

# 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.

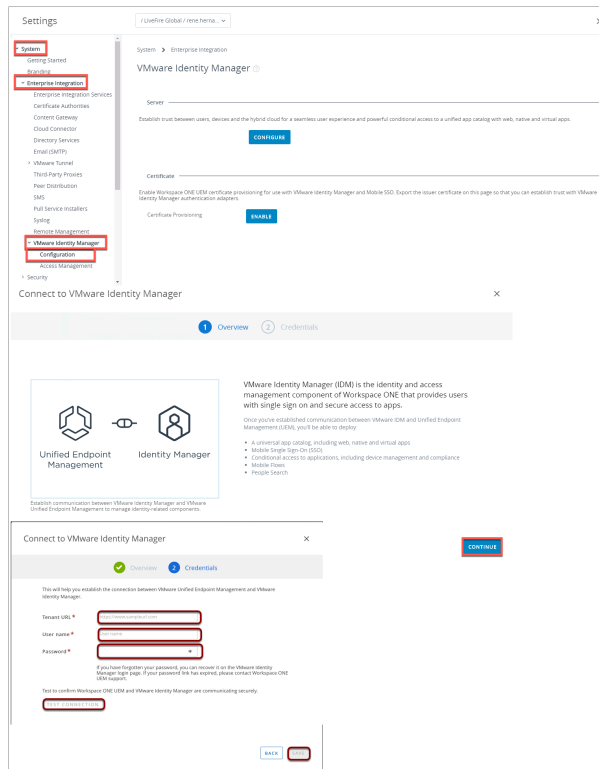
1. Switch back to the Workspace ONE UEM Admin console.
  - Be sure to make these settings at the **company organisation group**, then navigate to **Groups and Settings > All Settings > System > Enterprise Integration > VMware Identity Manager > Configuration**
2. Click **CONFIGURE** under **Server**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

/ LiveFire Global / rene.herna...

**Server**

Establish trust between users, devices and the hybrid cloud for a seamless user experience and powerful conditional access to a unified app catalog with web, native and virtual apps.

URL:

Admin User Name:

Active Directory Basic: ☐ **ENABLED** **DISABLED**

Use this Action Button to update Workspace ONE IDMA-UEM configuration to use Auto-Generated UEM API Key

**USE AUTOGENERATED API KEY** vDM's AirWatch settings have been updated to use auto-generated API keys

**Certificate**

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

Certificate Provisioning: **ENABLE**

**DELETE**

**Certificate**

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

Certificate Provisioning: **ENABLE**

**Certificate**

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

Certificate	Type	Pfx
	Valid From	4/6/2019
	Valid To	4/6/2029
	Thumbprint	0CCB6D13FB8024980B91B896E014B73E578AF2A

Issuer Certificate: **EXPORT**

**DELETE**

## Part 1B. Creating a custom REST API Account

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



System > Advanced > API

## REST API ?

**General** Authentication Usage

Current Setting ☐ Inherit ☒ Override

Enable API Access ENABLED DISABLED ? 1

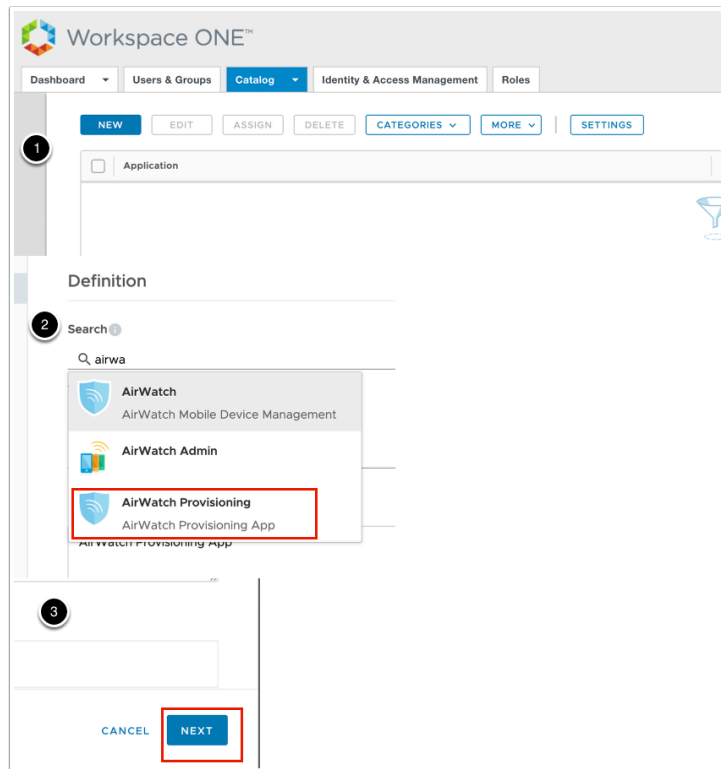
AirWatchAPI 2 Admin XijRwFyaR25ZGWkszMexFZZzOKoT7dpSeFeunMxdkl=

