# Table of Contents

Lab Overview - HOL-1951-01-VWS - VMware Workspace ONE Getting Started .......... 2  
Lab Guidance ............................................................................................................. 3  
Module 1 - Workspace ONE Overview (15 minutes) .................................................. 9  
  Introduction ............................................................................................................... 10  
  Workspace ONE Features ....................................................................................... 12  
  Workspace ONE Architecture for Horizon ............................................................. 15  
  Workspace ONE Login ............................................................................................ 18  
  vIDM Admin Console ............................................................................................. 23  
  Conclusion ............................................................................................................... 28  
Module 2 - Workspace ONE Integration with Horizon 7 (15 minutes) .................... 30  
  Introduction ............................................................................................................... 31  
  Benefits of Integrating Workspace ONE and Horizon 7 ........................................ 32  
  Considerations for Integrating Workspace ONE with Horizon 7 ............................ 34  
  Review Configuration of Horizon 7 ........................................................................ 35  
  Review Configuration of VMware Identity Manager ............................................ 40  
  Verify User Access to Desktop in Workspace ONE ................................................ 44  
  Conclusion ............................................................................................................... 48  
Module 3 - Overview of Workspace ONE Advanced Integration (30 minutes) ....... 49  
  Introduction ............................................................................................................... 50  
  Workspace ONE integration with SaaS applications ............................................. 51  
  Workspace ONE UEM (formerly AirWatch UEM) ................................................ 62  
  Workspace ONE integration with Citrix ................................................................. 64  
  Conclusion ............................................................................................................... 69
Lab Guidance

Note: It may take 60 minutes to complete this lab. You may 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.

Use VMware Workspace ONE and VMware Horizon Single Sign-On to launch applications and desktops as an end user. Explore Workspace ONE integration with VMware Horizon 7, Accessing SAML based web applications, Workspace ONE UEM (formerly AirWatch UEM) and Citrix.

Lab Module List:

- **Module 1 - Workspace ONE Overview** (15 minutes) (Basic) This lab is an introduction to Workspace ONE and its key features.
- **Module 2 - Workspace ONE integration with Horizon 7** (15 minutes) (Basic) This lab will provide a high level overview of integrating Workspace ONE with Horizon 7.
- **Module 3 - Overview of Workspace ONE Advanced Integration** (30 minutes) (Basic) The lab will explain and demonstrate Workspace ONE integration with SAML Based Web Applications, Workspace ONE UEM (formerly AirWatch UEM) and Citrix integration.

Lab Captains:

- Laurel Spadaro, Senior Solution Engineer, US
- Pamela Norris, Staff TAM/DWS TAS, US
- Karsten Giessen, Staff Solution Engineer, US

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 your lab has not changed to "Ready", please ask for assistance.
Module 1 - Workspace ONE Overview (15 minutes)
Introduction

VMware Workspace ONE is a simple and secure enterprise platform that delivers and manages any app on any device by integrating identity, application, and enterprise mobility management.

Workspace ONE is built on the VMware Workspace ONE Unified Endpoint Management (formally AirWatch UEM) technology and integrates with virtual application delivery (VMware Horizon) on a common identity framework. With Workspace ONE, organizations can now evolve siloed cloud and mobile investments, enabling all employees, devices and things across the organization to accelerate their digital transformation journey with a platform-based approach.

It begins with consumer simple, single sign-on access to cloud, mobile, web and Windows apps in one unified catalog and includes powerfully integrated email, calendar, file and social collaboration tools that engage employees. Employees are put in the driver seat to choose their own devices or benefit from employer provided devices with the ability for IT to enforce fine-grained, risk-based conditional access policies that also take into account device compliance information delivered by Workspace ONE Unified Endpoint Management technology. Workspace ONE automates traditional on-boarding and laptop and mobile device configuration, and delivers real-time application lifecycle management that bridges between legacy enterprise client-server apps to the mobile cloud era. The Workspace ONE platform is powered by Intelligence and uniquely combines workspace data aggregation and correlation to deliver integrated insights and automation that help organizations manage complexity and security without compromising on user experience.

Workspace ONE Digital Workspace Platform
Workspace ONE is a digital workspace PLATFORM that enables our IT customers to empower their workforce to securely bring the technology of their choice (devices and apps) at the pace and cost the business needs. It is built on two key tenets of consumer simple and enterprise secure. At the end of the day, if the technology you deliver is unusable, you will be back to square one, where your employees will start bypassing IT and bring in their tools of choice resulting in cost and lack of security. With Workspace ONE you now can meet your business objectives by delivering a great user experience and you don’t need to compromise enterprise security to get there.

**Digital Workspace**

Workspace ONE is truly the industry's first digital workspace platform breaking across silos. Combining unified endpoint management together with a layer of identity that provides capabilities, such as single sign on, a single catalog experience to access all of the applications or multi-factor authentication.

