# Federating a SAML application with Workspace ONE Access

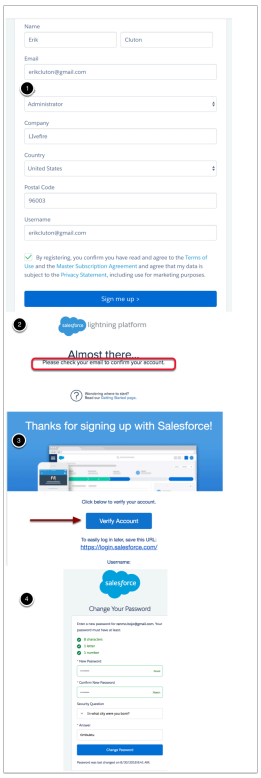
## VMware Identity Manager SaaS application

## Part 1. SFDC Pre-Requisites Setup

This lab is intended to prepare those federating SaaS applications for authentication via Workspace ONE Access. As SAML is a standard authentication type, this example is just one of many documented integrations. See here for more examples: **https://www.vmware.com/support/pubs/Workspace ONE Access_webapp_sso.html**

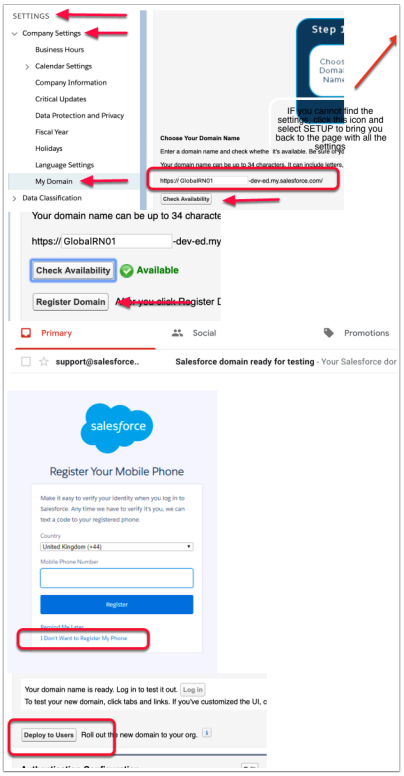
### 1.1 First we will sign up for a SFDC developer trial account.

- Open your Browser on the Control Center VM
  1. Navigate to **https://developer.salesforce.com/signup** for a free account.
     - Fill in your details using a personal e-mail address. Please ensure this e-mail address has not previously been used with SFDC
  2. *Go to your **email** and confirm your registration*. Select Verify Account. This will take you to the **Change Your Password** Site.
  3. **Set a password of your choosing** and provide a security question and answer
  4. Select **Change Password** to save and you will be redirected automatically to the Setup Home page.



1.2 You should still be automatically logged in with the user that you have created above, if not navigate to https://login.salesforce.com and login with the details for your account.

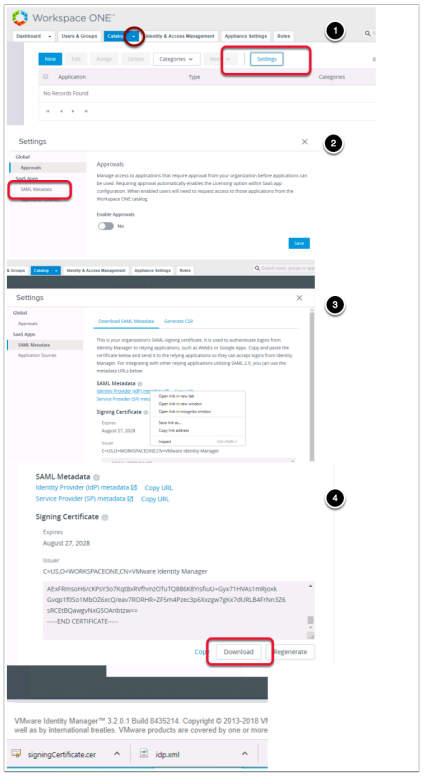
- **NOTE**: Salesforce has two Web Interfaces and this can get quite confusing. Please be sure to use the **lightning experience** interface rather than the classic interface. **You will now register a unique domain name for you SFDC dev account**
  1. On the Home page **Navigate to Settings** > **Company Settings** > **My Domain**
  2. Enter a **unique domain name** under "**Choose Your Domain Name" - first letter of first name plus last name plus livefire** - ***For example*** - globalrn01
  3. Click **check availability**, If available select **Register Domain**. *This process usually takes about 5 to 10 minutes.* (SalesForce has to publish that unique domain name) You can move on to "**Establish SAML Trust**" Section below come back to this section once you get asked to login to your unique URL.
  4. You will receive an e-mail to the address specified in your developer's account once it has successfully registered. **Click the link provided** in the **e-mail** to confirm your domain registration and login using the credentials you created above. **NOTE: at this point it might prompt you for a phone number. You can easily select I don't want to register my phone. Then it will just use your e-mail address as the second factor authentication.**
  5. Now Navigate back to **Settings** > **Company Settings** > **My Domain** and select the **Deploy to users** and confirm the pop-up.




