# Table of Contents

Lab Overview - HOL-1857-02-UEM - Workspace ONE UEM - Management for Windows 10 .......................................................... 2

Lab Guidance .......................................................................................................................................................................................... 3

Module 1 - Windows 10 Software Distribution and Troubleshooting (45 minutes) ................................................................. 9

Introduction............................................................................................................................................................................................ 10

Connect to Windows 10 VM ......................................................................................................................................................... 12
Login to the AirWatch Console ...................................................................................................................................................... 13
Enrolling Your Windows 10 Device ........................................................................................................................................... 17
Deploying Notepad++ ................................................................................................................................................................. 28
Confirm the aduser Certificate Has Installed ............................................................................................................................... 47
Login to the Workspace ONE Application ....................................................................................................................................... 53
Verify Notepad++ Deployment ..................................................................................................................................................... 56
Deploying Office 365 ProPlus ....................................................................................................................................................... 74
Verifying Office 365 Pro Plus Deployment ................................................................................................................................... 98
Un-enrolling your Windows 10 Device ....................................................................................................................................... 111
Sign Out of the Workspace ONE Application ................................................................................................................................ 116
Close Chrome to Clear Session Cookies ...................................................................................................................................... 118

Module 2 - Windows 10 Real-Time and Automated Security Protection and Compliance (45 Minutes) ................................................................. 120

Introduction............................................................................................................................................................................................ 121
Connect to Windows 10 VM ......................................................................................................................................................... 122
Login to the AirWatch Console ...................................................................................................................................................... 123
Device Posture and Real-Time Compliance ................................................................................................................................... 127
Conditional Access ........................................................................................................................................................................... 130
Enrolling Your Windows 10 Device ............................................................................................................................................... 135
Confirm the aduser Certificate Has Installed ............................................................................................................................... 146
Compliance with Workspace ONE .................................................................................................................................................. 152
Login to the Workspace ONE Application ....................................................................................................................................... 153
Confirm Successful Login to the Workspace ONE App .................................................................................................................. 156
Sign Out of the Workspace ONE Application .................................................................................................................................... 157
Create a Compliance Rule ............................................................................................................................................................ 159
Data Loss Prevention ......................................................................................................................................................................... 172
Un-enrolling your Windows 10 Device ........................................................................................................................................... 174
Remove the Compliance Policy .................................................................................................................................................... 179
Close Chrome to Clear Session Cookies ....................................................................................................................................... 180
Conclusion........................................................................................................................................................................................... 181
Lab Guidance

NOTE - It may take more than 90 minutes to complete this lab. You should expect to only finish 1-2 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.

The Unified Endpoint Management for Windows 10 lab is designed to dive deeper into the aspects of managing, securing, and configuring Windows 10 devices. Each Module can be taken independently or you can start at the beginning and work your way through each module in sequence. In most cases, a unique "sandbox" instance of AirWatch will be created just for you when you begin a Module. When the Module has ended, this sandbox will be deleted and the device that you are enrolling in the lab will be returned to the state that it was in prior to the lab. The approximate time it will take to go through all the modules is around 2 hours.

Lab Module List:

- **Module 1 - Windows 10 Software Distribution and Troubleshooting** (45 minutes) (Basic) Utilize Software Distribution in AirWatch to configure and deploy Notepad++ and Office 365 to Windows 10 devices.

- **Module 2 - Windows 10 Real-Time and Automated Security Protection and Compliance** (45 minutes) (Basic) Use VMware AirWatch Unified Endpoint Management to establish user trust, assess device posture, enforce conditional access and enable data loss prevention.

- **Lab Captains - All modules: Roger Deane, Shardul Navare, Justin Sheets.**

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:

Location of the Main Console

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 - Windows 10
Software Distribution and Troubleshooting (45 minutes)
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. VMware AirWatch on Windows 10 introduces features and tools to simplify application integration and management.

