# Table of Contents

Lab Overview - HOL-1957-03-UEM - Workspace ONE UEM - Intelligence .......................... 2  
   Lab Guidance .................................................................................................................. 3  
Module 1 - Introduction to Dashboards, Automation, and Reports................................. 8  
   Introduction.................................................................................................................... 9  
   Change the Screen Resolution ...................................................................................... 10  
   Login to the Workspace ONE UEM Console ............................................................... 12  
   Intelligence Opt-in Process............................................................................................ 18  
   Connect to Windows 10 VM.......................................................................................... 25  
   Enrolling Your Windows 10 Device with a Basic Account ............................................ 26  
   Data Visualization through Dashboards ....................................................................... 38  
   Getting Insights through Reports .................................................................................. 45  
   Integrating Automation and Workspace ONE UEM API ............................................. 58  
   Predicting Windows 10 Dell Battery Failures and Automate Replacement .................. 66  
   Un-enrolling your Windows 10 Device......................................................................... 72  
   Conclusion...................................................................................................................... 78  
Module 2 - Mobile Flows ................................................................................................. 79  
   Introduction.................................................................................................................... 80  
   Change the Screen Resolution ...................................................................................... 81  
   Mobile Flows Logical Overview................................................................................... 83  
   High Level Configuration Walkthrough ....................................................................... 84  
   Integrate Workspace ONE with VMware Identity Manager ....................................... 85  
   Configure Remote App Access Template in VMware Identity Manager ....................... 86  
   Build Mobile Flows Connector .................................................................................... 87  
   Login to the Workspace ONE UEM Console ............................................................... 89  
   Configure Connectors in Workspace ONE UEM Console ............................................ 95  
   Configuration File for mapping of keywords to Apps .................................................. 96  
   Retrieve Your Exchange Account Details .................................................................... 97  
   Switch Account Role to the Mobile Flows Organization Group ................................... 99  
   Configure VMware Boxer to leverage Mobile Flows .................................................. 101  
   iOS Device Enrollment for Mobile Flows .................................................................... 111  
   Validate that the Coupa App is assigned .................................................................... 131  
   Experience Mobile Flows in action ............................................................................. 136  
   Un-enrolling Your Device ......................................................................................... 147  
   Conclusion...................................................................................................................... 156
Lab Overview - HOL-1957-03-UEM - Workspace ONE UEM - Intelligence
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 the latest features of Workspace ONE Intelligence which provides rich analytics from your deployments and applications while reducing the cumbersome administrative workload by automating tasks and OS updates and patches. Learn how you can interact with different business systems without ever leaving VMware Boxer lab to maximize the productivity of your users.

Lab Module List:

- **Module 1 - Introduction to Dashboards, Automation, and Reports** (30 minutes) (Beginner) Explore the Workspace ONE Intelligence Console to view how Dashboards and Reports can provide customized inspection for your deployments at a glance. Configure Automation tasks and discover how to reduce your manual administrative workload.
- **Module 2 - Mobile Flows (45 minutes)** (Beginner) Wish there was an easier way to integrate the various components your workforce utilizes to increase productivity streamline simplicity? Explore Mobile Flows and learn how you can enable your apps and services to easily perform cross-application tasks without leaving your current app.

Lab Captains:

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

Subject Matter Experts:

- Karim Chelouati, Sr. Technical Marketing Manager, USA

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

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 - Introduction to Dashboards, Automation, and Reports
Introduction

With so much data available to IT admins managing modern, mobile work styles and no single tool to make sense of it, IT is faced with a huge challenge to manage the digital workspace. The lack of unified visibility across devices, applications and users makes it particularly hard to make data-driven decisions. As a result, manual processes become the norm, and IT is cornered into being reactive to employee demands and external events instead of being proactive.

Deep insights empower IT admins to better plan and optimize their app and policy deployments based on network performance, resource entitlement and deployment risk. And with the ability to automate processes, IT admins can proactively increase their level of security hygiene and meet compliance requirements, while improving user experiences.

With the new rules engine at the heart of Workspace ONE Intelligence, IT admins can automate processes across their environments by defining rules that take actions based on a rich set of parameters. This allows IT to create contextual workflows that take automated remediation actions based on security threats, and meet compliance requirements through automated access control. And because Workspace ONE Intelligence provides extensibility with an API layer for third parties, IT admins can build workflows that leverage their unique environment to meet their needs.

With automation, Workspace ONE Intelligence helps IT meet compliance requirements and increase security through automated remediation.
**Change the Screen Resolution**

Before proceeding to the Workspace ONE Intelligent Console, you will increase the screen resolution of the virtual machine for a better experience.

**NOTE: The Intelligent Opt-In form will NOT be visible later in the lab unless the resolution is increased!**

**Open the Screen Resolution Settings**

Return to the Desktop, then **right-click** and select **Screen Resolution**.
Increase the Screen Resolution

1. Click the **Resolution** dropdown.
2. Increase the Resolution to **1280x800**.
3. Click **Apply**.

Keep Display Settings

Click **Keep Changes** when prompted after changing your resolution.
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...
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 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.
Intelligence Opt-in Process

The first step to start using Workspace ONE Intelligence is to authorize the data synchronization between Workspace ONE UEM and Intelligence Cloud Service, this is done through the Opt-in Process that needs to performed by some one with administrator privilege at Workspace ONE UEM.

Access to Intelligence

In the Workspace ONE UEM Console,

1. Click **HUB**.
2. Click **Intelligence**.
Getting Started

Click **GET STARTED** to initiate the Opt-in process
Authorizing Intelligence to collect and replicate the data (Opt-In)

1. You may need to scroll down to find the Opt In button.
2. **Enable** the Opt In checkbox.
3. Click **Next**.
Complete the Terms of Service

Hub

Terms of Service

You must accept the following terms of service to use Intelligence.

VMware Cloud Services

TERMS OF SERVICE

By using a VMware cloud service offering ("Service Offering"), you agree to be bound by these terms of service between you and VMware ("Terms of Service"), and by the applicable Service Description, the VMware Data Processing Addendum, the applicable Support Policy, and the applicable Service Level Agreement, Terms, all of which together constitute the "Agreement". If you do not agree to these Terms of Service or to any other portion of the Agreement you must not use the Service Offering. "You" means you individually (and, as applicable, your Users) or the entity that you represent. If you are entering into the Agreement for an entity, you represent that you have the authority to bind that entity. "VMware", "we" or "us" means VMware, Inc., a Delaware corporation, if the billing address for your Order is in the United States, or VMware International Limited, a company organized and existing under the laws of Ireland, if the billing address for your Order is outside the United States. Capitalized terms used in these Terms of Service are defined throughout these Terms of Service and in Section 14 ("Definitions"). Section references in this document are to the provisions of these Terms of Service.