# Part 2. Establish SAML Trust

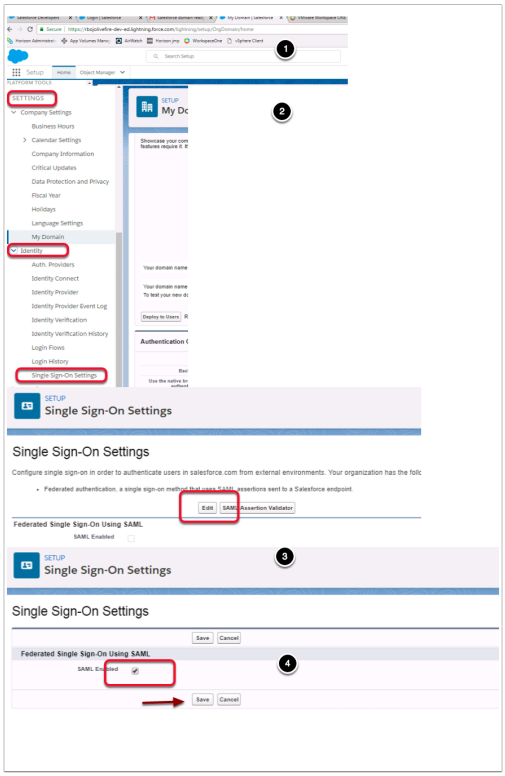
2.1

- Now we will download the identity provider Signing certificate from Workspace ONE Access and upload it into SFDC to create the trust relationship for authentication.
  1. **Login** to your Saas Workspace ONE Access as sysadmin
  2. Select the **Catalog** tab and select **Settings**
  3. Select **Settings** select SAML Metadata
  4. Right click on **Identity Provider (Idp) metadata** and select **save link as**, this will open your **Save As** window. Leave the **Downloads** folder as default and the name as **idp.xml** and select **Save**
  5. Go to the **Signing Certificate** area and select **Download** , you should now have a **signingCertificate.cer** and a **idp.xml** in the **Downloads** folder