Software Distribution and Lifecycle Flow with VMware AirWatch

You can deploy Win32 applications from the Apps & Books section of the AirWatch 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 VMware AirWatch 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 Win10-01.rdp shortcut on the lab desktop.

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

- Username: corp\administrator
- Password: VMware1!
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.

Authenticate to the AirWatch Administration Console

Username
Your VLP Email Address

Password
VMware1!

Login

Trouble Logging In
The default home page for the browser is https://hol.awmdm.com. Enter your AirWatch 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 AirWatch Hands On Labs server.**

**Accept the End User License Agreement**

You must accept the following AirWatch software license agreement to use AirWatch Mobile Device Management.

**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 AirWatch 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. Save the settings.
7. Click the **Save** button when finished.

**Close the Welcome Message**

After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

1. Click on the **Don't show this message again** check box.
2. Close the pop-up by clicking on the **X** in the upper-right corner.
Enrolling Your Windows 10 Device

We will now enroll our Windows 10 device in AirWatch. First, we will need to download the AirWatch Agent.

Download AirWatch Agent

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

2. Click **Download**.
   *NOTE* - Please wait while the AirWatch Agent 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 AirWatch Agent 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.

**Ignore Windows SmartScreen**

Due to Firewall restrictions, Windows SmartScreen won't be available in the lab network. Click **Run** to continue.

*NOTE* - Windows SmartScreen may take several seconds to display after clicking the AirWatchAgent.msi
Install Additional Required Features

If any required features are missing, you will be prompted that the installer will install them for you. Click **OK** to continue.

Click the Additional Features Installer

The additional features that need to be installed will begin, click the flashing installer icon from your bottom toolbar.
Allow the Additional Features To Be Installed

Click **Yes** when asked if you wish to allow the application to make changes.

*NOTE - You may see the installer pause while this process completes. Please be patient, the installer when continue when it is finished.*

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 AirWatch Agent Install

Click **Install** to start the installer.

Allow the AirWatch Agent to Make Changes

Click **Yes** when prompted if you should allow the AirWatch Agent to make changes.
Complete the AirWatch Agent Installer

Click **Finish** to complete the AirWatch Agent installer.

**NOTE - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into AirWatch. If it does not show up immediately, wait a moment for the next prompt to appear.**

Allow the NativeEnrollment Application to Make Changes

Click **Yes** when asked if you want to allow the NativeEnrollment app to make changes.
Enroll Your Windows 10 Device Using the AirWatch Agent

Click **Server Detail**.

**Find your Group ID from AirWatch Console**

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.
NOTE - The Group ID is required when enrolling your device in the following steps.

Enter the Server Details

1. Enter "hol.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.**
Finish the AirWatch Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into AirWatch.
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 AirWatch**

1. Click **Apps & Books**.
2. Click **Applications**.
3. Click **Native**.
4. Click the **Internal** tab.
5. Click **Add Application**.

**Upload Application File**
Click **Upload**.

**Choose Application File to Upload**

![Choose File](image)

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

1. Click **Documents**.
2. Click **HOL**.
3. Click **Windows 10**.
4. Click **Notepad++ Installer.exe**.
5. 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 **MB** for the RAM Required Units.
Configure Install Options

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.
4. Select **Defining Criteria** for Identity Application By.
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 **Windows 10**.
4. Click **Notepad++.png**.
5. 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

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

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

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

1. Click **Apps & Books**.
2. Click **Applications**.
3. Click **Native**.
4. Click **Internal** tab.
5. Ensure the **Notepad++** application was added successfully.
**Confirm the aduser Certificate Has Installed**

We have configured a 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 AirWatch 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 Win 10 - 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. You may need to scroll to the right to find the **Refresh** button.
2. Click **Refresh**.
3. 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

1. The server address "https://ws1user.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 Next.

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.*
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. Click Catalog.
2. Ensure the Notepad++ app displays and shows as Installed.
3. 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.
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 AirWatch 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 AirWatch Console,

1. Click **Apps & Books**.
2. Click **Applications**.
3. Click **Native**.
4. Click **Internal**.
5. Click **Notepad++**.