1. THE SERVICE OFFERING.

1.1 Generally. We may deliver the Service Offering with the assistance of our affiliates, licensors, and service providers. For purposes of the Agreement, a "Service Offering" includes services to host, on your behalf, VMware Software to enable you to use the software in a production environment via internet-based consoles.

1.2 Use of the Service Offering.

This is the final step on the opt-in Process, where you will be providing your information and accept the VMware Cloud Services TERMS OF SERVICE

1. Enter your Name
2. Enter your Email Address
3. Enter your Title
4. Enter your Company Name
5. Enter your Company Address
6. Click Accept

After the accepting you will be redirect to the Workspace ONE Intelligence Console.
Start the 30 Day Trial

Welcome to Workspace ONE Intelligence

Congratulations!

30 Day Free Trial

You are eligible to try all paid features of Workspace ONE Intelligence for free once you enroll for 30 days. You will gain access to features like Dashboards to visualize app engagement, security risk or create custom widgets with KPIs of interest. Plus, automate processes across your environment by defining rules that take actions.

Click Start 30 Day Trial in the bottom-right corner.
Enter the details for 30 Day trial

Welcome to Workspace ONE Intelligence

Start 30 Day Free Trial

Enter User Account Details

1. Enter your Name.
2. Enter your Email Address.
3. Enter your Job Title.
4. Enter your Company Name.
5. Enter your Phone Number.

Note: By accepting this trial you are agreeing to be contacted by...

6. Click Accept.

Returning to Workspace ONE UEM Console

In order to execute this lab properly, you need to setup the Workspace ONE UEM Automation Connector between Workspace ONE UEM and Intelligence.
Let's return to the Workspace ONE UEM Console where the first setup needs to be made.

1. Click on the **Square menu**
2. Click on **Workspace ONE UEM Console**

![Workspace ONE UEM Console](image)
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!`
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

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
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 **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.
Data Visualization through Dashboards

Dashboard is a powerful tool in Workspace ONE Intelligence that allows IT Administrators to build a rich data visualization of the data available, most of the time reports are the primary source of data representation and provide helpful information, however using charts or graphs to visualize large amounts of complex data is easier than over spreadsheets or reports.

Data Visualization can also:

1. Identify areas that need attention or improvement.
2. Clarify which factors influence employee adoption of specific applications.
3. Help you understand how secure your environment is based on OS Updates applied to the machine and new patches available out there.
4. Predict hardware failures
5. Etc..

Workspace ONE Intelligence brings out of the box on Dashboard, that includes nine Widgets and you can customize as you want.

For this chapter you will be adding a new widget based on Historical information showing enrollment over the 14 days, different from current widget on the standard dashboard that only show amount of enrollment today and total overtime.
Launch Intelligence Console

1. Click **HUB**
2. Click **Intelligence**
3. Click **Launch**
Add Widget

1. Click on **My Dashboard**
2. Click on **Add Widget**

**Selecting Category**

When adding widgets, the first step is to select from each category you want to obtain data, which can be a snapshot of most recent data or historical that you can look into the data overtime and represent that into the charts.
Each category comes with a set of templates that can be customized as you create the widget, you can use start from scratch using Starter/blank template.

Add Widget

Select Template

Choose a category followed by a template below to start creating your widget.

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank</td>
<td>Create a widget from scratch</td>
</tr>
<tr>
<td>Compromised Status By OS Version</td>
<td>Count of Devices grouped by OS Version and Compromised Status</td>
</tr>
<tr>
<td>1.2 Total Enrollments</td>
<td>Number of Enrollments to Date</td>
</tr>
<tr>
<td>iOS Device and OS Breakdown</td>
<td>Count of iOS Devices by OS Version and Model</td>
</tr>
<tr>
<td>1.2 Number of Enrollments Today</td>
<td>Total Number of New Enrollments Today</td>
</tr>
<tr>
<td>Windows Devices by OS Version</td>
<td>Count of Windows devices grouped by OS Version</td>
</tr>
</tbody>
</table>

1. Click **Devices**
2. Select **Total Enrollments** template
3. Select **Next**
Using Total Enrollments Template

Customize

Customize your widget by selecting the filters you want to apply and how you would like to visualize data.

Filters

- **Enrollment Status equals (Enrolled)**

Data Visualization

- **Chart Title**
  
  Total Enrollments

  
  **SNAPSHOT** **HISTORICAL**

  **Chart Type**

  - **Measure**
    - Count of Key Device GJID

  **Results per group**

  - 30

The default template show the amount of devices enrollment today.

Based on that template you will learn how to make changes that will show the enrollment overtime, looking at the historical data.
Creating Total Enrollments Over time Widget

1. Scroll down until you see the option for **Data Visualization**
2. Enter **Total Enrollments Over time** for Chart Title
3. Click **Historical**
4. Click **Line** for Chart Type
5. Enter **Platform** for by Group
6. Set **Last 14 Days** to Date Range
7. Click **Save**

**Note:** The above chart is an chart example with certain amount of data, your chart will be presented based on the current amount of devices and results will differ from that.
Setting Widget location and sizing on the Dashboard

The Widget has been added to the bottom of your dashboard.

1. You can move the widget around, clicking and holding on the Chart tile.
2. Also you resize the widget selecting the edges and dragging.
Getting Insights through Reports

Report is a powerful tool in Workspace ONE Intelligence that allows IT Administrator to get easy access and visibility into devices, applications and OS update data. It's a scalable and won't impact on the performance of the entire solution because you have a lot of data or are running too many reports daily.

All the data synced by the Workspace ONE Intelligence Connector (ETL service) is available through reports, after opt-in on Intelligence, ETL service will push all the available on AirWatch database and after that just the delta, the delta is based on device samples sent to Workspace ONE UEM.

In this chapter you will learn how to create reports that can drive business decisions, help to mitigate issues and automatically share information with other departments.

Creating Device Report

1. Click Reports
2. Click Add Report
Selecting Report Category

When creating reports, the first step is to select from each category you want to obtain data, the columns to display and to be used as filter on the report relays on that information.

The categories available today are:

- Apps
- Devices
- OS Updates

Each category comes with a set of templates that can be customized as you create the report, you can use start from scratch using Starter/blank template.

Feel free to click on each category and check the templates available to each, in this module we will create two reports, one based on Device Category and the other based on OS Updates.

1. Click **Devices**
2. Select **Enrolled Devices**
3. Click **Next**
Customizing Report Filter

The Enrolled Devices template creates a report with pre-defined columns and filtering only enrolled devices, right after you can see a preview of the report based on live data.

1. Click + to add a new filter
2. Enter Platform for the field
3. Select Includes for the filter type
4. Enter WinRT, Android and Apple for the value field

The Report Preview will show the number of Windows devices enrolled at this point.