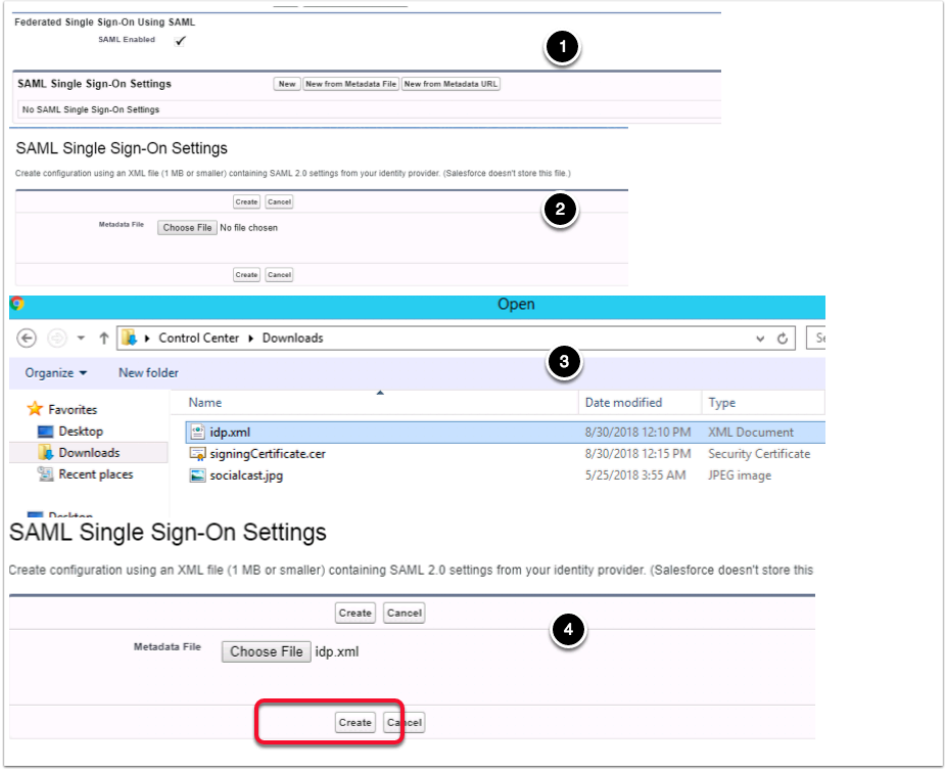

2.2

- Navigate back to your SalesForce site where you should now be able to login with your unique registered domain ***-dev-ed.lightning.force.com**
  1. On the home page for the admin user you will find **Settings** > **Identity** > **Single Sign-On Settings** **NOTE:** if you can't locate these options on the initials login page select the cog wheel in the top right hand side of the page and select setup and it will take you to the correct configuration page.
  2. On the **Single Sign-On Settings** Page next **SAML Assertion Validator** select **Edit**, below **Federated Single Sign-on Using SAML**, select the **SAML Enabled checkbox**. Select **Save.**