→ SAVE 3

## 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
  - In the **Admin Console** select the **Catalog** tab and select **NEW**
  - On the **New SaaS Application**, next to section **1.Definition** under **search** type **AirWa** and you should see **Airwatch Provisioning**. Select **AirWatch Provisioning**
  - 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**

The image displays three sequential screenshots of the 'Edit SaaS Application' wizard interface.

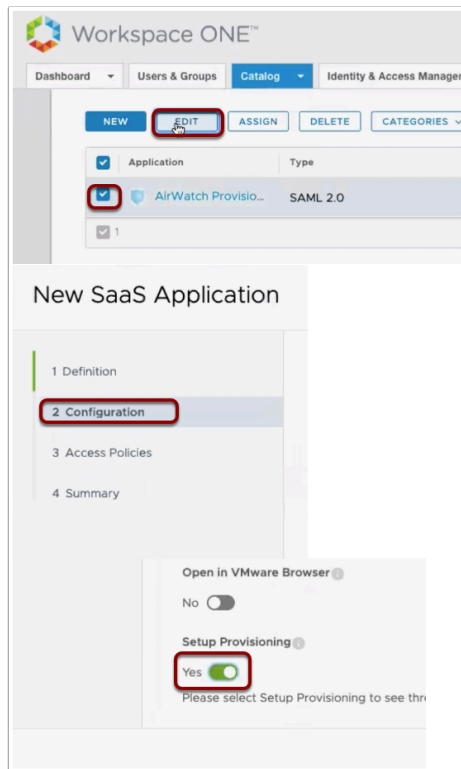
**Top Screenshot (Configuration Step):** The left sidebar shows steps 1 (Definition), 2 (Configuration), 3 (Access Policies), and 4 (Summary). The main area is titled 'Configuration' and contains fields for 'Single Sign-On URL', 'Recipient URL', 'Application ID', 'Username Format', 'Username Value', and 'Relay State URL'. The 'Username Value' field is highlighted with a red box and contains the text 'airwatch-provisioning'.

**Middle Screenshot (Access Policies Step):** The left sidebar shows steps 1 (Definition), 2 (Configuration), 3 (Access Policies), and 4 (Summary). The main area is titled 'Access Policies' and contains a list of policies. The policy 'airwatch\_policy\_001' is highlighted with a red box.

**Bottom Screenshot (Summary Step):** The left sidebar shows steps 1 (Definition), 2 (Configuration), 3 (Access Policies), and 4 (Summary). The main area is titled 'Definition' and contains fields for 'Name', 'Description', 'Icon', 'Component', 'Authentication Type', and 'Configuration'. The 'Configuration' field is highlighted with a red box and contains the text 'Manual'.