The focus of this lab is virtual application delivery integrating Workspace ONE with Horizon. The HOL-1957 labs go over the Workspace ONE integration with VMware Unified Endpoint Management technology.
Workspace ONE Features

Workspace ONE provides

- Choice to use any device
- Secure Productivity Apps
- Data Security and Endpoint Compliance
- Real-time App Delivery and Automation
- Seamless Access to Apps
- Integration with Horizon

Consumer-simple access to cloud, web, mobile, Windows and Mac Apps

On-boarding new apps and new employees couldn't be easier. Once authenticated through the VMware Workspace ONE app, employees will instantly access their personalized enterprise app catalog where they can subscribe to virtually any published app, VDI Desktop, Web/SaaS. Workspace ONE simplifies application and access management by offering single sign-on (SSO) capabilities and support for multi-factor authentication.
Choice to use any device; BYOD or Corporate Owned

The architecture you deploy today needs to work with devices coming in the future. Keeping employees productive means that their apps need to be available when and where they are. While some of these devices may be corporate owned and require IT to configure and manage them through their lifecycle, many will be owned by the employees themselves. VMware Workspace ONE with adaptive management puts the choice in employees hands for the level of convenience, access, security and management that makes sense for their workstyle providing friction-free adoption of BYOD programs while getting IT out of the device business.

Secure Productivity Apps: Mail, Calendar, Docs and Social

Workspace ONE includes email, calendar, contacts, documents, and chat that employees want to use while invisible security measures protect the organization from data leakage by restricting how attachments and files can be edited and shared.

Data Security and Endpoint Compliance with Conditional Access

To protect the most sensitive information, Workspace ONE combines identity and device management to enforce access decisions based on a range of conditions from strength of authentication, network, location, and device compliance.

Further building on security themes, Workspace ONE provides options for Data Loss Prevention (DLP) and multifactor authentication (MFA) technology to ensure that enterprise information is protected on mobile platforms. When additional means of authentication are required, you can also easily implement a secure and easy-to-use solution.

Real-time App Delivery and Automation

Workspace ONE takes full advantage of the new capabilities of Windows and leverages the industry leading Workspace ONE Unified Endpoint Management or UEM (formally AirWatch UEM) technology to enable desktop administrators to automate application distribution and updates on the fly. Combined with award-winning Horizon virtualization technology, automating the application delivery process enables better security and compliance.

Seamless Access to Apps

Making end-user access to applications seamless is a sure way to encourage adoption of those apps, so Workspace ONE introduces One-Touch Mobile SSO. This feature allows use of capabilities, such as Apple Touch ID on an iPhone, fingerprint readers on Android...
devices, and Microsoft Windows Hello on a Surface Pro, to provide a password-free and secure means of logging in to all the applications that end users need.

**Integrates with Horizon**

Workspace ONE integrates with VMware Horizon either to cloud-hosted virtual desktops and applications with VMware Horizon Cloud Service or to VMware Horizon 7 on-premises virtual desktops and published applications. This integration provides fast SSO access to a Windows 10 desktop or set of Windows applications for those users that require it.

The solution integrates tightly with infrastructure services such as Microsoft Active Directory, DNS, certificate services, and edge services, such as load balancing and firewalls, to provide a highly available, secure, and federated solution.

Module 2 of this lab will go over Horizon integration with Workspace ONE.
Workspace ONE Architecture for Horizon

VMware Identity Manager is a key component of VMware Workspace ONE.

VMware Identity Manager

VMware Identity Manager provides single sign-on (SSO) to an application store for software-as-a-service (SaaS)-based Horizon 7, Citrix, VMware ThinApp and web applications, as well as for Horizon 7 Virtual Desktops and Published Apps. It also provides a set of networking and authentication policies to control application access. We can create detailed rules specifying specific authentication rules based on range, what device the request is coming from, and the Active Directory group. It is important that you connect Workspace ONE to an existing directory infrastructure. You can
configure Workspace ONE to use Active Directory or another LDAP based directory, for user synchronization, authentication, and application access.

Identity Manager Architecture Overview

The diagram illustrates a typical production architecture for VMware Identity Manager in a production Horizon environment.

VMware Identity Manager can be implemented using on-premises or SaaS-based implementation models. We used the on-premises model in this lab environment.

In a SaaS-based implementation, a VMware Identity Manager Connector virtual appliance synchronizes user accounts from Active Directory to the VMware Identity Manager service. Applications can then be accessed from a cloud-based entry point.

In an on-premises deployment, like this lab, VMware Identity Manager is available as either a Linux-based virtual appliance or as a service installed in a Windows VM. The Windows-based installer is a component of the VMware Enterprise Systems Connector,
which also contains the AirWatch Cloud Connector (ACC). For this lab, we used the Linux-based virtual appliance.

VMware Identity Manager can also be integrated with the rest of the Horizon 7 Enterprise components to provide access to Horizon 7 desktops and published applications. The VMware Identity Manager VM handles authentication and provides SSO services to applications and desktops. You will see how that integration is done later in this lab.

Syncing resources such as Active Directory and Horizon 7 and can be done either by using a separate VMware Identity Manager Connector or by using the built-in connector of an on-premises VMware Identity Manager VM. The separate connector can run inside the LAN in outbound-only connection mode, meaning the connector receives no incoming connections from the DMZ.

