

Workspace ONE Access and Workspace ONE UEM Integration

Part 1: Workspace ONE UEM integration with Workspace ONE Access

In this section we will do the Workspace ONE UEM side of the configuration.

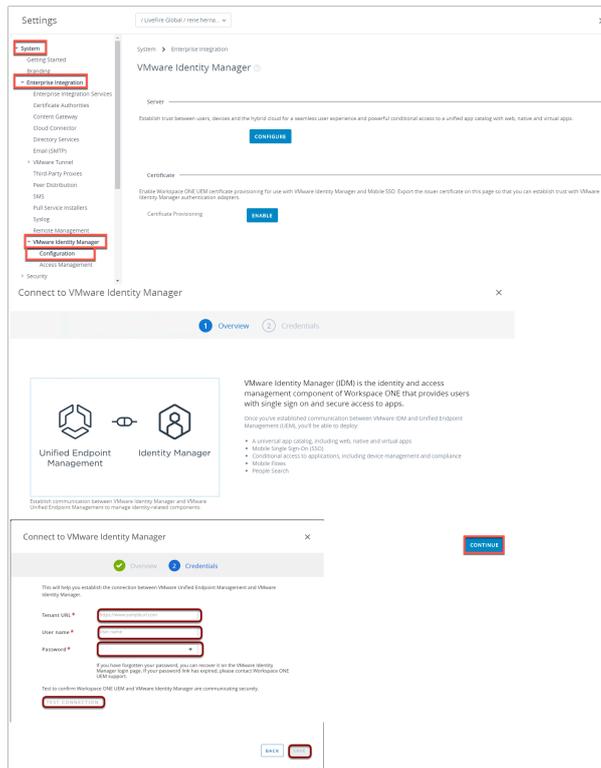
1. Switch back to the Workspace ONE UEM Admin console.
 - Be sure to make these settings at the **company organisation group**, then navigate to [Groups and Settings > All Settings > System > Enterprise Integration > VMware Identity Manager > Configuration](#)
2. Click **CONFIGURE** under **Server** settings
3. Click **CONTINUE**

On the Connect to **VMware Identity Manager** window enter the following:

1. **Tenant URL:** **Your Tenant** eg. <https://aw-euclivefiret3rn.vidmpreview.com>
2. **User Name:** **Your Tenant Admin account**
3. **Password:** **Your Tenant Password**

Select **TEST CONNECTION** to ensure Tenant configuration has been entered successfully.

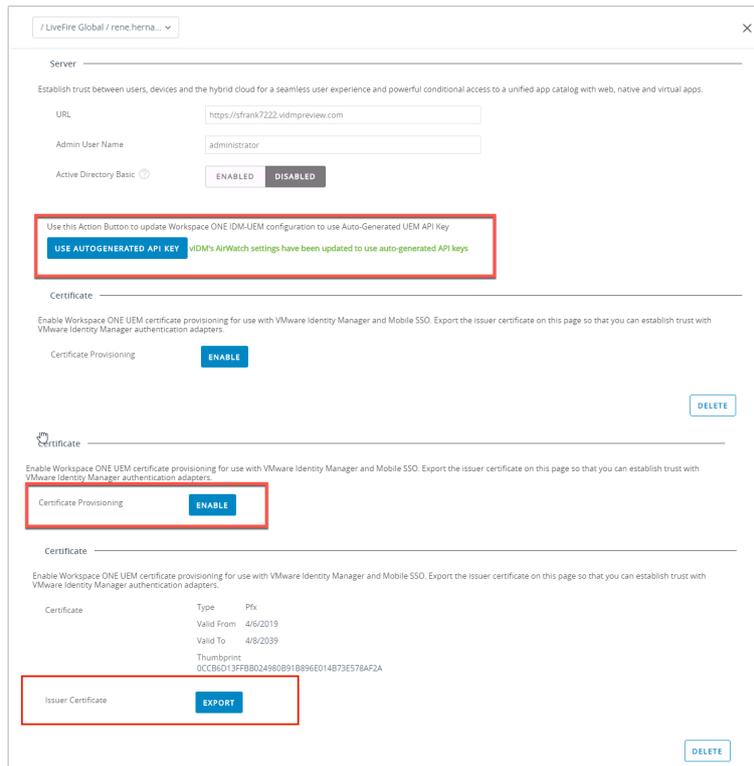
4. Select **SAVE** and close the settings window



1. Click **"Use Autogenerated API KEY"**

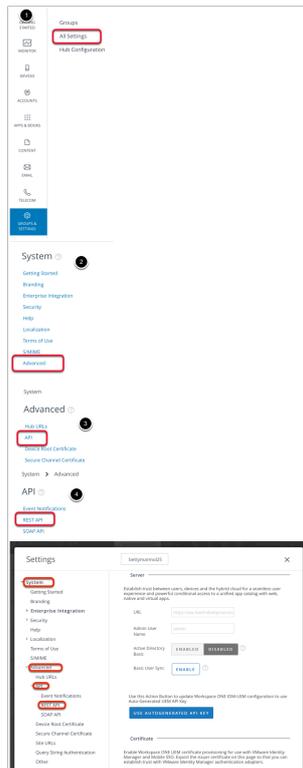
2. In the **Certificate** section, next to **Certificate Provisioning** click **ENABLE** - we will use this certificate later for Single-Sign-On with Windows 10