### 3. AirWatch Provisioning Adaptor

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



#### 4. AirWatch Provisioning Adaptor

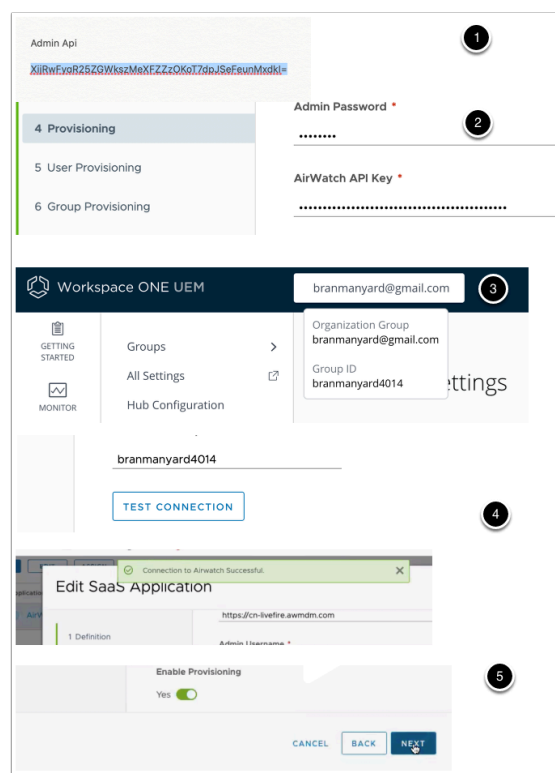
- In this section we will continue in the Workspace ONE Access console
  - In the **Edit SaaS Application** wizard select section **4 Provisioning**
  - In the middle pane under **Airwatch Host** type : - <https://cn-livewire.awmdm.com>
    - Under **Admin Username** type your **custom Workspace ONE UEM Admin account**
    - Under **Admin Password** type your the **custom Admin password (should be VMware1!)**

#### 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 Succesful** 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**

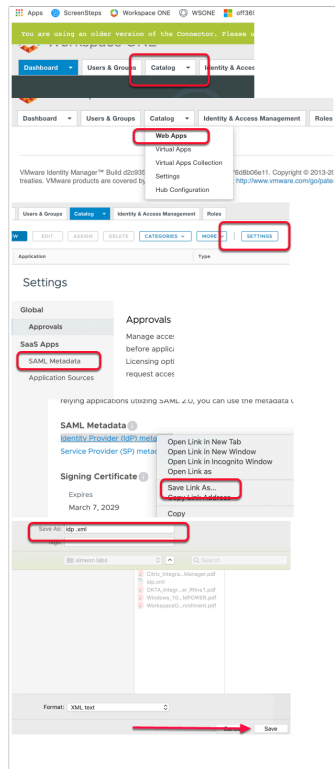
Attribute Name	Value
User Name	\${user.userName}
First Name	\${user.firstName}
Last Name	\${user.lastName}
User Email	\${user.email}
User Principal Name	\${user.userName}@\${user.domain}
External Id	\${user.externalId}
User Domain	\${user.domain}
Role	Full Access

Attribute Name	Value
Group Name	Marketing@euc-livewire.com
Group Mail Nickname	marketing