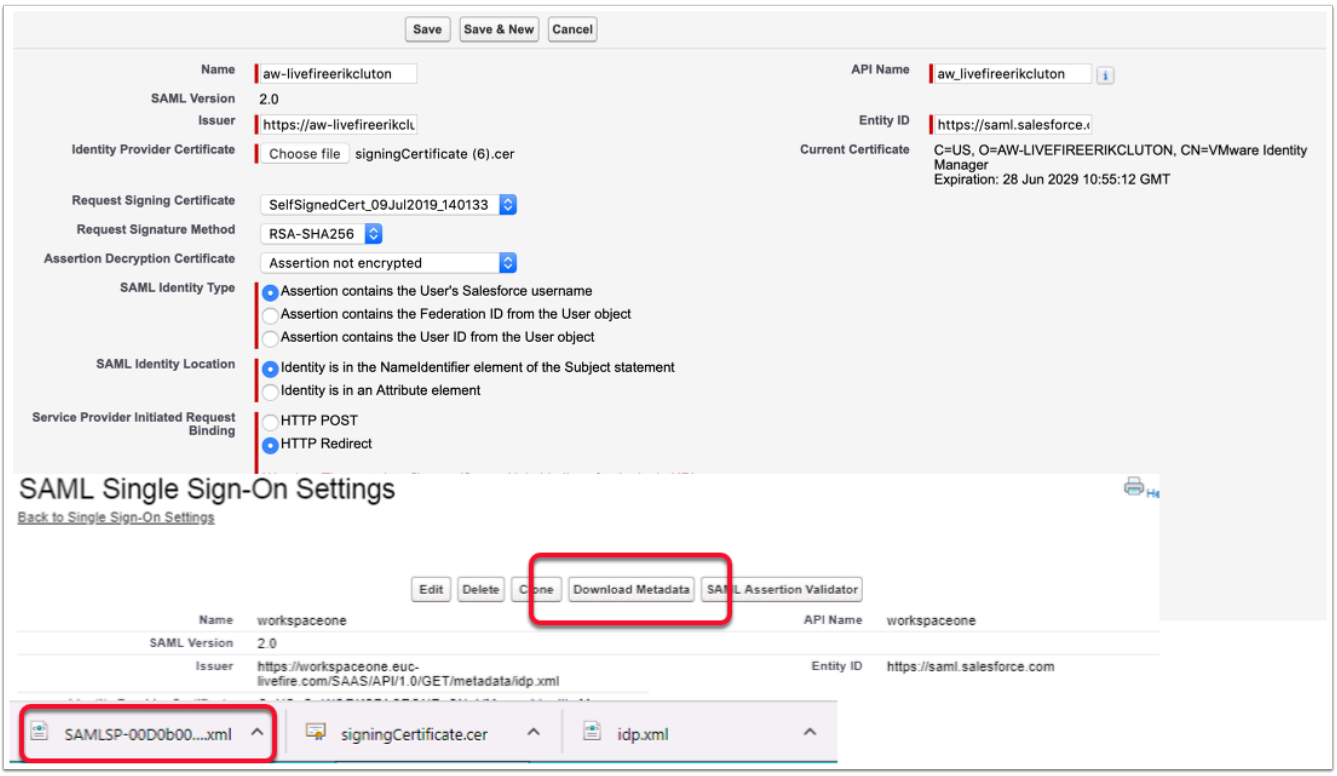

2.3

- Now select **New From Metadata File** just underneath where the SAML settings have been enabled.
  1. This will take you to the **SAML Single Sign-On Settings** page where it will request the SAML metadata**.**
  2. Click **Choose File** that you have downloaded into the **Downloads** Folder from Workspace ONE Access named **idm.xml** (created in step 5). select the **idp.xml** and select **Open** select **Create.**




2.4

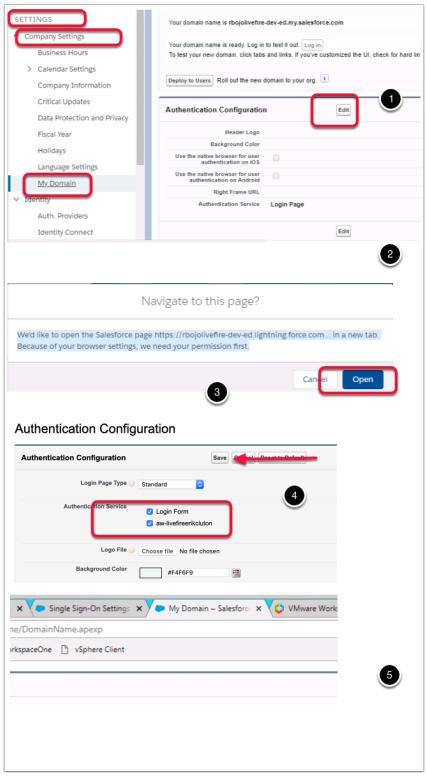
- Notice now that the fields have been auto populated with the correct data from Workspace ONE Access
  1. Ensure the Following are correct in the settings:
     - Next to **NAME:** *leave as default*
     - Next to **ISSUER:** *leave as default*, This is the XML that is provided for the Metadata -
     - Next to **Provider Certificate**: Upload the signingCertificate.cer into this field (this was created in step 5)
     - Next to **SAML Identity Type:** leave as default "Assertion contains the User's Salesforce username
     - Next to **SAML Identity Location**: *leave as default* "Identity is in the NameIdentifier element of the Subject statement
     - Next to **API Name:** *leave as default*
     - Next to **Entity ID:** Change to **https://saml.salesforce.com**
     - Next to **Identity Provider Login URL:** *l*eave as default
     - Next to **Custom Logout URL: your Workspace ONE Access URL**
       - **e.g.** https://aw-livefireerikcluton.vidmpreview.com
     - Ensure the check box from **Single Logout Enabled** is **removed.**
  2. Select **Save**.
  3. On the **SAML Single Sign-On Settings** page select **Download Metadata**.
     - **NOTE:** *Download metadata* is not available in the **edit view** you have to click on the policy This will **download an xml** file beginning with **SAMLSP.....xml**




2.5

- On the SalesForce admin console
  1. Navigate to **Settings** > Company Settings > My Domain
  2. In the **Authentication Configuration** section select **edit,** this will open a new tab. Ensure that you observe Pop-up Blocker in your browser and select the radio button **to Always allow pop-ups.**...,
  3. Select **Done,** and then on the **Navigate to this page?** window select **Open**
  4. Under **Authentication Configuration** page next to **Authentication Service** select the **check box** that has **"YOUR Saas Workspace ONE Access"** and select **Save**
     - **NB! Notice that this pop-up window opened up in a new window on a new TAB.**