Note: The report preview results is an example based on certain amount of data, your report results will be presented based on the current amount of devices and results will differ from that.
Customizing Report Columns

Customize

Customizing a report to meet your unique needs is easy. Just select the filters you wish to add and delete columns.

Filters

```
Enrollment Status equals (Enrolled) AND Platform includes (WinRT, Android, Apple)
```

Report Preview

This report preview features 9 of 3 total rows. Save Report to see the complete set of data.

<table>
<thead>
<tr>
<th>Last Seen</th>
<th>Friendly Name</th>
<th>Ownership</th>
<th>Username</th>
<th>First Name</th>
<th>Last Name</th>
<th>Email</th>
<th>Platform</th>
<th>OS Version</th>
<th>Enrollment Status</th>
<th>Compliance Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 17, 2016</td>
<td>Joe Desktop</td>
<td>Corporate</td>
<td>Joe</td>
<td>Joe</td>
<td>nophere...</td>
<td>WinRT</td>
<td>10.0.17134</td>
<td>Enrolled</td>
<td>Compliant</td>
<td></td>
</tr>
<tr>
<td>Jun 20, 2016</td>
<td>Joe iPad</td>
<td>Corporate</td>
<td>Joe</td>
<td>Joe</td>
<td>nophere...</td>
<td>Apple</td>
<td>11.4.0</td>
<td>Enrolled</td>
<td>Compliant</td>
<td></td>
</tr>
</tbody>
</table>

You can easily add or remove columns from the report, to start:

1. Scroll down until you see the option **Report Preview**
2. Click **Edit Columns**
Selecting Columns

1. Select the following columns: **Available Capacity, Available Physical Memory, BIOS Version and Battery Percent**
2. Click **ADD**
Changing Columns Order

1. Select the four columns you just added, clicking on each one
2. Click **Down button** four times
3. Click **Save**
Preview with new columns

Customize

Customizing a report to meet your unique needs is easy. Just select the filters you wish to add and edit columns.

Filters

- Enrollment Status equals (Enrolled) AND Platform includes (Windows, Android, Apple)

- Enrollment Status
  - Equals
  - Enrolled

- Platform
  - Includes

Report Preview

This report preview features 9 of 9 total rows. Save Report to see the complete set of data.

<table>
<thead>
<tr>
<th>Last Seen</th>
<th>Friendly No.</th>
<th>Ownership</th>
<th>Username</th>
<th>Available Capacity</th>
<th>Available Physical Memory</th>
<th>BIOS Version</th>
<th>Battery Percentage</th>
<th>First Name</th>
<th>Last Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 17, 20</td>
<td>jdoe Desk 1</td>
<td>Corporate</td>
<td>jdoe</td>
<td>N/A</td>
<td>N/A</td>
<td>2.6.2</td>
<td>0.26</td>
<td>Joe</td>
<td>Doe</td>
</tr>
<tr>
<td>Jun 20, 2</td>
<td>jdoe PD 1</td>
<td>Corporate</td>
<td>jdoe</td>
<td>111.32 GB</td>
<td>17.4 GB</td>
<td>2.6.2</td>
<td>0.26</td>
<td>Joe</td>
<td>Doe</td>
</tr>
</tbody>
</table>

1. New columns has been added to the report and are available on the Report Preview.
2. Click **Next**
Saving the Report

1. Enter **Windows, Android and Apple Enrolled Devices** for the Report name
2. Enter **All enrolled Windows, Android and Apple devices with details** for the Description
3. **Check** the Run Report now - that will generate a CSV file and make available for download - we will review that later in this chapter
4. Click **Save**
Windows, Android and Apple Enrolled Devices

Click **Overview**

A preview of the report will show up based on the conditions previous defined, this report is part of the list of reports available. The EDIT option allow you to make changes on the report.
1. Click Downloads
2. Click on the Refresh Icon
3. Validate that the status is now Completed
4. Click Download link to download the report in CSV format
5. Validate that report gets downloaded in the CSV format.
**Adding Schedule Report**

Requests for reports is something quite common in every organization, most of the time marketing, purchased, HR and other departments request some type of report regarding their Digital Workspace to be send on weekly, monthly or sometime other time period. Workspace ONE Intelligence allow Reports to be schedule, which runs the report and send via e-mail to a list of people or distribution list defined by the IT Administrator.

<table>
<thead>
<tr>
<th>Schedules</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD</td>
</tr>
</tbody>
</table>

1. Click **Schedules**
2. Click **ADD**

### Windows, Android and Apple Enrolled Devices

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Report Schedule

Schedule "Windows, Android and Apple Enrolled Devices"

1. Enter “Windows, Android and Apple Enrolled Devices” for Schedule Name
2. Select “Monthly” for Recurrence
3. Select 1 for Day of the Month
4. Enter 08:00 AM for Starts At
5. Set 12/31/2018 as the End date
6. Enter your company e-mail and press ENTER
7. Enter “Windows, Android and Apple Enrolled Devices” for Subject
8. Enter “Monthly report containing the list of Windows Desktop, Android and Apple devices managed by Workspace ONE UEM” for Message
9. Click SCHEDULE
Confirming Report Schedule

1. Click on Schedules
2. Confirm that your schedule has been added based on the parameters previously defined.
Integrating Automation and Workspace ONE UEM API

Returning to Workspace ONE UEM Console

1. Click on the **Square menu**
2. Click on **Workspace ONE UEM Console**
Access All Settings

1. Click Groups & Settings
2. Click All Settings

Enable Workspace ONE UEM API

In this step you will obtain the API Key for your Tenant and later use on Workspace ONE Intelligence Console, to keep that information we recommend you to open Notepad on your Windows Desktop and copy/paste the API Key there, you can also just copy using CTRL+C, but reminder that right after this step you will be using the API Key value, see below the steps on how to obtain the API Key.
Navigate to REST API

1. Click on System
2. Click on Advanced
3. Click on API
4. Click on REST API
5. Click Override, that will generate a new API Key and is required to Override the Customer OG when integrating with Workspace ONE Intelligence
6. Select the API Key for AirWatchAPI Service and right click Copy, switch to Notepad and right click to paste the API Key
7. Click Save
8. Click X to close the pop-up window
Save API Key

1. Click the Windows button.
2. Type Notepad to search.
3. Click Notepad from the list of results.

Enable Word Wrap

1. Click Format.
2. Click Word Wrap.
Paste the Session Token

Right-click and click Paste.

If you need to refer back to your API for future steps, open your Notepad file and copy the sessionToken that is pasted here.