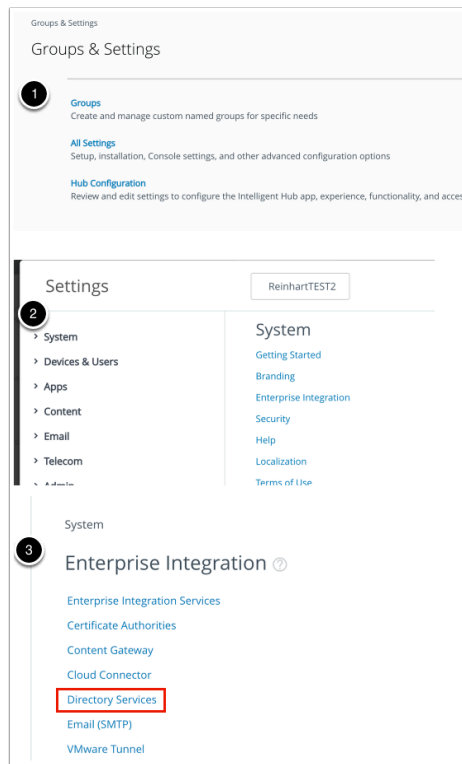
## 7. AirWatch Provisioning Adaptor

- 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**



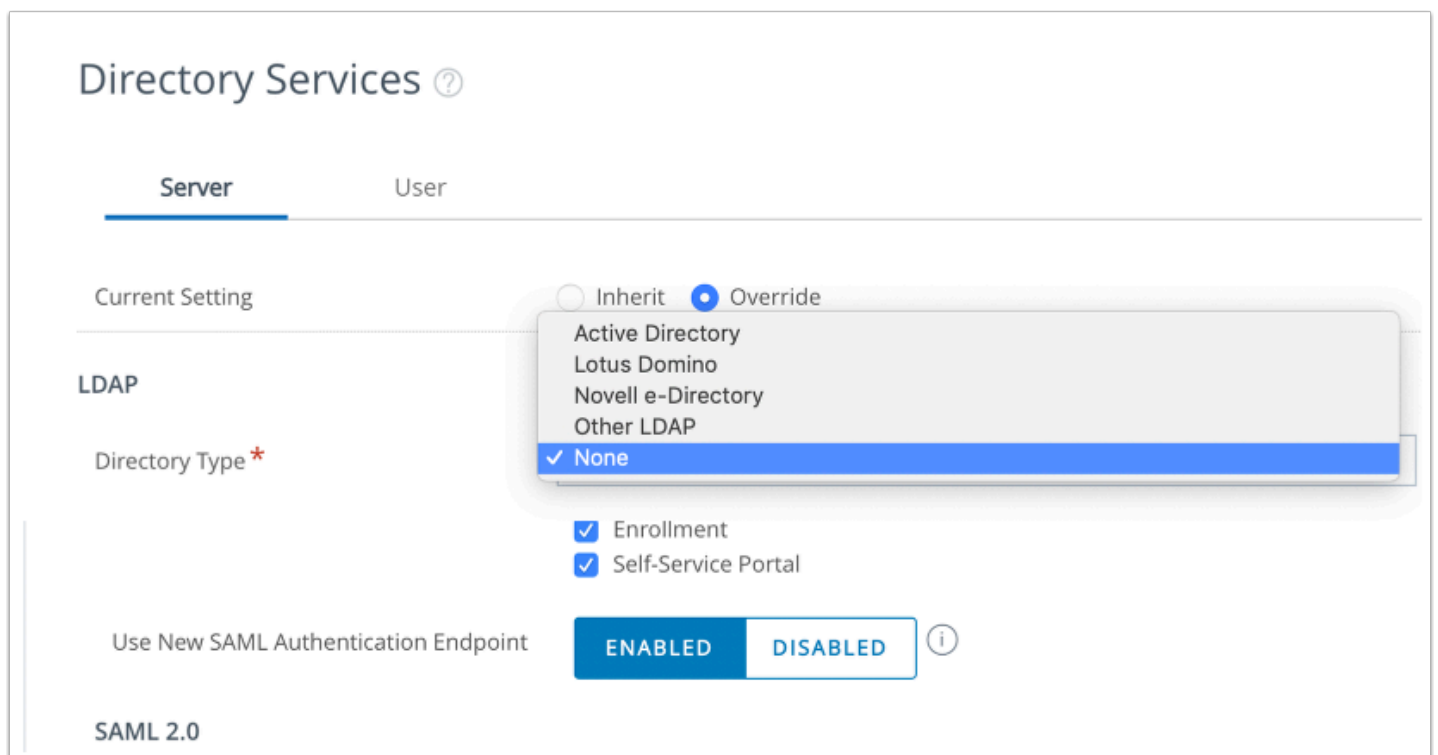
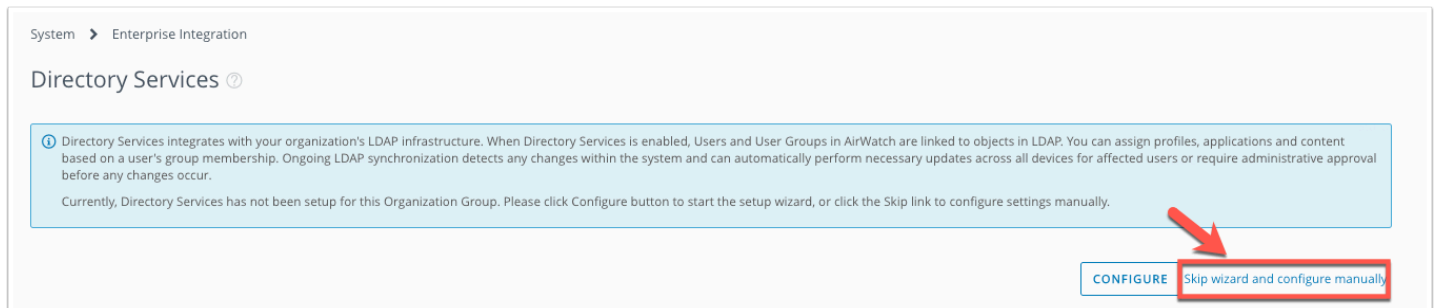
## 8. AirWatch Provisioning Adaptor