3. Now click **EXPORT** - we will use this certificate in a later exercise. leave this window open for the next part.



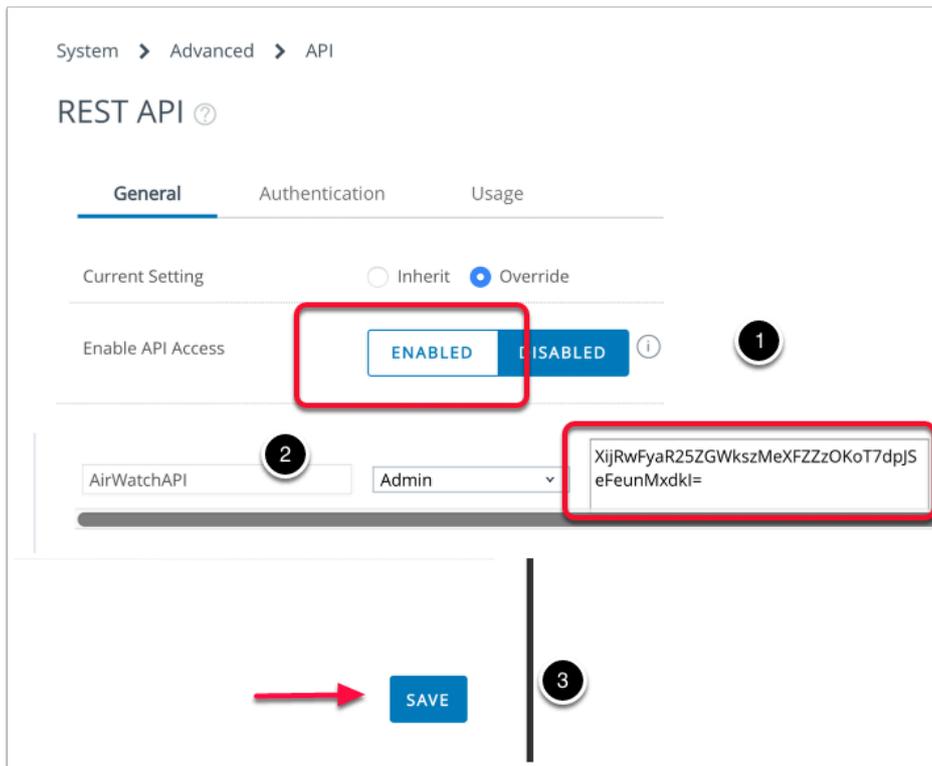
Part 1B. Creating a custom REST API Account

- We will configure this REST API Account in preparation for Part 2 of this Lab
 1. If you closed the settings windows in the previous part navigate in the Workspace ONE UEM Admin Console to **Groups & Settings > All Settings**
 2. Under **System** select **Advanced**
 3. Under **Advanced** select **API**
 4. Under **API** select **REST API**



2. Part 1B. continued..

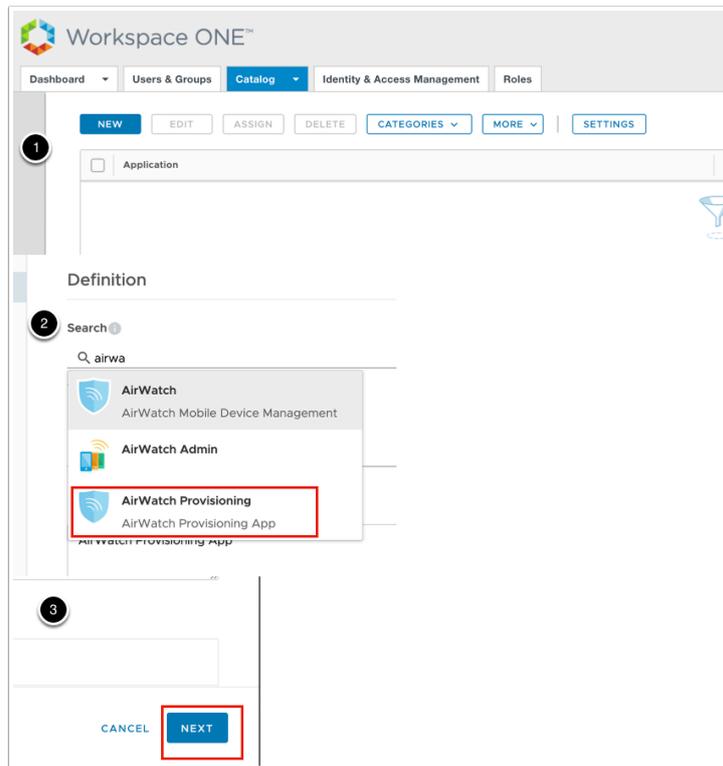
- Creating a custom REST API Account
 1. Under **REST API** under **General** next to **Current Setting** select the **Override radio button**. Next to **ENABLE API Access** ensure that **ENABLED** is selected.
 2. You will notice an **AirWatchAPI Admin** is automatically generated. **Copy the API Token and save to a text editor**
 3. Select **SAVE**
 4. After the settings have been save successfully select the **X** in the right corner to close the window



Part 2: Configuring the AirWatch Provisioning Adaptor in Workspace ONE Access for Workspace ONE UEM

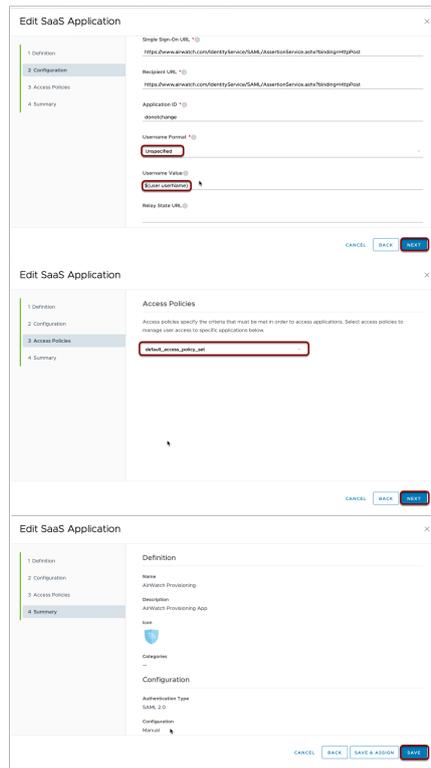
1. AirWatch Provisioning Adaptor

- This first section will be done in the **Workspace ONE Access** SaaS console
 1. In the **Admin Console** select the **Catalog** tab and select **NEW**
 2. On the **New SaaS Application**, next to section **1.Definition** under **search** type **AirWa** and you should see **Airwatch Provisioning**. Select **AirWatch Provisioning**
 3. Select **Next**



