace ONE Intelligent Hub.

Download the Workspace ONE Intelligent Hub on the Windows 10 VM

From a new tab in the browser, if not opened already,

2. Click **Download Hub for Windows 10**.  
   **NOTE:** Please wait while the Workspace ONE Intelligent Hub installer finishes downloading.
3. Click **Keep** when warned about the AirWatchAgent.msi download.

**NOTE - If you do not see the warning about the AirWatchAgent.msi file, skip this and continue to the next step.**

**Launch the Workspace ONE Intelligent Hub Installer**

Click the AirWatchAgent.msi file in your download bar.

**NOTE - The installer may take a few seconds to launch, please be patient after clicking the AirWatchAgent.msi file.**

**Click Run**

Click **Run** to proceed with the installation.
Accept the Default Install Location

Leave the default install location and click **Next**.

*NOTE - The Next button may take several seconds to enable while the required additional features are installed.*
Accept the License Agreement

1. Select I accept the terms of the license agreement.
2. Click Next.
Start the Workspace ONE Intelligent Hub Install

Click **Install** to start the installer.
Allow the Workspace ONE Intelligent Hub Installer to Run (IF NEEDED)

If prompted to allow the app to make changes on your device, click Yes.
Complete the Workspace ONE Intelligent Hub Installer

Click **Finish** to complete the Workspace ONE Intelligent Hub installer.

*NOTE - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into Workspace ONE UEM. It will take around 45-60 seconds to launch the agent.*
Enroll Your Windows 10 Device Using the Workspace ONE Intelligent Hub

Click **Server Detail**.

**Find your Group ID from Workspace ONE UEM Console**

1. **your@email.shown.here**
2. **yourid1234**
The first step is to make sure you know what your **Organization Group ID** is.

1. To find the Group ID, hover your mouse over the Organization Group tab at the top of the screen. Look for the email address you used to log in to the lab portal.
2. Your **Group ID** is displayed at the bottom of the Organization Group pop up.

**Enter the Server Details**

1. Enter **labs.awmdm.com** for the **Server Name** field.
2. Enter **Your Group ID** for the **Group ID** field. If you forgot your Group ID, check the previous steps on how to retrieve it.
Enter Your User Credentials

1. Enter **aduser** in the **Username** field.
2. Enter **VMware1!** in the **Password** field.
3. Click **Next**

**NOTE - Wait while the server checks your enrollment details.**
Since our Workspace ONE UEM and VMware Identity Manager environments are linked for this environment, the Workspace ONE Application will automatically open after enrollment is complete. You will not need it for this exercise, so click Close.
Finish the Workspace ONE UEM Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into Workspace ONE UEM.
Login to the Workspace ONE UEM Console (IF NEEDED)

To perform most of the lab you will need to login to the Workspace ONE UEM Management Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.
Authenticate to the Workspace ONE UEM Administration Console

The default home page for the browser is https://labs.awmdm.com. Enter your Workspace ONE UEM Admin Account information and click the Login button.

**NOTE - If you see a Captcha, please be aware that it is case sensitive!**

1. Enter your Username. This is your email address that you have associated with your VMware Learning Platform (VLP) account.
2. Enter VMware1! for the Password field.
3. Click the Login button.
NOTE - Due to lab restrictions, you may need to wait here for a minute or so while the Hands On Lab contacts the Workspace ONE UEM Hands On Labs server.
Verify GPO App Package Installed

With the application uploaded, assigned, and enrolled, we will now verify that the GPO app package is applied successfully to our enrolled device.

Verify the App Package Installed from the Workspace ONE UEM Console

1. Click Apps & Books.
2. Click Applications.
3. Click Native.
4. Click the Internal tab.
5. Click the uploaded GPO App Package. This will be in the name format `GPO <machinename> <date> <time>.zip`.

This will open the Details View page of the GPO App Package, allowing you to see additional details about the application.
Verify the Install Status of the GPO App Package

1. The **Install Status** section confirms how many devices have installed the application. You will likely see **1 Not Installed** when navigating here since you just enrolled your Windows 10 device and it has not had sufficient time to receive the install command yet.

2. The **Deployment Progress** section confirms which devices the app is assigned to, as well as the status and deployment configurations.