VMware Horizon users can access Workspace ONE from a Browser. For Mobile users, the end-user component is the Workspace ONE application. Access the application catalog can be done from either the browser or a native mobile application. End-users can install the Workspace ONE native application through the public application store on Android, iOS, and Windows 10. Once installed, end-users will login with their Active Directory credentials and see the applications that IT has enabled access to.

Applications with a star near the download button will require enrolling in management, which means that we will use the device APIs to handle endpoint management and ensure compliance. For applications that contain sensitive data, enrolling in management is the way to go, since it provides greater security including encryption, data protection, compliance, and removing enterprise applications when a device gets unenrolled.

End-users also get the benefit of mobile single sign-on, or as some call it, password-less authentication. For iOS a Kerberos certificate is passed down to the end-user device. For users who are successfully signed in to their domain, access to their Workspace ONE apps portal without additional credential prompts. Its really a win-win for IT and end-users.

Workspace ONE supports one-touch login that can be used by Android, iOS 9 and later, and Windows 10 devices. One-touch login establishes trust between the user, device, and enterprise for one-touch authentication. For more sensitive applications, IT can enable biometric or other multifactor authentication methods.

Horizon users typically access all their Workspace ONE resources, including VMware Horizon apps and desktops, SaaS-based SAML apps, with a web browser through the unified Workspace ONE app catalog. You will see the login and user experience in the next module.
Workspace ONE Login

Workspace ONE provides employees with a complete, self-service enterprise app catalog that can be easily customized and branded for your company.

We will be accessing Workspace ONE from a browser. This lab is using an on premise version of Workspace ONE as part of Horizon Enterprise.

Login Experience Across Devices

It begins with consumer simple, single sign-on access to cloud, mobile, web and Windows apps in one unified catalog.

Open Chrome Browser from Windows Quick Launch Task Bar

1. Click on the Chrome Icon on the Windows Quick Launch Task Bar.

Launch Workspace ONE in Chrome Browser

1. Click on the WS1 Bookmark in the Chrome Browser
2. Click on the VIDM-01 Bookmark

This will open up the login for Workspace ONE. The URL is https://vidm-01.corp.local
Login as User1Mod1 on Workspace ONE

1. Enter **User1Mod1** for the Username
2. Enter the password of **VMware1!**
3. Click **Sign In**

This will log User1Mod1 into Workspace ONE so we can view which applications this user has access to.
Explore the Workspace ONE Catalog

Let's explore the Workspace ONE

1. Workspace ONE App
2. Ability to Search the application catalog to quickly find the users apps.
3. Personalized App Catalog. This shows the apps that this user has in their catalog. User is also able to set Bookmarks for most frequently used apps in their catalog.
4. Shows what in the catalog that this user has been given access to. Can be Virtualized Apps, Published Apps, SaaS and Web Apps, Virtual Desktops, Linux Desktops, or 3D Graphic Resources.
5. Single Sign-on. Shows which user is logged in. In this case you will see the User1Mod1 user.
6. You can organize resources into logical categories to make it easier for users to locate the resource they need in their Workspace ONE portal.
Apps Made Available to User

The Workspace ONE app catalog is the repository of all the resources that you can entitle to users. Users can access enterprise applications that you manage in the Workspace ONE catalog based on the settings you establish for the application.

The User1Mod1 user has been given access in their catalog to the apps listed.

We will show the launching of these apps in other Modules of this lab. We will not be clicking on these apps in this module.

You can click on Calculator just to see it launch and you are not asked for authentication since you authenticated through Workspace ONE. We will talk more about that in the next lessons.

If you opened Calculator, click X in the top right corner to close the application.
Sign User Out of Workspace ONE

You can sign out of the Workspace ONE app.

1. Click on the drop down arrow next to the user User1Mod1 in upper right corner.
2. Click on Sign Out from that drop down.
vIDM Admin Console

The VMware Identity Manager administration console is a web-based application for managing your cloud instance, or tenant. VMware Identity Manager services provide the identity-related components, including authentication for users who single sign-on to their resources for the VMware Workspace ONE platform.

Getting Started with vIDM

To deploy VMware Identity Manager, you deploy the OVF template using the vSphere Client or the vSphere Web Client, power on the VMware Identity Manager virtual appliance, and configure settings. After the VMware Identity Manager virtual appliance is deployed, you use the Setup wizard to set up the VMware Identity Manager environment.

You can use the administration console to entitle users to managed multi-device access to your organization's applications, including Windows applications, software as a service (SaaS) applications, and View or Horizon desktops. The admin console is used not only to manage identity management but also it controls the look and feel of the Workspace ONE Portal.

*The vIDM environment has already been set up for you in the Module. We will just explore the Admin Console for vIDM as Administrator.*
Sign in as Administrator to vIDM Admin Console

Click on the WS1 pull down saved bookmark and click on VIDM-01 Admin. We will log in as Administrator.