Return to Workspace ONE Intelligence Console

1. Click HUB
2. Click Intelligence
3. Click Launch
1. Under **Reporting**, click on **Settings**
2. For the option **Automation Connection**, select **VIEW**

**Setup Workspace ONE UEM Connector**

Click **Authorize** for **Workspace ONE UEM API**
Provide Credentials for Workspace ONE UEM Connector

Connection: Workspace ONE UEM API

1. Click **Provide Credentials**
2. Enter **https://labs.awmdm.com** for Base URL
3. Enter **YOUR VLP e-mail** for API User Name
4. Enter **VMware1!** for API User Password
5. Enter the **API Key that you just saved on your Notepad** for Workspace ONE UEM Tenant Code
6. Click **Connect**
Validate Successful Authorization

You should see **DEAUTHORIZE** on the Workspace ONE UEM Card, that confirms the integration was done successfully.
Predicting Windows 10 Dell Battery Failures and Automate Replacement

Employees are using Windows devices that no longer last a full work day without charging. It disrupts their workday, reduces mobility, increases dissatisfaction and employees either seek remediation via helpdesk or do nothing and end up plugging their laptops at all times.

**How Workspace ONE Intelligence can help:**

- Monitor Windows 10 Dell devices with poor battery health (overall remaining life of the battery) Reports or Dashboards
- Create visualization that proactively highlight users who are experiencing poor battery life
- As the battery life decreases, so does its maximum charge capacity
- Create automation to tag devices with poor battery life in Workspace ONE UEM to help with reporting and assignment, create Service Now ticket with device info to order new battery and notify employees via Slack or email that a battery replacement is on its way

**Key benefits:** Reduce costs linked to user-generated support tickets or calls, increase employee experience and productivity. Increase lifespan of devices.

**Creating Automation**

Click **Add Automation**
Select Automation Template

Add Automation

Select Template

Create an automation from scratch or use a template to start

1. Create a custom automation
2. IOS Roaming Remediation

1. Click on Create a custom automation
2. Click Next

Defining the conditions to Trigger the automation

Template Category: Devices

Name: * Dell Battery Replacement

Trigger (When)

Device Data - New incoming state

Filter (If)

Dell Battery Health less than 25

Dell Battery Health Less Than 25
1. Under **Filter**, Enter **Dell Battery Replacement** for Name
2. Enter **Dell Battery Health** for the filter field
3. Enter **Less Than** for the Condition
4. Enter **25** for the field value

**Adding Workspace ONE UEM Action**

1. Scroll down until you see the section **Add Action**
2. Click on **+ sign** to expand the options
3. Click on **Workspace ONE UEM API**
4. Click on **Add Tag to Device**

### Configuring Action

**Action (Then)**

1. Enter **257** for Tag ID - that will tag the device on Workspace ONE UEM Console as **Needs battery replacement**
2. Turn **ON** for Enable this automation after saving
3. Click **Save**

### Saving and Enabling Automation

**Save & Enable**

Do you want to save and enable this automation?

1. Click **Save & Enable**
Access to Automation Logs

The automation that will always be looking for Dell Devices that needs battery replacement has been created, the View Logs shows the logs for each time this automation is triggered.
For this Lab you will see the log Empty, as we enrolled a Windows VM and not a physical Windows 10 Dell device.

The above image shows you a log example of multiple actions taking on different Services.

For this example that you just created, in a real world you could also setup a ServiceNow integration, and create a Helpdesk ticket that includes the user and devices information, requesting to ship a new battery to the user home.
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.

Reason:
lab completed

1. Enter the reason as **lab completed**.
2. Click on **Delete**.
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

Related settings
- Add or remove a provisioning package
- Export your management log files
- Set up an account for taking tests
- Enroll only in device management

View while Enrolled
- Connected to AirWatchMDM MDM
  Connected by testuser@corp.local

View after Un-enrollment
- Connected to CORP AD domain corp.local

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

\textbf{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 this module, you've learned:

• Create and automated reports to send relevant informations for those requesting and eliminate manual steps to the IT Team
• Add Widgets to Dashboards that shows Total Enrollments over time
• Predicate Windows 10 Dell Battery Failures and Automate Replacement tagging the device on Workspace ONE UEM Console
• You also learn that you can leverage integration with 3rd party services, like Service Now to trigger actions on automation.

For additional on Workspace ONE Intelligence, be sure to check out the VMware Workspace ONE Intelligence page at https://www.vmware.com/products/workspace-one/intelligence.html
Module 2 - Mobile Flows
Introduction

Workspace ONE Mobile Flows is the latest addition to the VMware Workspace ONE platform. Mobile Flows helps device users perform tasks across multiple business backend systems within any application that has been integrated with Mobile Flows. This eliminates the need to visit multiple websites to perform different business tasks. You can use the Mobile Flows either by leveraging different preconfigured connectors or by building custom developed services.
Change the Screen Resolution

Before proceeding to the Workspace ONE Intelligent Console, you will increase the screen resolution of the virtual machine for a better experience.

**NOTE:** The Intelligent Opt-In form will NOT be visible later in the lab unless the resolution is increased!

Open the Screen Resolution Settings

Return to the Desktop, then **right-click** and select **Screen Resolution**.
Increase the Screen Resolution

1. Click the **Resolution** dropdown.
2. Increase the Resolution to **1280x800**.
3. Click **Apply**.

Keep Display Settings

Click **Keep Changes** when prompted after changing your resolution.
Mobile Flows Logical Overview

In this section, we are going to see what are the different components and sub-systems involved with Mobile Flows and how they interact with each other.

1. The VMware Identity Manager instance is registered with the Mobile Flows Server.
2. Application fetches a JSON Web Token (JWT) for Authentication.
3. Application sends request to Mobile Flows Server to query details to form a Mobile Flow Card.
5. Connector fetches and consolidates business system data for the Mobile Flow Card.
6. Data is returned to the Mobile Flows Server.
7. Data is delivered to the app.
High Level Configuration Walkthrough

In order to limit the scope of the lab, you will be working with a pre-configured setup. The high level steps of setting up Mobile Flows are as follows:

1. Integrate Workspace ONE UEM with VMware Identity Manager.
2. Configure Remote App Access template in VMware Identity Manager.
3. Build a custom Mobile Flows Connector or use the Out of the Box Connector.
4. Install Mobile Flows Connector on a server with a public URL.
7. Install VMware Boxer on a managed device.
Integrate Workspace ONE with VMware Identity Manager

VMware Identity Manager (vIDM) can be used to authenticate the information transfer when using connectors for client applications. If your environment includes VMware Identity Manager, you can create a VMware Identity Manager template to fetch user specific JSON Web Token (JWT) for connector authentication.

We have already integrated Workspace ONE and VMware Identity Manager for this lab. However, if you want to learn more about how this integration and configuration can be performed, please refer the following HOL from Workspace ONE HOL Catalog - HOL-1957-01-UEM / Module 1 - Workspace ONE Setup and Configuration. This lab will also walk through the AD integration using VMware Enterprise Systems Connector to so that we can leverage AD accounts as administrators.
Configure Remote App Access Template in VMware Identity Manager

This section will walk you through on how to create a template within VMware Identity Manager (vIDM) to request the JSON Web Token (JWT) token to authenticate Mobile Flows traffic. This template is already setup for you for this lab. Let’s go through the following video to see how the template was configured.