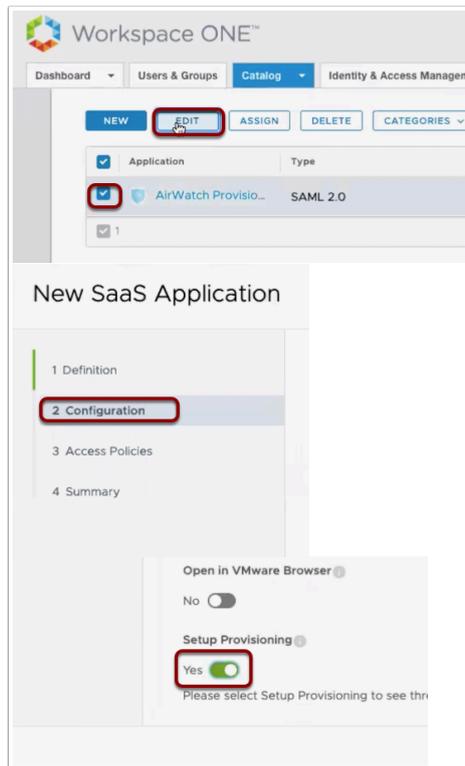
2. AirWatch Provisioning Adaptor

- In the NEW SaaS Application wizard continued...
 1. In Section **2.Configuration** ensure the following is configured:-
 - Under **Username Format** ensure **Unspecified** is selected, Under **Username Value** ensure **`${user.userName}`** is selected and click **NEXT**
 2. In Section **3. Access Policies** accept the default and select **NEXT**
 3. In Section **4.Summary** select **SAVE**



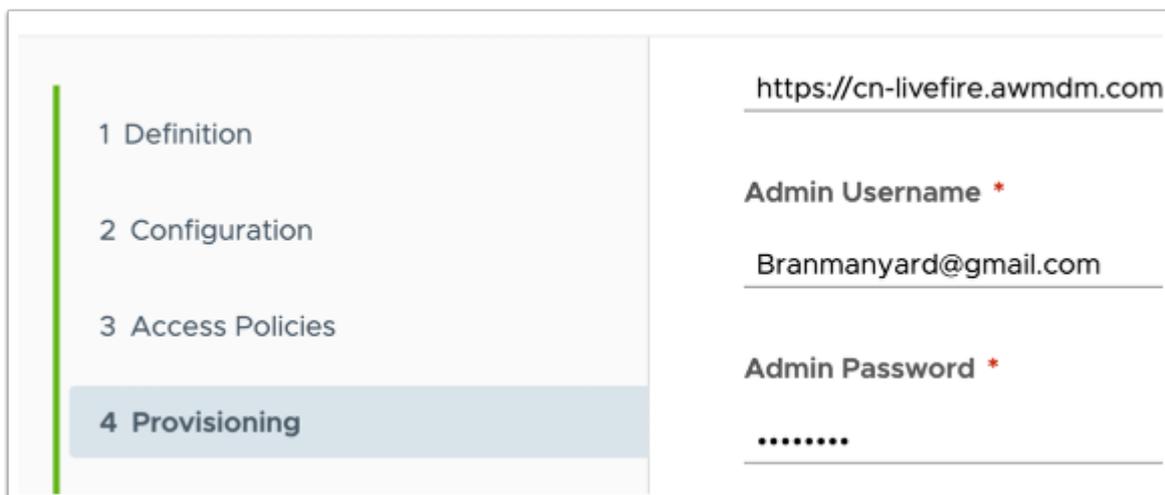
3. AirWatch Provisioning Adaptor

- Under the **Catalog tab**
 1. select the **check box** next to **Airwatch Provisioning** and select **EDIT**
 2. In the **Edit SaaS Application** wizard in the left pane select **2 Configuration**
 3. In the Configuration section **scroll down**, expand **Advanced Properties** and change **Setup Provisioning toggle** from **No** to **Yes**



4. AirWatch Provisioning Adaptor

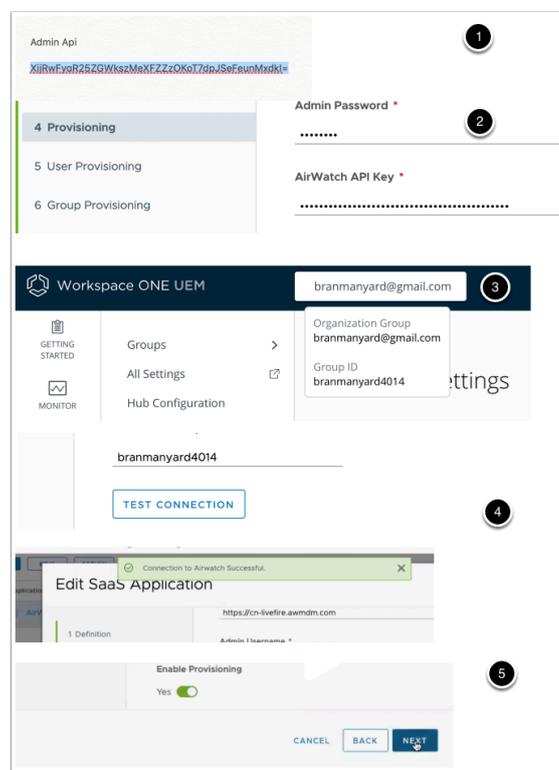
- In this section we will continue in the Workspace ONE Access console
 - In the **Edit SaaS Application** wizard select section **4 Provisioning**
 - In the middle pane under **Airwatch Host** type : - <https://cn-livewire.awmdm.com>
 - Under **Admin Username** type your **custom Workspace ONE UEM Admin account**
 - Under **Admin Password** type your the **custom Admin password (should be VMware!)**