Sign in with username: Administrator and password VMware1! then click Sign In.
Lets Explore the Admin Console for Workspace ONE

The first thing that an administrator sees in the Admin Console is the User Engagement Dashboard.

The HOL-1951-03 Workspace ONE Advanced lab in Module 1 - Installation and Configuration of VMware Identity Manager has a detailed walk-through of the Admin Console.
Customize Branding

You can customize the logos, fonts, and background that appear in the administration console, the user and administrator sign-in screens, the Web view of the Workspace ONE applications portal, and the Web view of the Workspace ONE application on mobile devices.

1. To see this click on **Identity & Access Management** Tab in Workspace ONE Admin Console,
2. Click on **Setup** on the Right side
3. Click on **Custom Branding** Tab
4. You can see from this **Names & Logos** screen that you can customize: Company Name, Product Name, Favicon
5. And from the **Sign-In Screen** you can customize: Logo, Background Color, Box Background Color, Login button Background color, and Login Button text color.
Sign out of Admin Console and Workspace ONE

1. Click the arrow for the **Corp Administrator** pull down
2. Select **Logout**.
Conclusion

In this module you learned about what Workspace ONE is. This module went over the Workspace ONE features. The module also showed a user logging into Workspace ONE app.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on Workspace ONE, try one of these:

- Click on this https://www.vmware.com/products/workspace-one.html
- Or go to https://tinyurl.com/y73e7lwv
- Or use your smart device to scan the QRC Code.

You can find more information on VMware Workspace ONE on our Techzone Website:

https://techzone.vmware.com/resource/workspace-one

Proceed to any module below which interests you most.

- **Module 2 - Workspace ONE Integration with Horizon 7** (45 minutes)
  Workspace ONE user experience of launching applications and desktops. The lab will explain and demonstrate Workspace ONE integration with Horizon 7
- **Module 3 - Overview of Workspace ONE Advanced Integration** (30 minutes)
  The lab will explain and demonstrate Workspace ONE integration with SAML Based Wed Applications, Workspace ONE UEM (formerly Airwatch UEM) and Citrix
If you do not want to continue to the next module you can End the Lab

If you do not want to continue to the next two modules then you can end your lab

Click on the **END** button.
Module 2 - Workspace ONE Integration with Horizon 7 (15 minutes)
Introduction

This Module contains a high level overview of integrating Workspace ONE with Horizon 7. You will be:

- Reviewing the benefits of integrating the two solutions
- The process involved to integrate the two solutions
- Reviewing the Horizon feature Workspace ONE mode.
- Launch a Horizon Virtual Desktop from the Workspace ONE portal.

If you are interested in more advanced options on how to integrate VMware Workspace ONE with Horizon 7 please visit the VMware Workspace ONE - Advanced Topics (1951-03-VWS).
Benefits of Integrating Workspace ONE and Horizon 7

VMware's Workspace ONE provides simple and secure access to any application on any device. Also referred to as a Bring-Your-Own Anything. Offering flexibility to the users by allowing them to choose what device they are accessing a variety of applications from. While providing IT the ability to manage all the devices from a single console.

Horizon 7 is an enterprise class virtual desktop solution that allows users to access their virtual desktop and RDSH applications through a single client.

Though cloud based applications have grown in popularity there is still a need for virtual desktops in today's market. Whether it be because a particular set of applications still requires computing resources supplied by a virtual desktop or your users like to access their applications in a way they are comfortable with. By integrating the two solutions you get the best of both worlds.

Licensing

In order to integrate Workspace ONE with Horizon 7 you will require an Advanced, Enterprise, Horizon Apps Standard, or Horizon Apps Advanced License. Each of those
versions come with VMware Identity Manager Standard. VMware Identity Manager (vIDM) is the appliance, along with a software layer within the appliance, that supports the Workspace ONE portal.
Considerations for Integrating Workspace ONE with Horizon 7

When preparing to integrate the two solutions there are a few factors that should be considered.

**Determine Deployment Type**

VMware offers Workspace ONE and Horizon 7 on-premise, cloud based, and hybrid deployment options. With the on-premise option, the software is installed and runs on computing resources that are located in your datacenter and managed by you. To learn more about VMware's on premise solution visit our VMware Horizon 7 Enterprise Advanced Lab (1951-04). Cloud based solutions are where services such as compute, storage, networking and applications are provided to you as a service. VMware's cloud based offerings include VMware Horizon Cloud Hosted, Horizon Cloud on Microsoft Azure, and Horizon on VMware Cloud on AWS. Each solution offers a variety of features and functionality. To find out more about these solutions please visit:

VMware Horizon Cloud Service on Microsoft Azure - Getting Started Lab (1954-01-ISIM)

VMware Horizon Cloud with Hosted Infrastructure - Getting Started Lab (1955-01-ISIM)

Horizon 7 Enterprise - Advanced Topics| Module 3 - Horizon on VMware Cloud on AWS Lab ( 1951-04-VWS)

A hybrid deployment is a combination of on-premise and a cloud based deployment options.

In this lab we will be using an on-premise configuration.