Remote App Access Template in VMware Identity Manager

This video will walk you through how to setup and configure Remote App Access Template in VMware Identity Manager.

**NOTE** - The video contains no spoken instructions. Please refer to the subtitles for instructions about the installation process. Do not attempt to make any of the configurations or changes shown in the demo video! This demonstration is only to highlight the configuration and installation process for your knowledge.
Build Mobile Flows Connector

Mobile Flows Connectors are the components responsible for interacting with the backend business systems that you integrate with. They are responsible for data fetching and also for performing the actions as requested by the client application.

Workspace ONE offers out-of-the-box connectors targeting top use cases with the most popular business systems. All the source code for these connectors is open source, so anyone can modify the existing connectors or build their own custom connector using our API spec and sample connectors. Custom connectors can be built in around 250 lines of code or less and are flexible to be built using your preferred programming language. Custom Connectors allow you to match the data model of your business system and to create business logic that will meet the needs of your end users.

Workspace ONE Mobile Flows Connector

Workspace ONE administrators deploy a lot of applications to their end users targeting different use cases. Sometimes it might happen that your end users don't know that they have certain applications available to download On-Demand. While other times, they are aware that a certain application is available in their Workspace ONE catalog but they don't know what it is used for.

The Workspace ONE Connector presents Mobile Flows Cards inviting users to install apps that are missing from the user's device. The Mobile Flows Client Framework is in the VMware Boxer app and is responsible for parsing the e-mail body for keyword. Once one of the keywords matches, the Workspace ONE Connector is responsible for requesting the application from the Workspace ONE Catalog via a Mobile Flows Card within that particular e-mail itself. This connector uses application keywords, device UDID and device platform to request the correct app from Workspace ONE Catalog.
Setup and Configuration Video

This video will walk you through how to setup and configure Workspace ONE Connector.

**NOTE** - The video contains no spoken instructions. Please refer to the subtitles for instructions about the installation process. Do not attempt to make any of the configurations or changes shown in the demo video! This demonstration is only to highlight the configuration and installation process for your knowledge.
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 *
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 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.
Configure Connectors in Workspace ONE UEM Console

Once we have successfully deployed the Mobile Flows Connector on a public facing URL, the next step is to add the connection information in the Workspace ONE Console. These details will be used by Mobile Flows server for Connector discovery and by the client applications to interact with the backend systems.

For this lab, Workspace ONE App Discovery Connector is already hosted for you. The following video will walk you through the process.

Configure Connector in Console

This video will walk you through how to configure Mobile Flows Connector in Workspace ONE UEM Console.

**NOTE** - The video contains no spoken instructions. Please refer to the subtitles for instructions about the installation process. Do not attempt to make any of the configurations or changes shown in the demo video! This demonstration is only to highlight the configuration and installation process for your knowledge.
Configuration File for mapping of keywords to Apps

For this lab, we are going to validate the scenario where the email body is parsed for the keyword `travel` and it should populate a Mobile Flows Card to install the `Coupa` app.

Application Configuration File for mapping of keywords to Apps (FOLLOW ALONG)

The Mobile Flows Connector gets the mapping of keywords to apps from the file located at `/etc/opt/vmware/connectors/airwatch/managed-apps.yaml`.

For this lab, the file is configured as follows:

1. Populate the hero card pointing to the app with bundle ID `com.coupa.push`
2. For the keyword `travel`

**NOTE** - For the flow to work the application should already be assigned to the device with the deployment type as On Demand. Mobile Flows Cards will not appear if the app is already installed on the device.

**NOTE** - You do not need to complete any configurations on this step, it is only used to highlight the changes already setup for you.
Retrieve Your Exchange Account Details

A temporary Exchange mailbox has been generated for you to use throughout this lab. The account credentials are uploaded to the Content section of the Workspace ONE UEM Console.

Locate Your Exchange Account Details

In the Workspace ONE UEM Console,

1. Click **Content**
2. Expand **Content Locker**.
3. Click **List View**.
4. Find the text file named Mailbox Details for your@email.shown.here.txt and click the toggle button beside it to select the file.
5. Click **Download**.

In the Workspace ONE UEM Console,
Open the Downloaded Text File

After the file downloads, click the Mailbox Details for your@email.shown.here.txt file from the download bar to open it.

Note the Email Address

You will use this Email Address and sAMAccountName in an upcoming exercise enroll your iOS Device and to send an email with VMware Boxer. Leave this Notepad file open while you complete the lab to refer to the details when instructed.
Switch Account Role to the Mobile Flows Organization Group

Before making any configurations within the Workspace ONE UEM console, you will need to change your Account Role to the Mobile Flows organization group that has been created for you as part of this lab. This separate organization group in Workspace ONE UEM contains the various components you have been reviewing so far that have been preconfigured for you, requiring your additional console configurations to be made at this organization group to function properly once you enroll your device.

Switch to Your mflows Organization Group

In the Workspace ONE UEM Console,

1. Click the **User dropdown** in the top-right corner. The text will be your VLP Email Address.
2. Click the **Account Role** dropdown.
3. Click the **AirWatch Administrator at mflows_your@email.shown.here** role.

Confirm the mflows Organization Group is Active

1. The Organization Group tab at the top of the Workspace ONE Console should now show **mflows_your@email.shown.here**.
2. Make note of your **Group ID**. This Group ID is separate from your original Organization Group ID and will be used when you enroll a device in an coming exercise.
Configure VMware Boxer to leverage Mobile Flows

We have seen how to configure Workspace ONE Mobile Flows Connector for App Discovery. The Mobile Flows Client Framework embedded into VMware Boxer is responsible for parsing the email body for keywords and initiate the Mobile Flows card within the app. After that, Mobile Flows server does Connector discovery and authentication using the configuration in the Workspace ONE UEM Console.

In this section, we are going to see how we can use Application Configuration to enable VMware Boxer to leverage Mobile Flows.

Add the VMware Boxer Client as an iOS Public Application

1. Click Add.
2. Click Public Application.
Search for the Application to Add

1. Ensure your Managed By field shows **mflows_your@email.shown.here**. If it does not, refer to previous steps on how to change your current Account Role to the mflows_your@email.shown.here organization group!
2. Select **Apple iOS** from the Platform dropdown.
3. Enter **VMware Boxer** in the Name field.
4. Click **Next**.

Select the Application from the Search Results

**VMware Boxer**
- **Free**
- Category: Business
- Current Version: 4.13.1

VMware Boxer is the most innovative email, calendar and contacts app available for iPhone! Here's what people are saying about our app: The Webby Awards Nominated Boxer for Best Mobile Productivity App of the Year! ***** If you like to have a lot of control over how your app works, including the ability to customize swipe gestures, you should check out Boxer. With its fast notifications, plentiful customization options, and integrated calendar and contacts list, this iPhone app has a lot to o...
Click **Select** on the **VMware Boxer** application.