5. AirWatch Provisioning Adaptor

- In this section we will continue in the Workspace ONE Access console

1. Launch your **text editor** where you have documented your Identity Manager admin Token and **copy the admin token**
2. Switch back to your **VIDM Edit Saas Application** wizard and under **AirWatch API Key** **paste the token**
3. Switch back to your **Workspace ONE UEM** console, at the top of the Workspace ONE UEM Console you will see your Organization Name, Expand your Organization Name and copy your Group ID
4. Switch back to your **VIDM Edit Saas Application** wizard
 - Under **AirWatch Group ID** type **YOUR Group ID**
 - Scroll down and under **Enable Provisioning** change the **toggle** from **No** to **Yes**
 - Above **Enable Provisioning** select **TEST CONNECTION**, you should notice a **Connection to Airwatch Successful** message
5. At the bottom of the **VIDM Edit Saas Application** wizard select **NEXT**



6. AirWatch Provisioning Adaptor

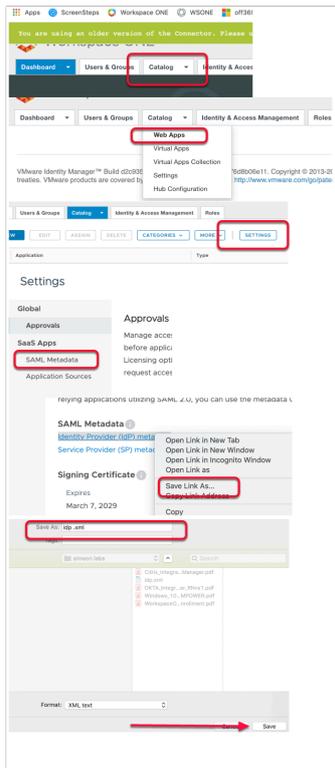
- In this section you will continue with the **VIDM Edit Saas Application** wizard
 1. In section **5 User Provisioning**, accept the default and select **NEXT**
 2. in section **6 Group Provisioning**, select **ADD GROUP**
 3. Under **Group Name** type **mark** and select **Marketing@euc-livewire.com**, under **Nickname** type **Marketing** and select **SAVE**
 4. On the **Group Provisioning** page select **NEXT**
 5. On section **7 Summary** select **SAVE**

Attribute Name	Value
User Name	\$(user.userName)
First Name	\$(user.firstName)
Last Name	\$(user.lastName)
User Email	\$(user.email)
User Principal Name	\$(user.userName)
External ID	\$(user.externalId)
User Domain	\$(user.domain)
Role	Full Access

Group Name	Group Mail Nickname
Marketing@euc-livefire.com	marketing

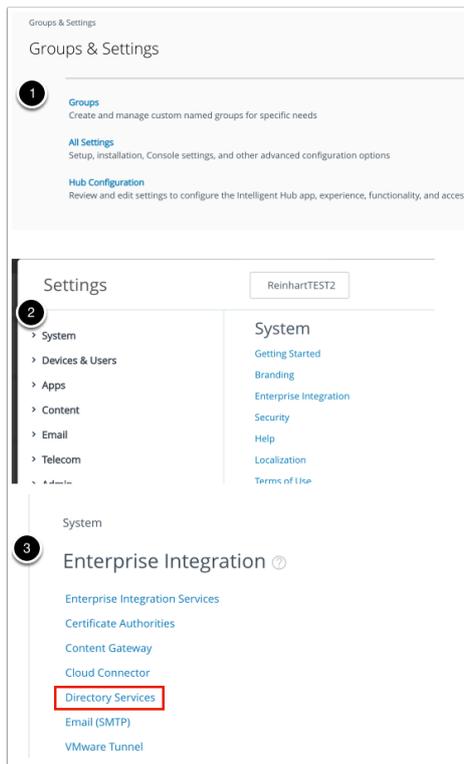
7. AirWatch Provisioning Adaptor

- In this section we will continue on the **Workspace ONE Access Admin Console** and download an .XML file:-
 - If you are not there already, navigate to **Catalog > Web Apps**
 - To the right select **SETTINGS**
 - Under **Settings > SaaS Apps** select **SAML Metadata**
 - Under **SAML Metadata** select **Identity Provider (IdP) metadata** right click and select **Save Link As**
 - In the **SAVE as** window select **Save**, you will notice the file name is **idp.xml**