**Version Requirements**

The Horizon Client, Horizon/Horizon (7), and the VMware Identity Manager appliance must all be running versions of said product that are compatible with each other. Please consult the [VMware Product Interoperability Matrices](#) to confirm interoperability.
Review Configuration of Horizon 7

Once Horizon 7 and Workspace ONE are up and running, there are some additional configuration steps required to integrate the two solutions. First you will review the settings in Horizon.

Launch Google Chrome

1. From the Main Console, launch Google Chrome

Open New Tab

1. From within Chrome, open a new tab

Launch Horizon Console

1. Select the Horizon bookmark folder
2. Select Horizon-01-Admin short cut
Login to Horizon Console

1. Enter password **VMware1!**
2. Click on **Log In**

Review Horizon Settings

Integration between Workspace ONE and Horizon is performed utilizing SAML 2.0. This setting is defined in the Connection Server settings. The View Connection Server(s) are responsible for brokering the connection between the user and their Virtual Desktop or Applications published by Horizon. To navigate to the Connection Server settings:

1. Click on **View Configuration**
2. Click on **Servers**
3. Click on the **Connection Servers** tab
4. Highlight **HORIZON-01**
5. Click on **Edit**

**Modify SAML Authenticator Settings**

1. Click on the **Authentication** tab

The SAML authenticator allows for the security credentials to be shared between the Horizon and vIDM environments. The SAML authenticator is defined per connection server. If you have multiple Connection Server Instances, you must associate the SAML authenticator with each instance. By default SAML is set to disabled. In this lab it is currently configured as Allowed. SAML must be set to Required in order to use Workspace ONE mode.

2. Click on the drop down arrow next to **Allowed**
3. Select **Required**
Workspace ONE Mode

Starting with Horizon 7.2 with Workspace ONE version 2.9.2 you can use Workspace ONE mode. Once enabled, when a user tries to access their published application or desktop through the Horizon Client, the user is redirected to the Workspace ONE portal. This allows for the enforcement of access policies defined in VMware Identity Manager (vIDM).

1. Check the **Enable Workspace ONE mode** box mode to enable this feature
2. Enter the host name of the vIDM appliance, in this case enter **vidm-01.corp.local**
3. Check **Block connections from clients that don't support Workspace ONE mode**. This will require users to be on Horizon Client 4.5 or later.
4. Click on **OK**
Verify Pool Entitlement

An Entitlement is how a user or group is granted access to an application or virtual desktop pool within Horizon. The same user or group that will be accessing the Workspace ONE portal must be defined as an Entitlement in Horizon View.

1. Click on Catalog
2. Click on Desktop Pools
3. Double-click on the instant clone pool IC-Pool1

Review Entitlements

1. Click on Entitlements
2. Confirm Domain Users/corp.local is listed
Review Configuration of VMware Identity Manager

Now you will review the configuration within VMware Identity Manager (vIDM).

Login to Workspace ONE

1. Open a new tab in Google Chrome

Launch Administration Console

1. Select the WS1 bookmark folder
2. Click on the VIDM-01 Admin shortcut
Login to Administration Console

1. Enter username: **administrator**
2. Enter password: **VMware1!**
3. Click on **Sign in**

Review Settings

Their are some additional settings within vIDM that must be configured.

User Attributes
A user attribute is a particular property within the user's account, in the lab it is Active Directory. In order for Workspace ONE to integrate with Horizon specific user attributes are required.

1. Click on **Identity & Access Management**
2. Click on **Setup**
3. Click on **User Attributes**
4. Scroll down
5. Confirm the check box next to **distinguishedName and userPrincipalName** has been selected

**Virtual Apps**

1. Click on drop down arrow next to **Catalog**
2. Select **Virtual Apps**

Virtual Apps Collections are defined in the Virtual Apps section of the catalog. A Virtual Apps Collection contains the configuration information that is used to synchronize data between vIDM and Horizon desktops (on-premise), Citrix published resources, Horizon Cloud, or Thin App.

3. Click on **Virtual App Configuration**

**Identity Manager Connector**

The Virtual Apps Collection is performed by the Identity Manager Connector.

You can create one or multiple connectors for any type of Virtual App excluding Thin App. Multiple collectors are used for load distribution.
1. In the lab the Horizon View On-Premise connector has been configured.

When new and or updated entitlements or pools have been defined within Horizon, a synchronization between VMware Identity Manager (vIDM) and Horizon must be performed. This is done from within vIDM. During the synchronization process, the Horizon Connector collects the Horizon pools and their corresponding entitlements. By default the Sync Frequency is set to Weekly, but can be defined within the connector. You also have the ability to perform a manual synchronization by clicking on Sync under Actions.

Logout of VMware Identity Manager

1. Click on the drop down arrow next to Corp Administrator
2. Select Logout

Minimize Google Chrome

1. Click on - to minimize Google Chrome
Verify User Access to Desktop in Workspace ONE

Now you are ready to verify the user can access their desktop through Workspace ONE.