**Save and Assign VMware Boxer**

![Add Application - VMware Boxer](image)

Click **SAVE & ASSIGN**
Add Assignment for VMware Boxer

VMware Boxer - Update Assignment

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

Please note that the newly added assignments will be added at the end of the list. Assignments can now be moved up or down in the priority list. Devices will receive application based on the below configuration. In the case where devices belong to multiple groups, they will receive application with highest priority (0 being highest priority).

Click + ADD ASSIGNMENT

Configure VMware Boxer Assignment Settings

1. Select the **mflows_your@email.shown.here** group for the Select Assignment Groups field.
2. Select **Auto** for the **App Delivery Method**.
Configure VMware Boxer Email Settings

1. Find the Email Settings section, you may need to scroll down.
2. Enter **HOL Email** for the **Account Name**. This is a friendly name used to identify this email account configuration.
3. Enter **https://sme.airwlab.com** for the **Exchange ActiveSync Host**.
4. Enter **hol** for the **Domain**.
5. Enter the lookup value **{UserPrincipalName}** for the **User**.
6. Enter the lookup value **{EmailAddress}** for the **Email Address**.
Configure Policies for VMware Boxer

VMware Boxer - Add Assignment

1. Scroll down to find the Policies section.
2. Select **ENABLED** for **Device must be MDM Managed to install this App**.
3. Select **ENABLED** for **Remove on Unenroll**.
4. Select **ENABLED** for **Prevent Application Backup**.

---

**Policies**

- **Device must be MDM Managed to install this App**: **ENABLED**
- **Remove On Unenroll**: **ENABLED**
- **Prevent Application Backup**: **ENABLED**
- **Make App MDM Managed if User Installed**: **DISABLED**
- **App Tunneling**: **ENABLED**

---

**Notes**

- **iOS 7+**
## Add Application Configuration

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Value Type</th>
<th>Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppMobileFlowsEnabled</td>
<td>Boolean</td>
<td>True</td>
</tr>
<tr>
<td>AppMobileFlowsHost</td>
<td>String</td>
<td><a href="https://prod.hero.vmwservices.com">https://prod.hero.vmwservices.com</a></td>
</tr>
<tr>
<td>AppMobileFlowsvIDM</td>
<td>String</td>
<td><a href="https://hol-cn1193-intelligence.vidmpreview.com">https://hol-cn1193-intelligence.vidmpreview.com</a></td>
</tr>
<tr>
<td>AppMobileFlowsSyncTimeHours</td>
<td>Integer</td>
<td>1</td>
</tr>
<tr>
<td>AppMobileFlowsAutoEnableConnectors</td>
<td>Boolean</td>
<td>True</td>
</tr>
</tbody>
</table>

1. Scroll down until you see the option for **Application Configuration**.
2. Enter Configuration Key as `AppMobileFlowsEnabled` Type as **Boolean** - Value as **True**. Click the **Add** Button in Blue to add a new row.
3. Enter Configuration Key as `AppMobileFlowsHost` Type as **String** - Value as `https://prod.hero.vmwservices.com`. Click the **Add** Button in Blue to add a new row.
4. Enter Configuration Key as `AppMobileFlowsvIDM` Type as **String** - Value as `https://hol-cn1193-intelligence.vidmpreview.com`. Click the **Add** Button in Blue to add a new row.
5. Enter Configuration Key as `AppMobileFlowsSyncTimeHours` Type as **Integer** - Value as **1**. Click the **Add** Button in Blue to add a new row.
6. Enter Configuration Key as `AppMobileFlowsAutoEnableConnectors` Type as **Boolean** - Value as **True**.
Click the **Add** button at the bottom of the page.
1. Confirm that the Assignment you just configured is displayed.
2. Click **SAVE & PUBLISH**
Preview Assigned Devices and Publish

Preview Assigned Devices

Assignment Status

Search List

Assignment Status  Friendly Name  User  Platform/OS/Model  Organization Group

No Records Found

Click PUBLISH
iOS Device Enrollment for Mobile Flows

Before enrolling, you will need to locate a few details from the Workspace ONE UEM Console and the Mailbox Details text file you downloaded previously in order to enroll your device. Follow the next steps to retrieve the needed details and make note of their values, as you will use them in the upcoming steps.

Locate your Exchange Account Credentials

1. Click the Mailbox Details for your@email.shown here text file from the task bar that you opened in the previous steps.
2. Note your Email Address. This will be the username you provide during iOS enrollment.
3. Note the Email Password. This will be the password you provide during iOS enrollment.
4. Note the sAMAccountName. This will be the username you provide when signing into the Workspace ONE App on the iOS device.

Leave this Notepad file open while you advance through the rest of the exercise, as you will need to refer back to these values in upcoming steps.

Enroll Your iOS Device

In this section, we are going to enroll an iOS device to complete the steps on the device side.
Download and Install Workspace ONE Intelligent Hub from App Store (IF NEEDED)

NOTE - Checked out devices will likely have the Workspace ONE Intelligent Hub already installed. You may skip this step if your device has the Workspace ONE Intelligent Hub installed.

At this point, if you are using your own iOS device or if the device you are using does NOT have the Workspace ONE Intelligent Hub Application installed, then install the application from the App Store.

To Install the Workspace ONE Intelligent Hub application from the App Store, open the App Store application and download the free Workspace ONE Intelligent Hub application.
Launching the Workspace ONE Intelligent Hub

Launch the **Hub** app on the device.

*NOTE - If you have your own iOS device and would like to test you will need to download the Workspace ONE Intelligent Hub app first.*
Enter the Server URL

1. Enter `labs.awmdm.com` for the Server URL.
2. Click **Next**.

Click on the **Server Details** button.

Find Your Group ID From the Workspace ONE UEM Console

Return to the Workspace ONE UEM 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.

**Attach the Workspace ONE Intelligent Hub to the HOL Sandbox**

1. Enter your **Group ID** for your Organization Group for the **Group ID** field. Your Group ID was noted previously in the **Finding your Group ID** step.
2. Tap the **Next** button.

**NOTE** - If on an iPhone, you may have to close the keyboard by clicking **Done** in order to click the **Next** button.
Enter User Credentials

1. Enter the email address copied from the previous steps in the **Username** field. This will be in the format `yourid1234@hol.airwlab.com`.
2. Enter **VMware1!** in the **Password** field.
3. Tap the **Next** button.

You will now provide user credentials to authenticate to Workspace ONE UEM.
Redirect to Safari and Enable MDM Enrollment in Settings

Workspace Services

This is required before the app can be installed. You automatically receive:

- Direct installation of all corporate resources.
- Secured corporate network access.
- Synchronized apps and content on all of your devices.
- An enhanced app experience that will make you more productive.

