## Getting Started with Workspace ONE UEM and Workspace ONE Access

Workspace ONE Access is engine that drives the Workspace ONE Platform. It not only provides Access Management capabilities but it connects the Workspace ONE Platform (and all the hub service components) to your enterprise directories and cloud services (including third party IdP’s).It may not always be clear on how to get started setting up Workspace ONE Access and linking it to your Workspace ONE UEM tenant. In this blog we will walk through the process of getting started with Workspace ONE Access and Workspace ONE UEM.

* [Connecting Workspace ONE Access](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#connectWS1A)
  + [Using the Getting Started Wizard](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#connectWizard)
  + [Validating the Getting Started Wizard](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#validateWizard)
  + [Manually Connecting Workspace ONE Access](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#manualSetupWS1A)
* [Configure Mobile Single-Sign-On Setup](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#configureMSSO)
* [Managing your Users](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#manageUsers)
* [Enabling Intelligent Hub Services](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#enableHubServices)
* [Enabling Workspace ONE Access as Source Authentication](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#enableAccessAuth)
* [Device Enrollment Test](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#deviceEnrollmentTest)
* [Troubleshooting the Enrollment Setup](https://theidentityguy.ca/2021/04/21/getting-started-with-workspace-one-uem-and-workspace-one-access/#troubleshooting)

**Connecting Workspace ONE Access**

To get started we need to connect Workspace ONE Access to Workspace ONE UEM. We always recommend to use the Wizards to get started. However, there are times when the wizards may not be available so I will walk through the process of using the Wizards and the manual steps as well.

**Using the Getting Started Wizard**

1. In Workspace ONE UEM, click on Getting Started (in the top left).
2. Click on Begin Setup for Workspace ONE

A screenshot of a computer

Description automatically generated

1. Scroll down to the “Identity and Access Management” section
2. Under “Connect to Workspace ONE Access”, click Configure.

A screenshot of a computer

Description automatically generated

1. On the splash screen, click Continue

A screenshot of a computer

Description automatically generated

1. Enter your Workspace ONE Tenant URL and your “System Domain” username and password:

A screenshot of a login box

Description automatically generated

1. Click Test Connection and verify that you have a “Test Connection Successful” message.
2. Click Save
3. This section should now be marked as complete

A screen shot of a computer

Description automatically generated

Troubleshooting:

* Verify that that you are using a system domain username and password
* If your Access Tenant was previously connected to another UEM tenant, you will need to delete the configuration from Workspace ONE Access. This can only be done via the API. I will try to add instructions at a later date.
* Make sure you have a Password (Local Directory) authentication method configured in Workspace ONE Access on your default access policy. You might have to move that policy to the top.
* Make sure you’ve not deleted or renamed the built-in IdP. You will need to re-created it.

**Validating the Getting Started Wizard**

So hopefully you ran the wizard successfully. So what did this wizard do?

If you log into your Workspace ONE Access Tenant and go to Identity & Access Management -> Setup (on the far right) -> VMware Workspace ONE UEM. You will now see your UEM tenant configured in Workspace ONE Access:

A screenshot of a computer

Description automatically generated

**Manually Connecting Workspace ONE Access**

As I mentioned before, if the wizards are available, please use the wizards. The wizards will create a service account along with API Keys that exempt from Workspace ONE UEM built-in rate limiting.

**Create a Service Account**

1. In Accounts -> Administrators
2. Create a new “Basic” administrator with the role “Console Administrator” (or AirWatch Administrator) for your Organization Group.
3. Under API, select certificates and create a password
4. Save the User and then export the certificate for the user.

A screenshot of a computer

Description automatically generated

**Create API Keys**

1. In Groups & Settings -> All Settings -> System -> Advanced -> API -> Rest API
2. Enable API Access (if not already enabled)
3. Create two new API Keys. One will be admin and the other will be Enrollment User.