Launch the VMware Horizon Client

1. Click on the VMware Horizon Client located on the Main Console Desktop

Connect to the Horizon Connection Server

1. Select horizon-01.corp.local, which is the connection server you just configured
**Login as User**

Notice how you were redirected to the Workspace ONE portal! This was due to the fact that you enabled Workspace ONE mode earlier in this lab.

1. Enter username: user1mod2
2. Enter password: VMware1!
3. Click on **Sign in**

Note: If you were not redirected to the Workspace ONE logon screen, confirm the horizon-01.corp.local connection server was chosen.
Launch Desktop

The Horizon desktop pool, you verified the entitlement of previously in this lab, is listed.

1. Click on Open on the Instant Clone Pool to launch the users virtual desktop

Review Desktop
You are now logged into your virtual desktop.

**Sign Out**

1. Right click on the **Windows logo**
2. Select **Shut down or sign out**
3. Select **Sign out**

**Verify Disconnected**

You have been disconnected.

1. Click on **Close** to disconnect from laptop

**Close Google Chrome**

1. Click on the **X** to close Google Chrome
Conclusion

You have just reviewed the process of integrating Workspace ONE with Horizon. The combination of the two solutions, provides the secure access to a user's virtual desktop or application published by Horizon View from any device. To learn more about the integration of the two solutions please visit the VMware Workspace ONE Advanced Lab (1951-03).

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on integrating Workspace ONE with Horizon 7 try one of these:

- Click on this link
- Or go to https://tinyurl.com/y8a33ow3
- Or use your smart device to scan the QRC Code.

Proceed to any module below which interests you most.

- **Module 1 - Workspace ONE Overview** (15 minutes) (Basic) This lab is an introduction to Workspace ONE and its key features.
- **Module 3 - Overview of Workspace ONE Advanced Integration** (30 minutes) (Basic) The lab will explain and demonstrate Workspace ONE integration with SAML Based Wed Applications, Workspace ONE UEM (formerly AirWatch UEM) and Citrix integration.

How to End Lab

To end your lab click on the END button.
Module 3 - Overview of Workspace ONE Advanced Integration (30 minutes)
Introduction

The lab will explain and demonstrate Workspace ONE integration with SaaS applications, Workspace ONE Unified Endpoint Management (formerly AirWatch UEM) and Citrix.
Workspace ONE integration with SaaS applications

With VMware Workspace ONE, you can provide Single-Sign-On (SSO) for your users to any Web or Software-as-a-Service (SaaS) application supporting Security Assertion Markup Language (SAML).

This will simplify a user’s digital workspace experience by allowing the user to have a single entry point for all applications (ThinApps, Citrix XenApp, RDSH, SaaS) and VDI Desktops from any device offering a browser. With VMware AirWatch, you can even extend this to mobile apps.

Workspace ONE Portal

Users can customize their portal by adding application bookmark from the catalog as shown in the sample picture of Workspace ONE portal above.

Show Workspace ONE and launch SaaS app

Integration uses the SAML 2.0 standard to establish mutual trust, which is essential for single sign-on (SSO) functionality. When SSO is enabled, users who log in to Workspace ONE with Active Directory credentials can launch remote desktops and applications without having to go through a second login procedure.
We have configured single sign-on for SAML-based apps with VMware Identity Manager and Workspace ONE.

**Open Chrome Browser from Windows Quick Launch Task Bar**

1. Click on the **Chrome Icon** on the Windows Quick Launch Task Bar.

**Start SAML Test App VM**

Due to resource constrains, not all VMs in this lab are started automatically. Before we begin this module, we need to start our SAML Test App VM.

1. Open a new Chrome Browser window and click on **vCenter**
2. Select RegionA vSphere Client (HTML)
3. Select **Use Windows session authentication**
4. Click **Login**

*We need to start the SAML-test VM if it isn't already started.*
Verify VM is started

1. Expand the RegionA01-COMP01 under RegionA01 of vcsa-01a.corp.local
2. Click on SAML-TEST
3. Verify the SAML-TEST is running and has an IP-Address

If VM is already powered on then you can skip the next step "Power ON SAML-Test" and Continue to Launch Workspace ONE.
Power On SAML-Test

Confirm that it is powered on or power on the SAML-Test VM. If the SAML-TEST VM is already powered on, you can skip this step.

1. Expand RegionA01-COMP01
2. Find the SAML-Test VM and right-click
3. Select Power from the menu
4. Select Power On

It only will take a couple seconds for the VM to start. If Power On is not an option move to next step to verify it is already started.

Launch Workspace ONE in Chrome Browser
1. Click on the **WS1** Bookmark in the Chrome Browser
2. Click on the **VIDM-01** Bookmark

This will open up the login for Workspace ONE. The URL is https://vidm-01.corp.local

**Login as User1Mod3 on Workspace ONE**

![Login to Workspace ONE](image)

1. Enter **User1Mod3** for the Username
2. Enter the password of **VMware1!**
3. Click **Sign In**

This will log User1Mod3 into Workspace ONE so we can view which applications this user has access to.
Apps Made Available to User

Some of these apps will NOT work as we are in a test lab environment and have only been added to show some sample applications.