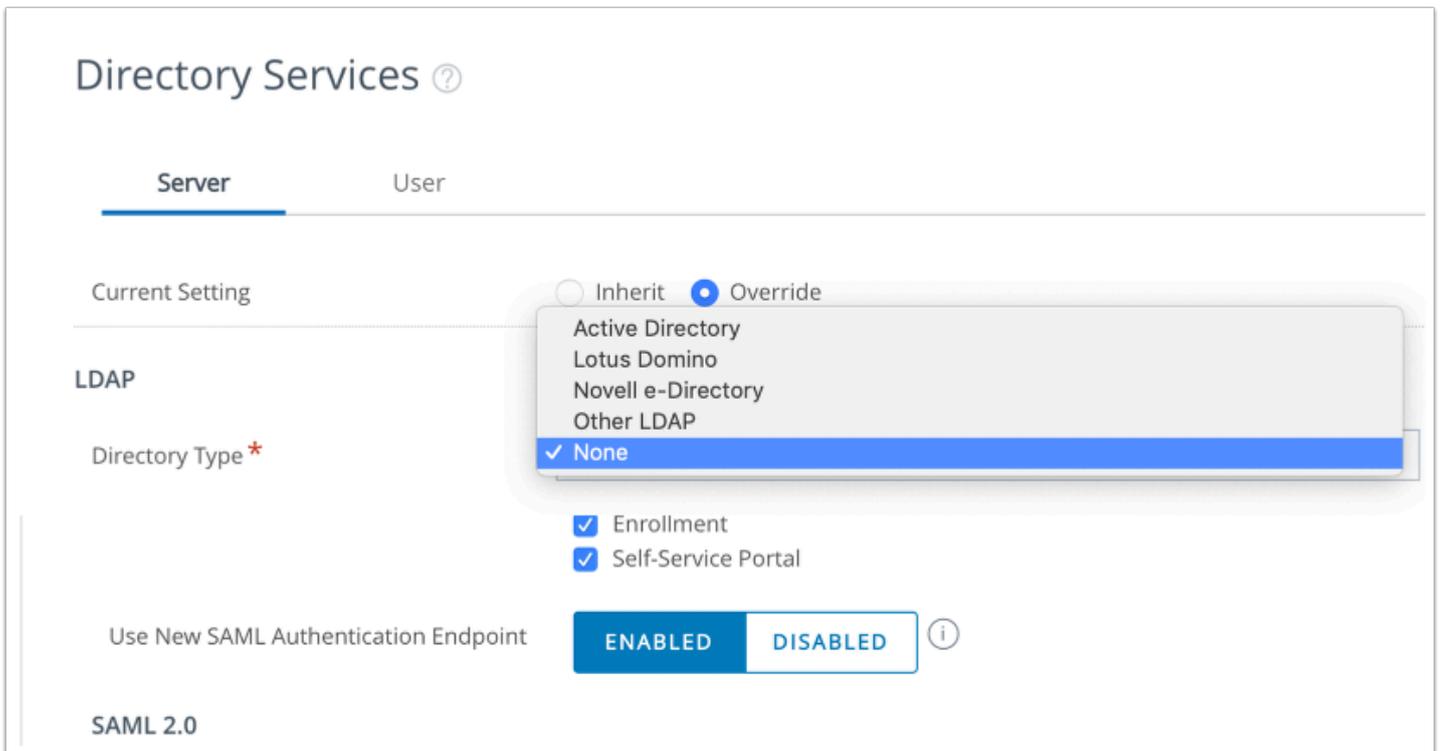
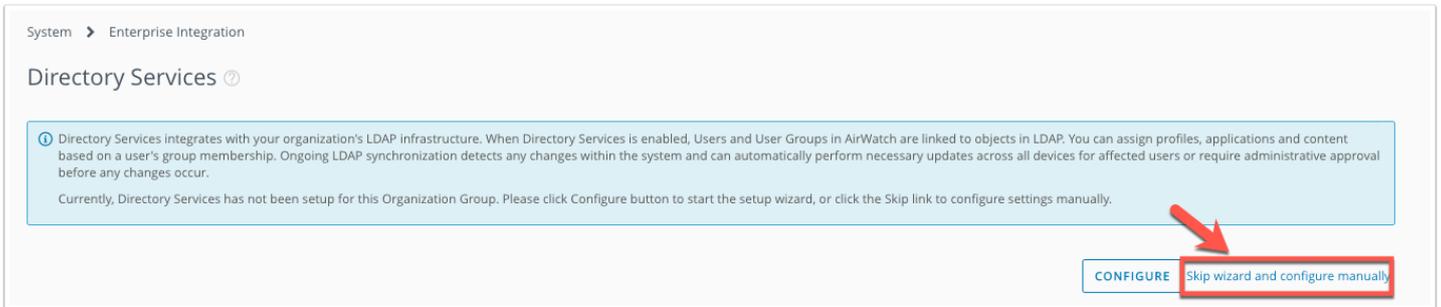
8. AirWatch Provisioning Adaptor

- In this section we will switch to the **Workspace ONE UEM** console
 - Go to **Groups & SETTINGS > ALL SETTINGS**
 - In the **Settings** window under **System** select **Enterprise Integration**
 - Under **Enterprise Integration** select **Directory Services**



9. AirWatch Provisioning Adaptor

1. In the **Directory Services** interface click "**Skip wizard and configure manually**"
2. Under the **Server** tab (default) next to **Current Setting** ensure the **Override radio button** is selected
3. Under **LDAP** next **Directory Type** change this from **Active Directory** to **None**
4. Under **LDAP** next to **Use SAML for Authentication** select the **ENABLED** box



10. AirWatch Provisioning Adaptor

1. Next to **Enable SAML Authentication For** put a check next to **Admin, Enrollment** and **Self-Service Portal**
2. Next to Use New SAML Authentication Endpoint select **Enabled**
3. Under **SAML 2.0** next to **Import Identity Provider Settings** select **UPLOAD** and choose your xml file.
4. At the bottom of the window select **SAVE**
5. Next to **Request Binding Type** select the **POST** radio button,
6. Next to **Response Binding Type** select the **POST** radio button, scroll down and select **SAVE**
7. Close the Settings window by selecting **X** to the right of the window

LDAP

Directory Type * ⓘ

Use Azure AD For Identity Services

Use SAML For Authentication

Enable SAML Authentication For * Admin ⓘ
 Enrollment
 Self-Service Portal

Use New SAML Authentication Endpoint ⓘ

SAML 2.0

Import Identity Provider Settings

⚠ To load the imported settings, click save. Any changes made to the form will be lost.