- 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 to **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 \*

None

Use Azure AD For Identity Services

ENABLED

DISABLED

Use SAML For Authentication

ENABLED

DISABLED

Enable SAML Authentication For \*

☒ Admin

☒ Enrollment

☒ Self-Service Portal

Use New SAML Authentication Endpoint

ENABLED

DISABLED

SAML 2.0

Import Identity Provider Settings

UPLOAD

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

LDAP

Directory Type \*

None

Use Azure AD For Identity Services

ENABLED

DISABLED

Use SAML For Authentication

ENABLED

DISABLED

Enable SAML Authentication For \*

☒ Admin

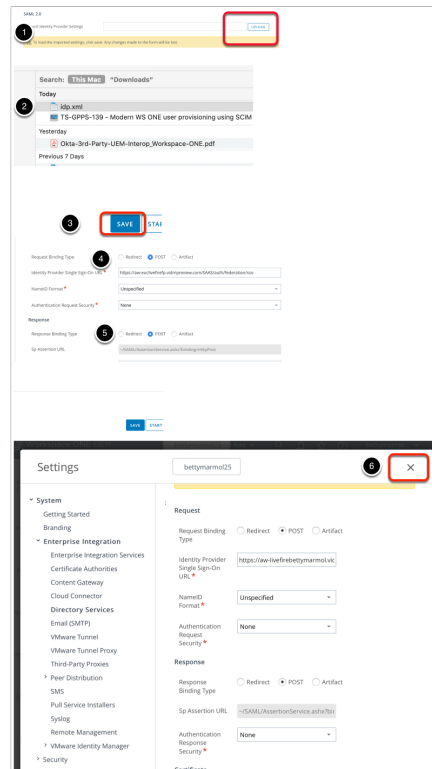
☒ Enrollment

☒ Self-Service Portal

Use New SAML Authentication Endpoint

ENABLED

DISABLED