A screenshot of a computer

Description automatically generated

**Configure VMware Workspace ONE UEM in Workspace ONE Access**

1. In the Workspace ONE Access console, go to Identity & Access Management -> Setup -> VMware Workspace ONE UEM
2. Enter your Workspace ONE UEM API URL, ie. [https://as135.awmdm.com](https://as135.awmdm.com/)
3. Upload the certificate you previously created for the service account along with the password
4. Enter your Admin API Key
5. Enter your Enrollment User API Key
6. Enter your top Group ID
7. Click Save
8. In the catalog section, enter your device services URL, ie. [https://ds135.awmdm.com](https://ds135.awmdm.com/)
9. Enable Device Compliance
10. Click Save

**Configure Mobile Single-Sign-On Setup**

We are now going to configure the Authentication Methods in Workspace ONE Access.

1. Lets go back to the “Getting Started Section” of Workspace ONE UEM
2. Under Workspace ONE -> Continue
3. Under Identity & Access Management -> Mobile Single-Sign-On, click Configure

A close up of a sign

Description automatically generated

1. On the splash screen, click “Getting Started”

A screen shot of a computer and phone

Description automatically generated

1. Click Continue
2. Click Start Configuration

A screenshot of a computer

Description automatically generated

1. This can take a few minutes to complete but you should see all green check marks:

A screenshot of a computer

Description automatically generated

**Validating the Mobile SSO Wizard**

If the Mobile SSO Wizard ran successfully, in Workspace ONE Access -> Identity & Access Management -> Identity Providers, you will see the Built-in IDP has been modified to include our new authentication methods:

A screenshot of a computer

Description automatically generated

In Authentication Methods, you will see our new Authentication Methods are configured and Enabled:

A screenshot of a computer

Description automatically generated

In your Access Policies, you will also see that they are pre-configured as well.

**Caveats of the Mobile SSO Wizard**

The Mobile SSO Wizard will definitely save you a lot of time but there are some special caveats that you should be aware:

* The Wizard creates Mobile SSO profiles in Workspace ONE UEM but they are not assigned to any smart groups. You will need to assign the profiles to your smart groups.
* The IOS Mobile SSO profile, in the Single-Sign-On payload, will contain a Realm of “VMWAREIDENTITY.COM” If your Workspace ONE Access tenant is using a different domain like workspaceoneaccess.com or vidmpreview.com, you will need to update the realm. The realm should be in all caps.
* For Android Mobile SSO, the tunnel proxy rule may incorrectly state the proxy url as “cert-proxy.vmwareidentity.com:5262” Please update the proxy URL to point to your correct tenant domain and remove the dash in the cert proxy. The correct value should look like “certproxy.vmwareidentity.com:5262” or “certproxy.workspaceoneaccess.com:5262”
* In the built-in IDP for Workspace ONE Access, you will need to select “All Ranges” for the network range.

If your Mobile SSO Wizard did not complete successfully, you will need to [complete it manually](https://theidentityguy.ca/2020/11/16/setting-up-mobile-sso-manually/).

**Managing your Users**

You need to sync Users into your Workspace ONE UEM and Workspace ONE Access environments. How you create users in Workspace ONE UEM and Access will have an impact on the capabilities or features you can use in the platform.

Its important to note that Workspace ONE UEM and Workspace ONE Access should be sourced from the SAME external identity source. This means if you are using a connector to pull users from Active Directory into Workspace ONE UEM, then you can NOT use Okta to create users in Workspace ONE Access.

**This blog is not intended to go through the intricacies or steps to configure user management but we’ll go through some of the more popular options at a high level.**

First, both Workspace ONE Access and Workspace ONE UEM leverage the “External ID” from the identity source. In both platforms, they contain attributes that need to be mapped to the External ID.