LDAP

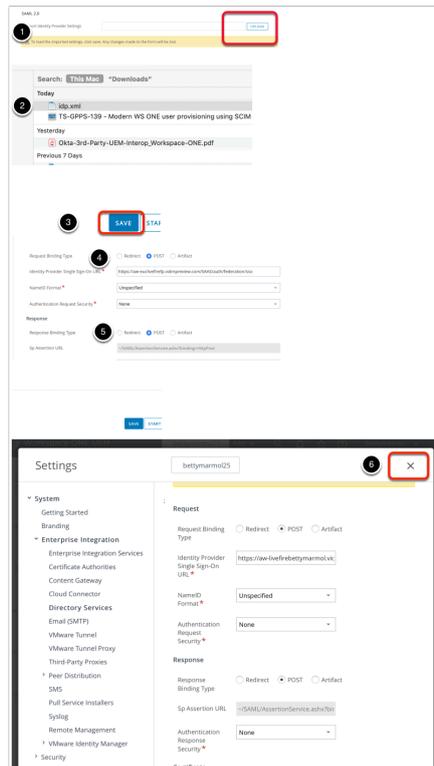
Directory Type * ⓘ

Use Azure AD For Identity Services

Use SAML For Authentication

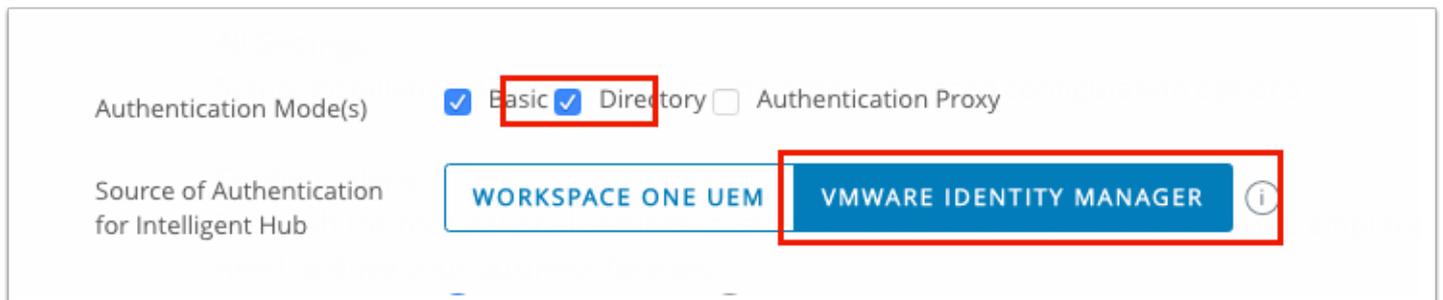
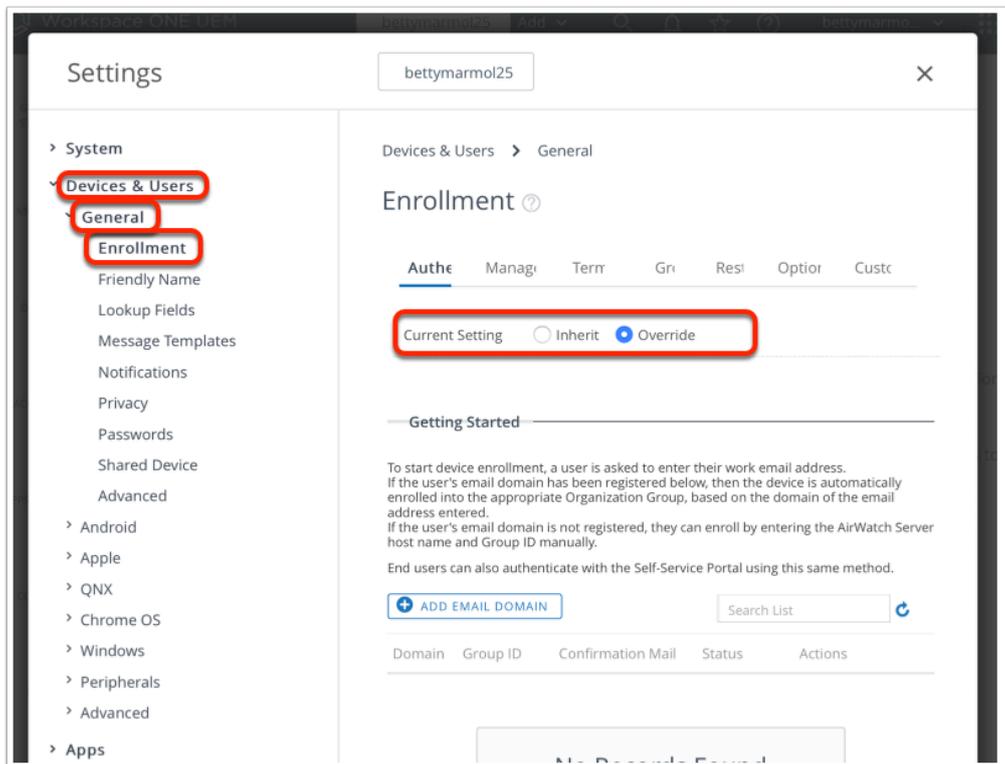
Enable SAML Authentication For * Admin ⓘ
 Enrollment
 Self-Service Portal