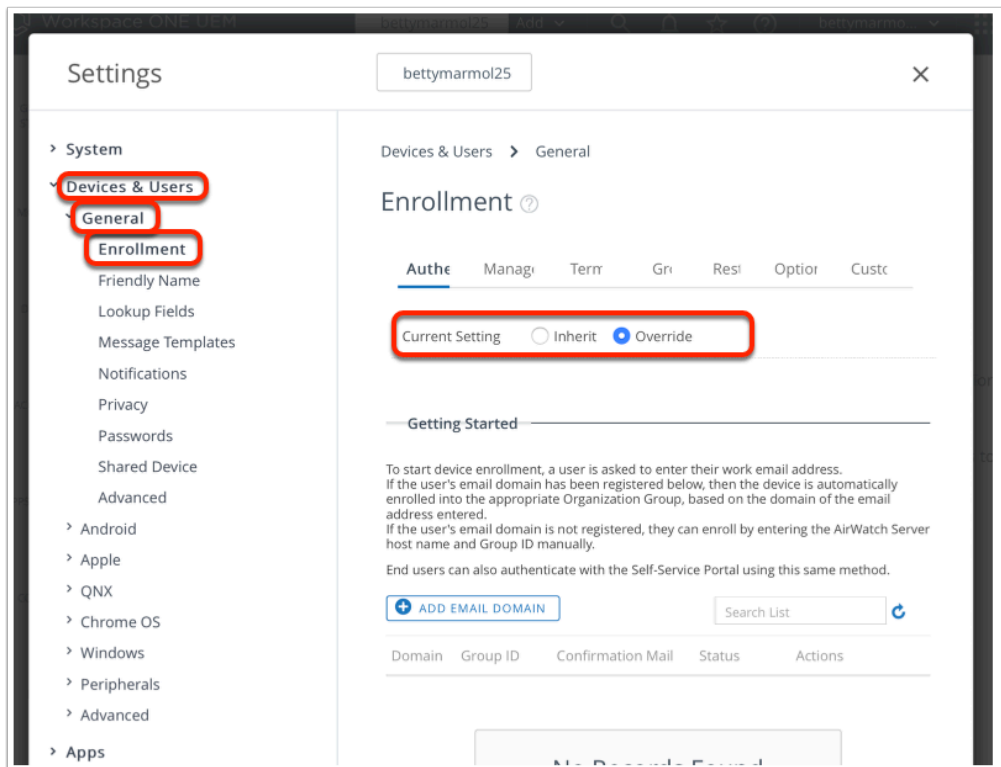


## 11. AirWatch Provisioning Adaptor

- 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**



Authentication Mode(s) ☒ Basic ☒ Directory ☐ Authentication Proxy

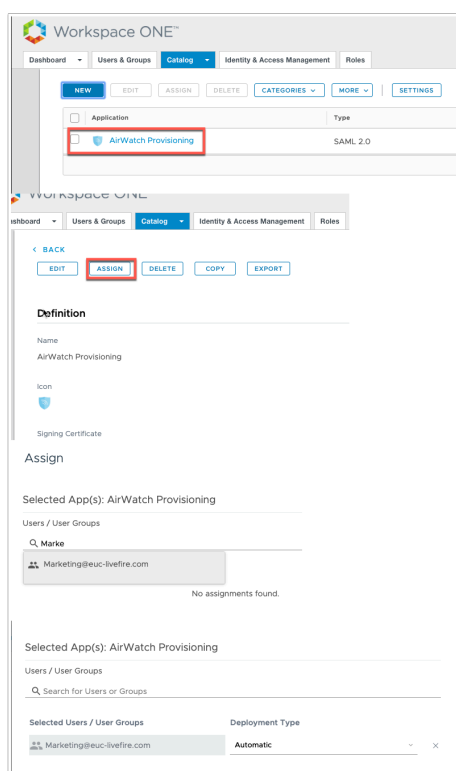
Source of Authentication for Intelligent Hub

WORKSPACE ONE UEM VMWARE IDENTITY MANAGER ⓘ

## 12. AirWatch Provisioning Adaptor

- Switch back to the **Workspace ONE Access Admin console**
  - Select **Catalog** and select the **checkbox** next to **AirWatch Provisioning** Application. Select **ASSIGN**.
  - In the Assign window under **Users / User Groups** type **Marketing**, select **Marketing@euc-livewire.com**.
  - Under **Deployment Type** change **User-Activated** to **Automatic** and **SAVE**.
  - 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.**