---

VMware AirWatch - Unified Endpoint Management for Windows 10
Additional Information and Troubleshooting in the AirWatch 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 AirWatch Console.

In the AirWatch Console,

1. Click **Apps & Books**.
2. Click **Applications**.
3. Click **Native**.
4. Click **Internal**.
5. 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 "C:\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 AirWatch 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 AirWatch Console to find the correct cache is an important step in debugging the correct deployment.
Obtain Access to the Application Cache Folder

Click Continue.

Enable User Account Control

Click Yes to allow User Account Control.
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 AirWatch 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. Begin typing, 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**.
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 AirWatch Console from the Deployment Options tab of your application.
- **ContentManifests** contains information about the options set in the AirWatch 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:

```
DEPLOYMENT_OPERATION_QUEUED = 0x000,
FIRST_DETECTION_INPROGRESS = 0x100,
FIRST_DETECTION_FAILED,
FIRST_DETECTION_SUCCESSFUL,
CHECK_REFERENCE_COUNT_INPROGRESS = 0x200,
CHECK_REFERENCE_COUNT_FAILED,
CHECK_REFERENCE_COUNT_SUCCESSFUL,
REQUIREMENTS_EVALUATION_INPROGRESS = 0x300,
REQUIREMENTS_EVALUATION_FAILED,
REQUIREMENTS_EVALUATION_SUCCESSFUL,
DEPENDENCIES_INPROGRESS = 0x400,
DEPENDENCIES_FAILED,
```
Conclusion

There are several ways to debug a failed or erroneous Software Distribution deployment, as we have reviewed. The AirWatch 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 AirWatch Console, we need to prepare and zip the files.

Open File Explorer

From the bottom toolbar, click the Folder icon to launch Explorer.

Package the Office 365 Files as a Zip
1. Expand the Documents folder under This PC.
2. Expand the HOL folder.
3. Click the Windows 10 folder.
4. Sort by Date Modified
5. Select the configuration.xml and setup.exe files (click + drag over both, or ctrl + click both files) and right-click.
6. Hover over Send to.
7. Click Compressed (zipped) folder.

**Rename the Zipped Folder**

[Image of zipped folder]

Rename the zipped folder to "**Office365ProPlus.zip**".

**NOTE** - If you accidentally cancelled 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 AirWatch**

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 AirWatch Console.

**Add an Internal Application**

Back in the AirWatch Console,

1. Click Apps & Books.
2. Expand Applications.
3. Click Native.
4. Click the Internal tab.
5. Click Add Application.

---

**VMware AirWatch - Unified Endpoint Management for Windows 10**

Page 77
Upload the Application File

Click **Upload**.

Choose the File to Upload

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

1. Expand the Documents folder under This PC.
2. Expand the HOL folder.
3. Click the Windows 10 folder.
4. Click to select the Office365ProPlus.zip file.
5. Click Open.
Save the Uploaded File

Click **Save**.
Continue after Saving the File

1. Select No for "Is this a dependency file?"
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**.
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 "60" 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**.
Add the Identify Application By Criteria

1. Select **File Exists** for the **Criteria Type**.
2. Enter `C:\Program Files (x86)\Microsoft Office\root\Office16` for the **Path**.
3. 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.
Configure Images

1. Click the **Images** tab.
2. Click the **Icon** tab.
3. Click the area labelled "Click or drag files here".
Select the O365 Logo for the Icon

1. Expand the Documents folder under This PC.
2. Expand the HOL folder.
3. Click the Windows 10 folder.
4. Click the o365-logo.jpg file to select it.
5. 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

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

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 AirWatch for deployment. Remember that AirWatch supports uploading and deploying MSIs, EXEs, as well as packaged apps like the zipped file we uploaded in this lab.