The Workspace ONE Intelligent Hub will prompt you to enable Workspace Services to enroll your device into Workspace ONE UEM.

Tap **Next** to begin.
Allow Website to Open Settings (IF NEEDED)

If you prompted to allow the website to open Settings to show you a configuration profile, tap **Allow**.

**NOTE - If you do not see this prompt, ignore this and continue to the next step. This prompt will only occur for iOS Devices on iOS 10.3.3 or later**
Install the Workspace ONE MDM Profile

Tap **Install** in the upper right corner of the Install Profile dialog box.
Enter Device Passcode (IF NEEDED)

If prompted, enter your device passcode to continue.
If you do NOT receive this prompt, continue to the next step.

Install and Verify the Workspace ONE MDM Profile

Tap **Install** when prompted at the Install Profile dialog.
**iOS MDM Profile Warning**

<table>
<thead>
<tr>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MOBILE DEVICE MANAGEMENT</strong></td>
</tr>
<tr>
<td>Installing this profile will allow the administrator at “<a href="https://ds1193.awmdm.com/DeviceServices/AppleMDM/Processor.aspx%E2%80%9D">https://ds1193.awmdm.com/DeviceServices/AppleMDM/Processor.aspx”</a> to remotely manage your iPad.</td>
</tr>
<tr>
<td>The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPad.</td>
</tr>
</tbody>
</table>

You should now see the iOS Profile Installation warning explaining what this profile installation will allow on the iOS device.

Tap **Install** in the upper-right corner of the screen.
Trust the Remote Management Profile.

You should now see the iOS request to trust the source of the MDM profile. Tap **Trust** when prompted at the Remote Management dialog.
iOS Profile Installation Complete

Profile Installed

Device Manager

Signed by: mobile.com
Verified

Description: Device Management profile to manage and activate access to work applications and services on your device.

Contains: Mobile Device Management Certificate

More Details

You should now see that the iOS Profile was successfully installed.

Tap Done in the upper right corner of the prompt.
Congratulations!

You have completed the initial configuration for your device. You will receive a notification prompt if further action is required.

You may navigate away from this page.

Open this page in “Hub”?

Cancel! Open

Your enrollment is now completed! Tap Open to navigate to the Workspace ONE Intelligent Hub.
Accept the Workspace ONE Intelligent Hub Notice

Your IT department will provide you access to a wide variety of company resources and apps and notify you if further action is required.

Tap **Done** to confirm the notice and continue.

**Accept Notifications for Hub (IF NEEDED)**

“Hub” Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Tap **Allow** if you get a prompt to allow notifications for the Hub app.
Accept the App Installation (IF NEEDED)

You may be prompted to install a series of applications depending on which Module you are taking. If prompted, tap **Install** to accept the application installation.
Confirm the Privacy Policy
Your privacy matters.

VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Hub to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.

Contact your company’s IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.

Data collected by Hub
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure company data stored on this device. Your company has access to this data and some data collected may be visible to your IT administrator.

Hub permissions
Tap here for an overview for the device permissions that this app will require to function properly. These permissions can be changed at any time within your device settings but may impact app functionality.

Your company's privacy policy
Contact your IT administrator for information about how your company handles information collected by this app.

I understand
Tap **I Understand** when shown the Privacy policy.

**Accept the Data Sharing Policy**

Help us improve and develop new app features and functionality that will make you even more productive.

We would like to collect information about your usage of our app to better understand how users interact with our apps and how we can improve the app experience. We analyze this usage data in the aggregate and not in any way that identifies you. If you change your mind, you can change this setting at any time.

For information about how VMware handles your usage data if you elect to share this data with VMware, visit [https://www.vmware.com/help/biography.html](https://www.vmware.com/help/biography.html)

Tap **I Agree** for the Data Sharing policy.
Confirm the Device Enrollment in the Hub App

Confirm that the Hub app shows the user account that you enrolled with.

You have now successfully enrolled your iOS device with Workspace ONE UEM! Continue to the next step.
Validate that the Coupa App is assigned

The pre-requisite for the Hero Card to populate is that the app needs to be assigned to the device with the deployment mode as **On Demand**.

Launch Workspace ONE App

Tap on the icon to launch the Workspace ONE App.
Select the HOL domain

1. Select `hol` for the domain.
2. Tap `Next`
Enter Credentials

1. Enter **Your sAMAccountName** from the Mailbox Details text file you downloaded when retrieving your Exchange Account Details.
2. Enter **VMware1!** for the password.
3. Tap **Sign in**.
Enter the App Catalog

Loading your workspace.

Welcome!
Your app catalog is almost ready.

Your workspace is ready to load.

Enter

You will see a series of screens updating the progress on building your workspace. When the process is complete, tap Enter.

Accept Push Notifications from Workspace ONE

"Workspace" Would Like to Send You Notifications
Notifications may include alerts, sounds, and icon badges. These can be configured in Settings.

Don’t Allow  Allow
Tap **Allow** when prompted to accept push notifications from Workspace ONE.

**Validate that Coupa app is assigned**

Validate that you see **Coupa - Expenses & Approvals** in the Workspace ONE Catalog. Do NOT install the application from Workspace ONE, as the application will need to be uninstalled for the upcoming Mobile Flows Hero Card demonstration to work.

In the next section, we will see how a Hero Card is populated to prompt the install of the Coupa App.

**Return to the iOS device Spring Board**

Click the home button of your iOS device to return to the Spring Board.
Experience Mobile Flows in action

in this section, we are going to see how to Mobile Flows enhances the functionality of VMware Boxer. We have already deployed the app with Application Configuration to enable Mobile Flows. The client framework is responsible to parse the email body for the keyword and it will trigger the Workspace ONE App Discovery Connector.

Launch VMware Boxer

Tap on the icon to launch VMware Boxer.
Accept the Privacy Prompt

Your privacy matters.
VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Boxer to provide optimal performance, security and support. For information about how your company handles information collected by Workspace ONE, please contact your company.

Contact your company’s IT administrator if you want to find out how to un-enroll your device and discontinue access to this app.

Data collected by Boxer
Tap here for an overview of the data that this app may collect about device hardware, diagnostics and user information to function properly, and to secure company data stored on this device. Your company has access to this data and some data collected may be visible to your IT administrator.

Boxer permissions
Tap here for an overview for the device permissions that this app will require to function properly. These permissions can be changed at any time within your device settings but may impact app functionality.

Your company’s privacy policy
Contact your IT administrator for information about how your company handles information collected by this app.