The User1Mod3 user has been given access in their catalog to the apps listed. We will show the launching the SAML based applications in this test.

1. Click on the **SAML Test** app to View the Details about that app.
Details on the SAML Test App

Here are the details of the SAML Test App including the Version #.

1. Click the **Back** button on the Workspace ONE details page to go back and we will now launch the app.

*You can click the Open button here or go back to the Workspace ONE catalog to Open the SAML Test app.*
Open the SAML Test App

1. Click on **Open** on the **SAML Test** app in the Workspace ONE catalog to launch the SAML Test application.
SAML Test App Launched

You will see a separate Tab open in the Chrome Browser. You will not be prompted for a Username and password since that is passed to the SAML application through Workspace ONE app.

Close SAML Test App Tab

Click the X to close the SAML Test App Tab
Sign User Out of Workspace ONE

You can sign out of the Workspace ONE app.

1. Click on the drop down arrow next to the user **User1Mod3** in upper right corner.
2. Click on **Sign Out** from that drop down.
Close the Workspace ONE browser

Click the X in the top right corner to close the Chrome Browser.

More Info

The Advanced Workspace ONE lab goes into configuring the Web and SaaS applications. **HOL-1951-03-VWS: Module 4 - Integrating Workspace ONE with SAML Based Web Applications.**

The SSO into Horizon Published Apps and Desktops is shown in **Module 2 - Workspace ONE Integration with Horizon 7.** Also the Advanced Workspace ONE lab **HOL-1951-03-VWS: Module 2: Integrating Workspace ONE with Horizon 7.5** has more information on this topic.
Workspace ONE UEM (formerly AirWatch UEM)

- Workspace ONE UEM services, formerly AirWatch, provide device enrollment, application distribution, and compliance checking tools to ensure that remote access devices meet corporate security standards. Users from enrolled devices can log in to their enabled applications securely without entering multiple passwords.

Workspace ONE Unified Endpoint Management (UEM)

![UEM with VMware](image)

**LIFECYCLE MANAGEMENT**
Manage the complete device lifecycle, from onboarding to retirement, across all your desktop, mobile, and purpose-built devices.

**ENDPOINT SECURITY**
Reduce security and compliance risks with unified, well-automated endpoint controls—without impeding productivity.

**INTELLIGENCE**
Leverage data analytics to gain rich insights into user behavior, device usage, and opportunities to improve efficiency.

Years ago, organizations adopted mobile device management (MDM). Then they moved on to enterprise mobility management (EMM). Today, as business requirements shift from connectivity to cross-platform innovation, organizations are thinking more broadly and evolving to unified endpoint management (UEM).

The leading unified endpoint management technology from VMware takes a user-centric approach to enable IT to centrally manage every device, every app, and every mobile use case, both corporate-owned and BYOD. VMware AirWatch powers VMware Workspace ONE, the integrated digital workspace platform.

With Workspace ONE UEM, manage the entire lifecycle of any endpoint (including desktops), across all major operating systems (including Windows 10, macOS, and Chrome OS), and any app, in a single management console. Support all your mobile use...
cases, including: full device management for corporate-owned, app-level management for BYOD, or line of business use cases such as kiosk or shared devices.

**Video link to Workspace ONE UEM Overview**

Click on this link to view a video overview of Workspace ONE UEM

https://www.youtube.com/watch?v=9yui5Fn90Hk

**What's New in Workspace ONE UEM Version 9.5**

Click on the link to view a video on What's New in Workspace ONE UEM Version 9.5

https://www.youtube.com/watch?v=RdwFbcXhRTQ

**Workspace ONE UEM Advanced Labs**

This lab was just an overview of Workspace ONE UEM. For more in depth Hands on please visit our Workspace ONE UEM labs in the HOL-1957 family of labs. Here is a summary of those labs:

- HOL-1957-01-UEM: VMware Workspace ONE UEM with Application and Access Management
- HOL-1957-02-UEM: VMware Workspace ONE UEM - Identity Management
- HOL-1957-03-UEM: VMware Workspace ONE UEM - Intelligence
- HOL-1957-07-UEM: VMware Workspace ONE UEM - Productivity Apps
- HOL-1957-08-UEM: VMware Workspace ONE UEM - Unified Access Gateway
Workspace ONE integration with Citrix

We do not have Citrix apps or desktops in this lab but wanted to cover at a high level the integration with Citrix and Workspace ONE.

You can provide Workspace ONE users access to Citrix-published resources by integrating your Citrix deployment with VMware Identity Manager. Citrix-published resources include applications and desktops within Citrix XenApp and XenDesktop server farms. Desktops are also referred to as Citrix-published delivery groups.

VMware Identity Manager uses the Integration Broker and other components to synchronize Citrix-published resources to VMware Identity Manager and to launch the resources from the Workspace ONE portal or app.

Video Overview of Workspace ONE and Citrix Published Apps

https://www.youtube.com/watch?v=QOsFZfoBOAA

Components required for Citrix Integration

To integrate a Citrix deployment with the VMware Identity Manager service, you need the following components.