**AirWatch 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.

Now that the Office 365 application is configured and deployed, the next step is to enroll the Windows 10 Virtual Machine into AirWatch using the AirWatch Agent. This will allow AirWatch to determine if the device should receive the Office 365 Pro Plus application we configured and prompt the Windows 10 device to begin installing the 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

[Image of VMware Workspace ONE interface showing the Office 365 ProPlus app in the Catalog with a status of "Installing".]
Within the Workspace ONE application:

1. Click **Refresh** icon
2. Click **Catalog**.
3. Notice that the **Office 365 ProPlus** application you configured within AirWatch 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 AirWatch Console,

1. Click **Apps & Books**
2. Expand **Applications**.
3. Click **Native**.
4. Click the **Internal** tab.
5. 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.
Application Devices View

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. Search for **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! 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 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 AirWatch Console in a real deployment.**
Navigate to the Details View of the Internal Application (follow along)

1. Click **Apps & Books**.
2. Expand **Applications**.
3. Click **Native**.
4. Click the **Internal** tab.
5. Click the "**Office 365 Pro Plus**" application you deployed.

**NOTE - As mentioned before, the Office 365 Pro Plus installation 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 AirWatch 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 AirWatch 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 AirWatch 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 AirWatch 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 AirWatch console, also known as managed content.

Delete Device from AirWatch Console

From the AirWatch 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 AirWatch 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 device management or other types.
Sign Out of the Workspace ONE Application

Within the Workspace ONE application,

1. Click the User Icon
2. 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 the 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.

This concludes the Deploying Office 365 Pro Plus module.
Module 2 - Windows 10
Real-Time and Automated
Security Protection and
Compliance (45 Minutes)
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 VMware AirWatch Unified Endpoint Management’s 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 VMware AirWatch Unified Endpoint Management 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 Win10-01.rdp shortcut on the lab desktop.

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

- Username: corp\administrator
- Password: VMware1!
Login to the AirWatch Console

To perform most of the lab you will need to login to the AirWatch Management Console.

Launch Chrome Browser

Double-click the Chrome Browser on the lab desktop.

Authenticate to the AirWatch Administration Console

Username
Your VLP Email Address

Password
VMware1!

Login

Trouble Logging In
The default home page for the browser is https://hol.awmdm.com. Enter your AirWatch 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 AirWatch Hands On Labs server.**

**Accept the End User License Agreement**

![End User License Agreement](image)

**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 AirWatch Terms of Use. Click the **Accept** button.
# Address the Initial Security Settings

## Security Settings

<table>
<thead>
<tr>
<th>Security Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Recovery Question</strong></td>
<td><strong>What was your childhood nickname?</strong></td>
</tr>
<tr>
<td><strong>Password Recovery Answer</strong></td>
<td><strong>VMware1!</strong></td>
</tr>
<tr>
<td><strong>Confirm Password Recovery Answer</strong></td>
<td><strong>VMware1!</strong></td>
</tr>
<tr>
<td><strong>Security PIN</strong></td>
<td><strong>1234</strong></td>
</tr>
<tr>
<td><strong>Confirm Security PIN</strong></td>
<td><strong>1234</strong></td>
</tr>
</tbody>
</table>

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**

After completing the Security Settings, you will be presented with the AirWatch Console Welcome pop-up.

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

VMware AirWatch assesses device posture by evaluating, locally enforcing, and remediating devices using the compliance engine, a VMware AirWatch 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. Verify that **Secure Boot Disabled** is **Checked** under the Compromised Status Definition section is checked.
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 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 VMware AirWatch 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

1. The server address "https://ws1user.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 Next.

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 AirWatch thus preventing any unauthorized users from accessing the application's information.
Close Workspace ONE

Close the Workspace ONE application by clicking on the "X" in the upper right corner.
Enrolling Your Windows 10 Device

We will now enroll our Windows 10 device in AirWatch. First, we will need to download the AirWatch Agent.