Tap I understand to accept the Privacy prompt.
Agree to the Data Sharing Prompt

Want an even better app experience?
Help us improve and develop new app features and functionality that will make you even more productive.
We would like to collect information about your usage of our app to better understand how users interact with our apps and how we can improve the app experience. We analyze this usage data in the aggregate and not in any way that identifies you. If you change your mind, you can change this setting at any time.

For information about how VMware handles your usage data if you elect to share this data with VMware, visit https://www.vmware.com/help/privacy.html.

I agree

Tap I agree to accept the Data Sharing Prompt

Enter the password for the email account

Welcome to a better inbox,
yourid1234@hol.airlwl.com

1. Enter VMware1! for the password.
2. Click Get Started.
Accept the Boxer Prompts

You might see several prompts for permissions and push notifications for Boxer. Click OK or Allow as necessary.

Enable Mobile Flows in Settings

From the bottom right corner, tap on the option Settings
1. Scroll down until you see the **MORE** section.
2. Tap on **Advanced**.

**Tap on Mobile Flows**

Under **ENABLED FEATURES**, tap on **Mobile Flows**

**Enable Mobile Flows**

Enable **Mobile Flows** using the slider.
Select the HOL domain

1. Select hol for the domain.
2. Tap Next
Enter Credentials

1. Enter **Your sAMAccountName** from the Mailbox Details text file you downloaded when retrieving your Exchange Account Details.
2. Enter **VMware1!** for the password.
3. Tap **Sign in**.

**Forgot Password?**

**Change to a different domain**
Validate that Mobile Flows and Connector are enabled

From the bottom toolbar, tap on option Mail to return to the Inbox

Compose a new email

Tap the icon to compose a new email.

Populate Email

Replace with your email address!
From the previous section, recall that our configuration file maps the keyword **Travel** to the application **Coupa**. You will compose an email to your provided exchange account with the Subject and email body containing this keyword so that the Hero Card is prompted when you view the email.

1. Enter **your email address** in the address field. This is the email address you enrolled with and is available in Mailbox Details text file you downloaded from the Workspace ONE UEM Console.
2. Enter subject as **Travel**.
3. Enter body as **Travel**.
4. Tap on the icon to **send** the email.

**Validate the Hero Card**

1. If the email does not display, you may need to swipe down to refresh your inbox.
2. Tap the email you sent to yourself, if it is not already selected.
3. After about 10 seconds, validate that the Hero Card pops up to prompt to install the **Coupa** app.
4. Tap **Install** to proceed with the installation.
Accept the prompt for Application Installation

Click **Install** to proceed with the installation of the Coupa app.

Validate the App Installation

Press the home button of the iOS Device to return to the Spring Board. Validate that the **Coupa** application is installed as initiated from the Hero Card within the Boxer email.
Un-enrolling Your Device

You are now going to un-enroll the iOS device from Workspace ONE UEM.

**NOTE - The term "Enterprise Wipe" does not mean reset or completely wipe your device. This only removes the MDM Profiles, Policies, and content which the AirWatch MDM Agent controls.**

It will NOT remove the AirWatch Agent application from the device as this was downloaded manually before Workspace ONE UEM had control of the device.

**Enterprise Wipe (un-enroll) your iOS device**

Enterprise Wipe will remove all the settings and content that were pushed to the device when it was enrolled. It will not affect anything that was on the device prior to enrollment.

To Enterprise Wipe your device you will first bring up the Workspace ONE UEM Console in a web browser. You may need to re-authenticate with your credentials (VLP registered email address and VMware1 as the password).

1. Click **Devices** on the left column.
2. Click **List View**.
3. Click the **Checkbox** next to the device you want to Enterprise Wipe.
NOTE - Your Device Friendly Name will very likely be different than what is shown. It will, however, be in the same location as shown on image in this step.

Find the Enterprise Wipe Option

1. Click More Actions. NOTE - If you do not see this option, ensure you have a device selected by clicking the checkbox next to the device.
2. Click Enterprise Wipe under Management.
Enter your security PIN

After selecting Enterprise Wipe, you will be prompted to enter your Security PIN which you set after your logged into the console (1234).

1. Scroll down until you see the option for entering Security PIN
2. Enter 1234 for the Security PIN. You will not need to press enter or continue, the console will confirm your PIN showing "Successful" below the Security PIN input field to indicate that an Enterprise Wipe has been requested.

NOTE - If 1234 does not work, then you provided a different Security PIN when you first logged into the Workspace ONE UEM Console. Use the value you specified for your Security PIN.

NOTE - If the Enterprise Wipe does not immediately occur, follow the below steps to force a device sync:

1. On your device, open the AirWatch Agent application.
2. Tap the Device section (under Status) in the middle of the screen.
3. Tap **Send Data** near the top of the screen. If this does not make the device check in and immediately un-enroll, continue to Step #4.
4. If the above doesn't make it immediately un-enroll, then tap **Connectivity [Status]** under Diagnostics.
5. Tap **Test Connectivity** at the top of the screen.

**NOTE** - Depending upon Internet connectivity of the device and responsiveness of the lab infrastructure, this could take a couple of minutes or more if there is excessive traffic occurring within the Hands On Lab environment.

Feel free to continue to the "**Force the Wipe**" step to manually uninstall the Workspace ONE UEM services from the device if network connectivity is failing.

**Verify the Un-Enrollment**
Press the Home button on the device to go back to the home screen. The applications pushed through Workspace ONE UEM should have been removed from the device.

**NOTE - The applications and settings pushed through Workspace ONE UEM should have been removed. The Agent will still be on the device because that was downloaded manually from the App Store. Due to lab environment settings, it may take some time for the signal to traverse through the various networks out and back to your device. Continue on to the next step to force the wipe if the needed.**
Force the Wipe - IF NECESSARY
If your device did not wipe, follow these instructions to ensure the wipe is forced immediately. Start by opening the iOS **Settings** app.

1. Tap **General** in the left column.
2. Scroll down to view the **Device Management** option.
3. Tap **Device Manager** at the bottom of the list of General settings.

**Force the Wipe - IF NECESSARY**

![Device Manager screenshot]

Tap the **Device Manager** profile that was pushed to the device.
Force the Wipe - IF NECESSARY

1. Tap **Remove Management** on the Device Manager profile.
   
   **NOTE - If prompted for a device PIN, enter it to continue. VMware provisioned devices should not have a device PIN enabled.**

2. Tap **Remove** on the Remove Management prompt.

After removing the Device Manager profile, the device will be un-enrolled. Feel free to return to the **Verify the Un-Enrollment** step to confirm the successful un-enrollment of the device.
Conclusion

Mobile Flows helps users to perform majority of business critical tasks from a single app which significantly reduces the overhead of switching amongst different apps and the related configurations. Mobile Flows Connectors are the components responsible for interacting with the business systems. These are offered out-of-the-box for a quick adoption and also open sourced so that they can be customized as per various use cases.
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-1957-03-UEM

Version: 20181104-163017