- A VMware Identity Manager instance installed on premises.
- An Integration Broker instance installed on a supported Windows server on premises. The Integration Broker, a component of VMware Identity Manager, is the component that communicates with Citrix server farms.

1. You can download the Integration Broker from https://my.vmware.com.

- A Citrix deployment on premises.

While deploying the components, ensure that you meet these requirements:

- The VMware Identity Manager service must be able to communicate with the Integration Broker. If you deploy multiple instances of the service appliance, ensure that all of them can communicate with the Integration Broker.
- The Integration Broker must be able to communicate with the Citrix server farm.
Sync of Citrix-published Resources and Entitlements

VMware Identity Manager synchronizes Citrix-published applications and desktops, and user entitlements, from the Citrix server farm to the VMware Identity Manager service. You can set a sync schedule to sync the resources and entitlements at regular intervals.

The Citrix farm is the single source of truth for all supported operations in VMware Identity Manager. You manage the resources and entitle users to them in Citrix.

When resources or entitlements are added, changed, or deleted in the Citrix farm, the information is updated in VMware Identity Manager after a sync.

Synchronization Architecture Diagram

- Users and groups are synced from your enterprise directory to the VMware Identity Manager service by the VMware Identity Manager connector.
- Citrix-published resources and entitlements are synced from the Citrix server farm to VMware Identity Manager using the connector, Integration Broker, and PowerShell SDK.
Launch of Citrix-published Apps and Desktops

VMware Identity Manager uses the Integration Broker component and the Citrix Web Interface SDK or Citrix StoreFront REST API to launch Citrix-published applications from the Workspace ONE portal or app. You can configure internal and external access to the Citrix-published resources. End users must install Citrix Receiver on their systems or devices to launch the applications and desktops.

Launch Architecture Diagram (Internal Access)

1. A user launches a Citrix-published application or desktop from the Workspace ONE portal or app.
2. The request goes to the VMware Identity Manager service, connector, and Integration Broker.
3. The Integration Broker communicates with the Citrix server farm through the Web Interface SDK or StoreFront REST API to authenticate and request the ICA file.
4. The ICA file is retrieved and passed to the Workspace ONE portal or app.
5. The ICA file is passed to the Citrix Receiver.
6. The Citrix Receiver launches the application or desktop.
Launch Architecture Diagram (External Access)

1. A user launches a Citrix-published application or desktop from the Workspace ONE portal or app.
2. The request goes to the VMware Identity Manager service, connector, and Integration Broker.
3. The Integration Broker communicates with the Citrix server farm through the Web Interface SDK or StoreFront REST API to authenticate and request the ICA file.
4. The ICA file is retrieved and passed to the Workspace ONE portal or app.
5. The ICA file is passed to the Citrix Receiver.
7. Netscaler communicates with the Citrix STA server with the STA ticket and gets the Citrix session server information.
8. Netscaler communicates with the Citrix Session Host server and creates a session for application launch.

Using StoreFront REST API or Web Interface SDK for Launch

The Integration Broker can use the Citrix Web Interface SDK and the Citrix StoreFront REST API to communicate with the Citrix deployment to launch applications or desktops. When the StoreFront REST API is used, the Integration Broker acts like a REST client. The Web Interface SDK and the StoreFront REST API are used to authenticate with and generate the ICA file from the Citrix deployment.
You can specify which option to use by selecting or deselecting the Use StoreFront check box in the Citrix configuration page in the VMware Identity Manager administration console.

An Integration Broker instance can use both the Web Interface SDK and the StoreFront REST API. If you want to communicate with one Citrix farm using the Web Interface SDK and another Citrix farm using the StoreFront REST API, select or deselect the Use StoreFront check box as required.

To use the StoreFront REST API option, which is available in VMware Identity Manager 2.9.1 and later, ensure the following requirements are met.

- Install Integration Broker 2.9.1 or later.
- Ensure that StoreFront is supported by the XenApp or XenDesktop version you are using.
- Ensure that the Integration Broker can communicate with the StoreFront server.

When you enable the StoreFront REST API, the Integration Broker communicates with the StoreFront server to generate the ICA file.

- Enable HTTP Basic Authentication as an authentication method in the Citrix StoreFront store. This is required for internal access only.

### Providing Access to Citrix-Published Resources

You can integrate your Citrix deployment with VMware Identity Manager to provide Workspace ONE users access to Citrix-published resources.

Conclusion

In this module you saw the integration of web-based applications with VMware Workspace ONE. If you are interested in learning how to add web-based applications to the catalog, make sure to take the more advanced LAB for Workspace ONE 
HOL-1951-03-VWS Module 4.

VMware Workspace ONE - Techzone

You can find more information on VMware Workspace ONE on our Techzone Website: 
https://techzone.vmware.com/resource/workspace-one

You've finished the Lab

Congratulations on completing the HOL-1951-01-VWS Lab

How to End the Lab

To end your lab click on the END button.
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-1951-01-VWS

Version: 20181112-174146