Download AirWatch Agent

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

2. Click **Download**.
   
   *NOTE - Please wait while the AirWatch Agent 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 AirWatch Agent Installer

![AirWatchAgent.msi](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.*

### Ignore Windows SmartScreen

![Windows SmartScreen](image)

Due to Firewall restrictions, Windows SmartScreen won't be available in the lab network. Click **Run** to continue.

*NOTE - Windows SmartScreen may take several seconds to display after clicking the AirWatchAgent.msi*
Install Additional Required Features

If any required features are missing, you will be prompted that the installer will install them for you. Click **OK** to continue.

**Click the Additional Features Installer**

The additional features that need to be installed will begin, click the flashing installer icon from your bottom toolbar.
Allow the Additional Features To Be Installed

Click **Yes** when asked if you wish to allow the application to make changes.

*NOTE - You may see the installer pause while this process completes. Please be patient, the installer when continue when it is finished.*

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 AirWatch Agent Install

Click **Install** to start the installer.

Allow the AirWatch Agent to Make Changes

Click **Yes** when prompted if you should allow the AirWatch Agent to make changes.
Complete the AirWatch Agent Installer

Click **Finish** to complete the AirWatch Agent installer.

*NOTE - After clicking finish, the Native Enrollment application will launch to guide you through enrolling into AirWatch. If it does not show up immediately, wait a moment for the next prompt to appear.*

Allow the NativeEnrollment Application to Make Changes

Click **Yes** when asked if you want to allow the NativeEnrollment app to make changes.
Enroll Your Windows 10 Device Using the AirWatch Agent

Click **Server Detail**.

Find your Group ID from AirWatch Console

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.
NOTE - The Group ID is required when enrolling your device in the following steps.

**Enter the Server Details**

1. Enter "hol.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.**
Finish the AirWatch Enrollment Process

Click **Finish** to end the Enrollment process. Your Windows 10 device is now successfully enrolled into AirWatch.
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 AirWatch 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 Win 10 - 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.

---

VMware AirWatch - Unified Endpoint Management for Windows 10
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. You may need to scroll to the right to find the **Refresh** button.
2. Click **Refresh**.
3. 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

![Image of User Account Control dialog]

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

1. The server address "https://ws1user.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 Next.

Enter Your Username for Workspace ONE

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

**Allow Access to Credentials**

![Credential Required dialog box]

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.*
Confirm Successful Login to the Workspace ONE App

Upon successfully logging in, you should see the Apps page of the Workspace ONE app with access to the Bookmarks and Catalog tabs.

Continue to the next step after confirming your login was successful.
Sign Out of the Workspace ONE Application

Within the Workspace ONE application,

1. Click the User Icon
2. 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 AirWatch console in Chrome browser,

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

Click on the Windows icon

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

Select Compliance Device Type

Click on the **Windows Desktop** icon
Select Encryption

1. Click the **Rules** dropdown and select **Encryption**
2. Ensure **is not encrypted** is selected
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. Click in the **Assigned Groups** field and select "All Devices (your@email.shown.here)"
2. Click **Next**
Activate the Compliance Rule

![Add Compliance Policy](image)

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 run 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. 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 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

1. The server address "https://ws1user_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 Next.

Enter Your Username for Workspace ONE

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

### Confirm Authentication Failure

1. Confirm that authentication into the Workspace ONE app 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 VMware AirWatch 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

AirWatch 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.

Bit Locker Encryption

With the latest release of AirWatch, you are now 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 AirWatch console, also known as managed content.

Delete Device from AirWatch Console

From the AirWatch 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 AirWatch 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 device management or other types.
Remove the Compliance Policy

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 VMware AirWatch including 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.
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-1857-02-UEM

Version: 20180425-080944