Use New SAML Authentication Endpoint ⓘ



11. AirWatch Provisioning Adaptor

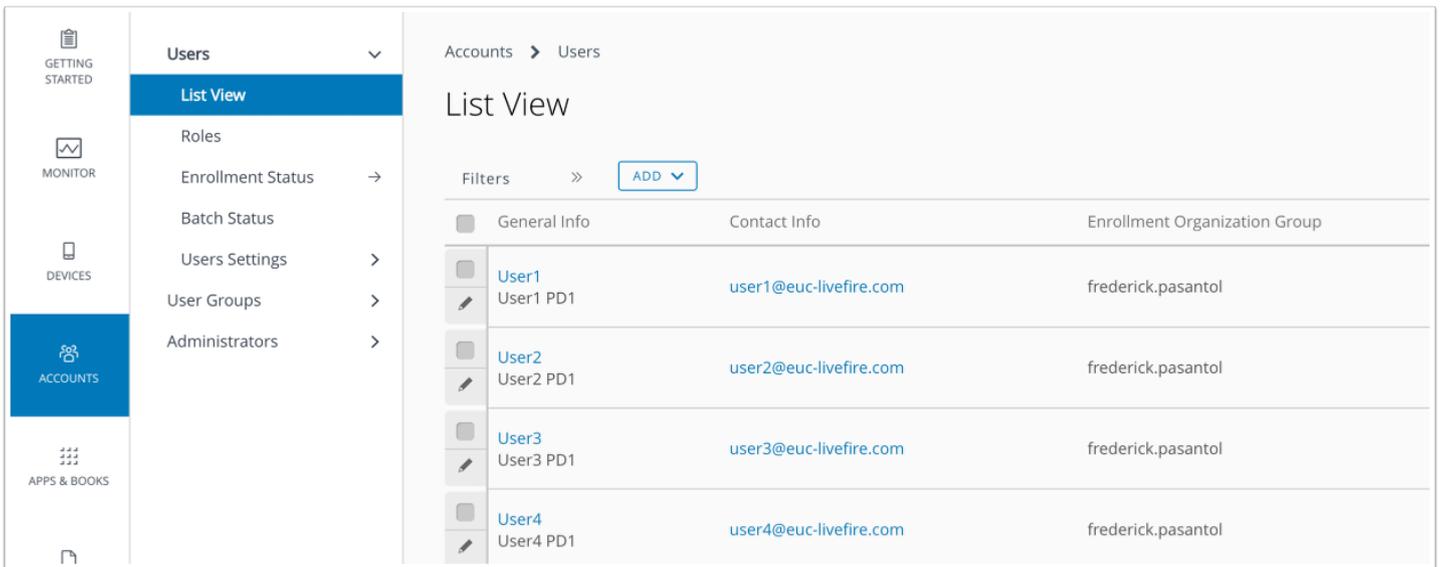
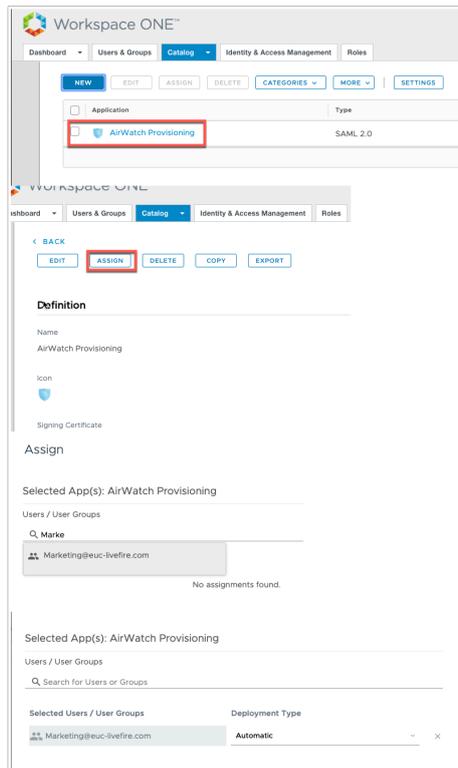
- In this section we will work **Workspace ONE UEM Admin Console**, Under **Groups and settings** > **All Settings** > **Devices & Users** > **General** > **Enrollment**
 - Next to **Current Settings** Click **Override**
 - Next to **Authentication Mode(s)** ensure the **Directory checkbox** is enabled
 - Next to **Source of Authentication for Intelligent Hub**. Select **VMWARE IDENTITY MANAGER**
NOTE: If SAML 2.0 is enabled as above it will still use Workspace ONE Access for authentication even if **WORKSPACE ONE UEM** is selected, but **People Search** and **Notifications** will only be enabled in **HUB** if **VMWARE IDENTITY MANAGER** is select here.
 - Select **SAVE**



12. AirWatch Provisioning Adaptor

- Switch back to the **Workspace ONE Access Admin console**
 1. Select **Catalog** and select the **checkbox** next to **AirWatch Provisioning** Application
Select **ASSIGN**
 2. In the Assign window under **Users / User Groups** type **Marketing**, select **Marketing@euc-livewire.com**
 3. Under **Deployment Type** change **User-Activated** to **Automatic** and **SAVE**
 4. The users should now be provisioned into **WorkspaceOne UEM**. You can check this by going into the **WorkspaceONE UEM console** select **Accounts > Users > List View**

Note! It could take up to 10 minutes for provisioning to work.