3. Click the **Devices** tab.
Send the Install Command to the Device (IF NEEDED)

To expedite the device receiving the install command for this lab, you will send the install command manually from the console.

1. Check the Install Status and Reason of your device. If you see Install Command Ready for Device for the Reason, that means the device has not received the install command yet. If the Install Status shows Installed already, you can skip to the next step.
2. Click the checkbox to select the device.
3. Click Install.
Confirm the Application Install Command (IF NEEEDED)

Click **OK** to confirm the application install command.

**Confirm the Install Command was Dispatched**

1. Confirm the Reason now shows Install Command Dispatched. This means the command has been sent to the device and is waiting to be processed.
2. Click **Refresh**. You should refresh periodically every 1-2 minutes until the Install Status or Reason updates.
Confirm the Application Installed

Confirm that the Install Status shows **Installed**.

**NOTE:** If you do not see the **Installed** status, you may need to continue refreshing. The application may take several minutes to download and deploy to the device before it reports as Installed.
Open Group Policy Editor

1. In Windows Search, enter `gpedit.msc`.
2. Click `gpedit.msc`. 
Allow Microsoft Management Console to Make Changes to Device (IF NEEDED)

If you are prompted to allow the Microsoft Management Console to make changes to your device, click Yes.

If you do not see this prompt, continue to the next step.

Navigate to Power Management Settings

1. Click Computer Configuration.
2. Click Administrative Templates.
3. Click System.
Open the Active Power Plan Settings

Double-click **Select an active power plan**.
Confirm Policy Settings

1. Confirm that the policy is **Enabled** and that the Active Power Plan is set to **High Performance**. These settings were applied by our GPO application package that was sent to our device.

2. Click **Close**.
Confirm Power and Sleep Settings

1. Right-click the Windows button.
2. Click Power Options.
Navigate to Additional Power Settings

Click **Additional power settings**.
Confirm the Power Options Settings shows High Performance

1. Confirm that the set plan is set to **High Performance**.
2. You should also see a notification above the power plans stating **Change settings that are currently unavailable**. Clicking this message will show that the settings are unavailable to change because they are being controlled by the system administrator through the policies we packaged and deployed through Workspace ONE UEM.

This shows how you can capture and export GPOs from one device and quickly apply the same settings to another device without the need to create profiles or policies manually.
Un-enrolling your Windows 10 Device

In this section, we are going to un-enroll our Windows 10 VM so that we can use it for other lab modules. We will delete the device record from the console, which will also un-enroll the device and remove all the apps and profiles that are pushed from Workspace ONE UEM console, also known as managed content.

Delete Device from Workspace ONE UEM Console

From the Workspace ONE UEM Console,

1. Click on **Devices**
2. Click on **List View**
3. Select the check box next to your device friendly name.
4. Click on **More Actions**
5. Click on **Delete Device**
Enter Reason and Delete

1. Enter the reason as **lab completed**.
2. Click on **Delete**
Validate DELETE IN PROGRESS...

1. You may see device friendly name changing to DELETE IN PROGRESS...
2. Click on the Refresh Icon to validate if the device deletion is successful.

Ensure that device record is deleted

1. Use the Refresh Button if needed.
2. Ensure that the device record is now deleted from the Workspace ONE UEM console and you see the message No Records Found.
Navigate to Windows 10 Settings

1. Click on the Windows Icon
2. Click on the gear icon to access Windows 10 Settings

Access Accounts Settings

From the Settings Menu, access Accounts
Validate That No Management Account Exists

1. Click on **Access work or school**
2. Validate that you DO NOT see any account connected to **AirWatchMDM**.

**NOTE** - The CORP AD domain is the local domain in this lab and is not controlled by AirWatch Enrollment, so you will see this connection if your device is enrolled or unenrolled.
Conclusion

Lab Conclusion

You have successfully completed the SCCM Migration lab.

In this lab, we covered migrating users and devices from SCCM to AirWatch, migrating applications from SCCM to AirWatch, and using the AirWatch GPO migration tool.

This concludes the SCCM Migration hands-on lab.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1957-04-UEM

Version: 20190430-172844