**The External ID in Workspace ONE UEM and Workspace ONE Access need to match.**

Here are some options for managing users:

* Use the Workspace ONE UEM Connector and Workspace ONE Access Connector to sync users from Active Directory
* Use a SCIM Connector to create users in Workspace ONE Access and use the AirWatch Provisioning Adapter to create users in Workspace ONE UEM.
* Use the Workspace ONE UEM Connector to Active Directory and use “Active Directory Basic” in UEM to sync users to Workspace ONE Access.
* Use JIT to create users in Workspace ONE Access and users the AirWatch Provisioning Adapter to create users in Workspace ONE UEM. You will need to make sure that when you JIT users into Workspace ONE UEM that you include an External ID attribute.
* Use JIT to create users in Workspace ONE Access (including the External ID) and use JIT to create users in Workspace ONE UEM (include the same External ID)

**Feature Matrix for User Sync Options**

| **Capability** | **UEM Connector with AD Basic** | **Access Connector** | **SCIM Connector/JIT** |
| --- | --- | --- | --- |
| User/Password Authentication (Single AD Domain) in WS1 Access | Supported | Supported |  |
| User/Password Authentication (Multiple AD Domain – 2 Way Trust) in WS1 Access |  | Supported |  |
| Okta Universal Directory |  |  | Supported |
| Mobile SSO (IOS/Android) | Supported | Supported | Supported |
| Certificate Authentication | Supported | Supported | Supported |
| 3rd Party IDP | Supported | Supported | Supported |
| Radius Authentication |  | Supported |  |
| IWA (Integrated Windows Auth) |  | Supported |  |
| Horizon |  | Supported |  |
| Citrix |  | Supported |  |
| Flexible Sync Schedule | UEM will sync users to Access based on the schedule when users are synced to UEM. | Supported | Supported – Based on capabilities of SCIM Provider |
| Sync Subset of Users | UEM will sync all users to Access | Supported | Supported – Based on capabilities of SCIM Provider |
| People Search |  | Supported |  |
| WS1 Intelligence | Supported | Supported | Supported |
| Universal Catalog | Supported | Supported | Supported |

**Enabling Intelligent Hub Services**

In order to use the full capabilities of Workspace ONE Access, we need to enable Hub Services.

1. In Workspace ONE UEM, go to Groups & Settings -> Configurations
2. If prompted, click Go To Configurations
3. Select Intelligent Hub
4. Select Getting Started
5. Select Yes to Activate Hub Services

A close-up of a web services

Description automatically generated

**Enabling Workspace ONE Access as Source Authentication**

1. In Workspace ONE UEM, go to Groups & Settings -> All Settings
2. Under Devices & Users -> General -> Enrollment
3. Click Override
4. Select Workspace ONE Access for Source of Authentication for Intelligent Hub

A screenshot of a computer screen

Description automatically generated

1. Click Save

**Device Enrollment Test**

1. On your Mobile Device, launch the Workspace ONE Intelligent Hub Application
2. Enter your UEM Device Services Server and your Group ID

A screenshot of a phone

Description automatically generated

1. Click Next
2. You will now be prompted for your credentials (or potentially redirected to a 3rd Party IDP)

A screenshot of a login screen

Description automatically generated

1. Upon Successful Authentication, you should proceed into the enrollment flow:

A screenshot of a phone

Description automatically generated

**Troubleshooting the Enrollment Setup**

* You received an error “No Application found” in Workspace ONE Access
  + Check to make sure you configured Workspace ONE Access Authentication in Enrollment Settings. See Section above.
  + Check to make sure you have configured Hub Services as outlined above
  + If you are doing a Web Enrollment or DEP, you need to configure the AirWatch Application in Workspace ONE Access.

A logo on a white background

Description automatically generated

* You received an Workspace ONE Hub Username & Password Prompt
  + You probably enabled Workspace ONE Access Authentication in Enrollment Settings but you did not enable Hub Services. See Section above.

A screenshot of a computer

Description automatically generated

* You received an error “Failed lookup subscription to resource” in Workspace ONE Access
  + Check to make sure you configured Workspace ONE Access Authentication in Enrollment Settings. See Section above.
  + Check to make sure you have configured Hub Services as outlined above
  + If you are doing a Web Enrollment or DEP, you need to configure the AirWatch Application in Workspace ONE Access and the application is assigned to All Users.

A logo on a white background

Description automatically generated

* You received an error “Access Denied” in Workspace ONE Access
  + Make sure your Device Enrollment Policy includes an authentication method that can be used during enrollment like Password (Cloud Deployment) or 3rd Party IDP.