<div>GETTING STARTED</div> <div>MONITOR</div> <div>DEVICES</div> <div>ACCOUNTS</div> <div>APPS &amp; BOOKS</div>	<div>Users</div> <div>List View</div> <div>Roles</div> <div>Enrollment Status</div> <div>Batch Status</div> <div>Users Settings</div> <div>User Groups</div> <div>Administrators</div>	<div>Accounts &gt; Users</div> <div>List View</div> <div>Filters</div> <div>ADD</div> <table> <tr> <th>General Info</th><th>Contact Info</th><th>Enrollment Organization Group</th></tr> <tr> <td>User1 User1 PD1</td><td>user1@euc-livefire.com</td><td>frederick.pasantol</td></tr> <tr> <td>User2 User2 PD1</td><td>user2@euc-livefire.com</td><td>frederick.pasantol</td></tr> <tr> <td>User3 User3 PD1</td><td>user3@euc-livefire.com</td><td>frederick.pasantol</td></tr> <tr> <td>User4 User4 PD1</td><td>user4@euc-livefire.com</td><td>frederick.pasantol</td></tr> </table>	General Info	Contact Info	Enrollment Organization Group	User1 User1 PD1	user1@euc-livefire.com	frederick.pasantol	User2 User2 PD1	user2@euc-livefire.com	frederick.pasantol	User3 User3 PD1	user3@euc-livefire.com	frederick.pasantol	User4 User4 PD1	user4@euc-livefire.com	frederick.pasantol
General Info	Contact Info	Enrollment Organization Group															
User1 User1 PD1	user1@euc-livefire.com	frederick.pasantol															
User2 User2 PD1	user2@euc-livefire.com	frederick.pasantol															
User3 User3 PD1	user3@euc-livefire.com	frederick.pasantol															
User4 User4 PD1	user4@euc-livefire.com	frederick.pasantol															

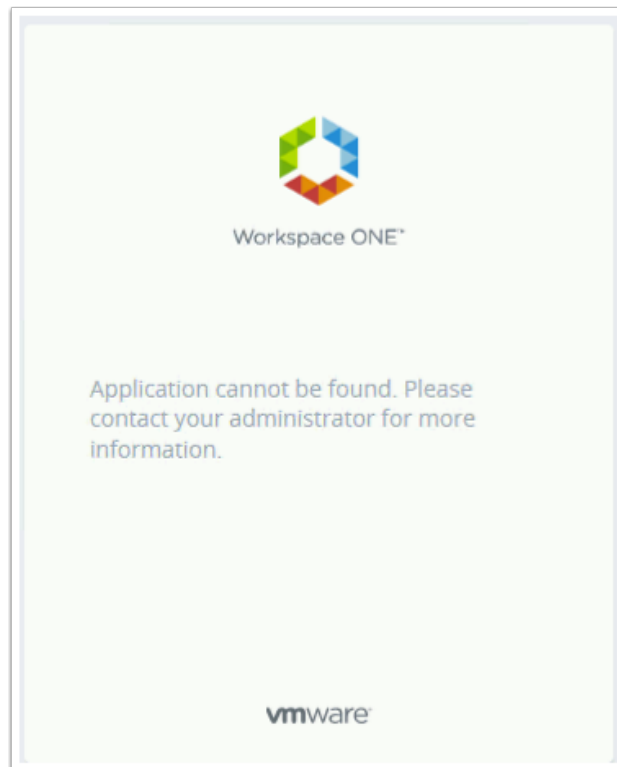
## Part 3: Completing full SAML configuration in Workspace ONE Access of Workspace ONE UEM

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**

Workspace ONE™

Dashboard Users & Groups Catalog Ide

NEW EDIT ASSIGN DELETE

Application

### New SaaS Application

1 Definition  
2 Configuration  
3 Access Policies  
4 Summary

Definition

Search

airwatch

AirWatch

AirWatch Mobile Device Management

AirWatch Admin

CANCEL NEXT

## 2. SAML integration Configuration (Part 4)

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

Application Parameters ⓘ



Name	Description	Default Value	Value
AWServerName	AirWatch Server Name		<a href="https://ds-livefire.awmdm.com">ds-livefire.awmdm.com</a>
ac	Group ID		<a href="#">Fran444</a>
audience	Service Provider (AirWz		<a href="#">AirWatch</a>

## 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**

NEWEDITASSIGNDELETECATEGORIES ▼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

Selected Users / User Groups

Marketing@euc-livefire.com

Deployment Type

Automatic ▼