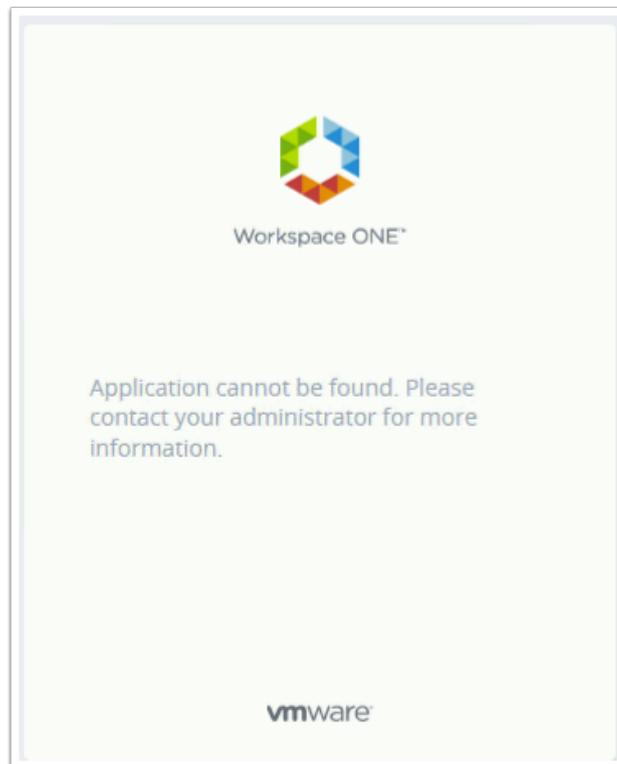


Part 3: Completing full SAML configuration in Workspace ONE Access of Workspace ONE UEM

The AirWatch Provisioning Adaptor is a new way to configure User and Group Provisioning. One of the steps we followed was to copy Workspace ONE Access Metadata into Workspace ONE UEM. What we have learned in our troubleshooting is that if we were to leave configuration as it is, enrollment of devices will fail. In testing with Windows 10 and Android based enrollment we got a common error message which looked as follows. Application cannot be found.

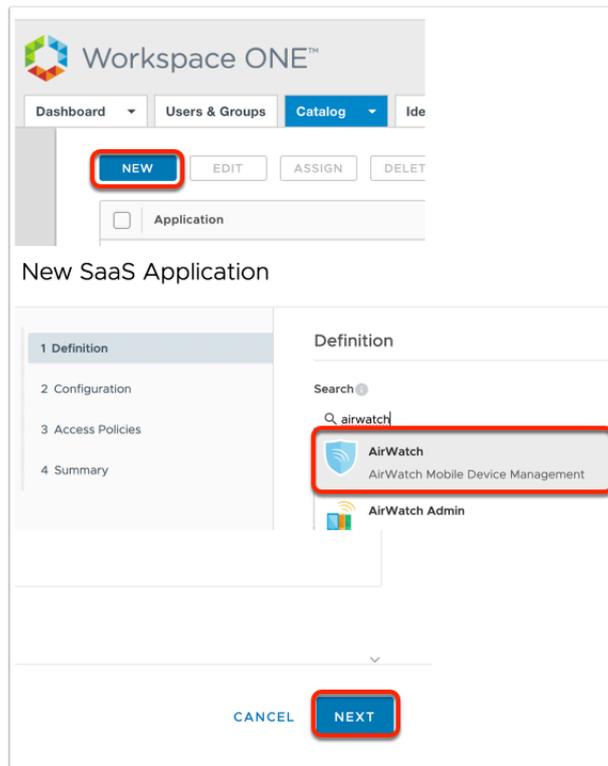
With extensive collaboration with the PSO team in our Atlanta USA office we were able to establish the cause.

We required full SAML configuration on both services that being Workspace ONE UEM and Workspace ONE Access. Up till now we have only configure SAML integration of Workspace ONE Access in Workspace ONE UEM. We will now configure SAML integration in Workspace ONE Access of Workspace ONE UEM.



1. SAML integration Configuration (Part 4)

- Switch to your **Workspace ONE Access** Console
 1. Select **Catalog > Web Apps** and then select **NEW**
 2. In the **New SaaS Application** under **Search** type **airwatch** and select **AirWatch Mobile Device Management**
 3. Scroll down to the bottom of the page and select **NEXT**



2. SAML integration Configuration (Part 4)

- Step 2 of the New SaaS Application wizard
 1. In the **New SaaS Application** wizard, step **2 Configuration**, scroll down to **Application Parameters** and configure the following:- next to :
 1. **AWServerName** under **Value** type : ds-livefire.awmdm.com
 2. **AC** type your Group ID under **Value** : [eg. Plaston444](#)
 3. **Audience** under **Value**: [AirWatch](#)
 4. Scroll down and move the **toggle** under **Show in User Portal** to **No**
 5. Select **NEXT**
 2. In step **3 Access Policies** select **NEXT**
 3. In step **4 Summary** select **SAVE**

Application Parameters ⓘ			
Name	Description	Default Value	Value
AWServerName	AirWatch Server Name		ds-livefire.awmdm.com
ac	Group ID		Fran444
audience	Service Provider (AirWz		AirWatch

5. SAML integration Configuration (Part 4)

- Select the **checkbox** next to **AirWatch** application and select **Assign**

1. In the **Assign** window under **Users** in the search type **Mark** and add **marketing@euc-livefire.com**, set the **Deployment Type** to **Automatic** and select **SAVE**

NEW **EDIT** **ASSIGN** **DELETE** **CATEGORIES** **MORE**

<input type="checkbox"/>	Application	Type
<input checked="" type="checkbox"/>	 AirWatch	SAML 2.0
<input type="checkbox"/>	 AirWatch Provisioning	SAML 2.0

Users / User Groups

Search for Users or Groups

Selected Users / User Groups	Deployment Type
 Marketing@euc-livefire.com	Automatic