**Revert back by selecting the original window Single Sign-On Settings tab to the left of your current window**



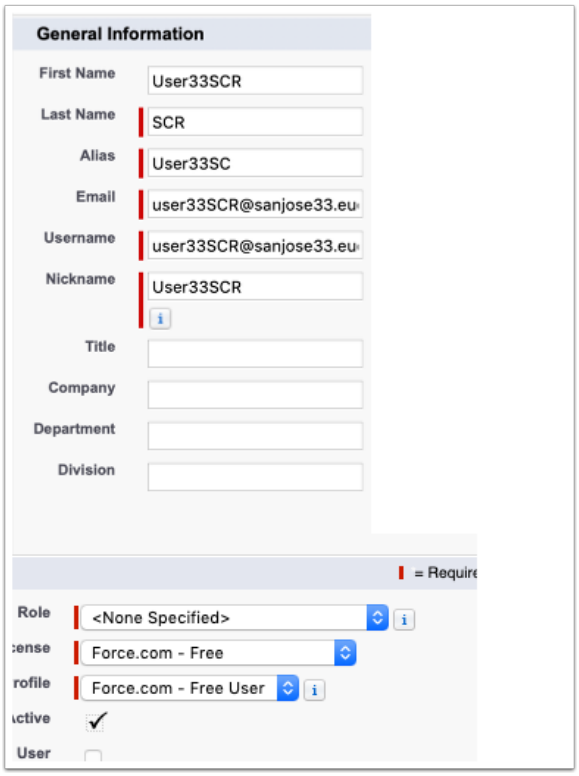

2.6

- Creating a unique user for your SalesForce environment.

NB! This has to be an Identical account to what you created at the beginning of the course

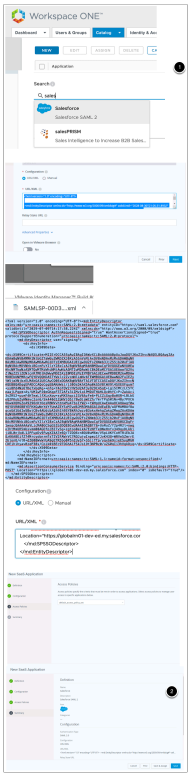
1. Navigate to **Administration** > **Users** > **Users** > click Select **New User**
2. Fill in the unique user details,
   - **First Name:** User xxxxx {your student number + {the first letter of your city and country abbreviation}} eg {for San jose, Costa Rica User33SCR}
   - **Last Name:** {the first letter of your city and country abbreviation} eg. SCR
   - **Alias:{same as your first name}**
   - **Email:{FirstName@customsuffix.euc-livefire.com}** (For Example: user33SCR@sanjose33.euc-livefire.com)
   - **Username:{FirstName@*customsuffix*.euc-livefire.com}** (For Example: user33SCR@sanjose33.euc-livefire.com)
   - **Nickname: {same as your FirstName}**
   - **Role: <None Specified >**
   - **User License: Force.com - Free**
   - **Profile:Force.com - Free User**
3. Click **Save**

This will be the user we will use to test the authentication



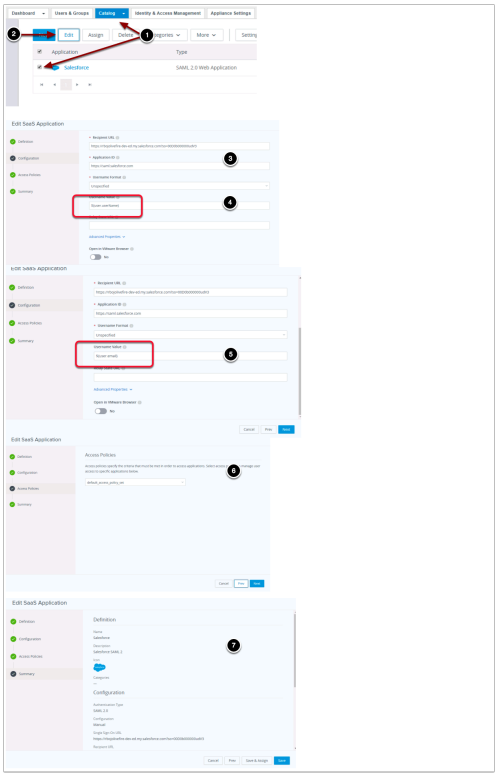

2.7

- Navigate back to your **Workspace ONE Access console from your Controlcenter machine**
  1. Select the **Catalog** tab, select **New**
  2. On the **New Saas Application** window, in the search type **sales** and select **Salesforce**, select **Next**,
  3. Under the **Single Sign-On** section under **Configuration**, select the **URL/XML radio** button.
  4. Open **file Explorer** window and browse to Downloads. Right click and open the **metadata file** you downloaded from **Sales force** that was called **SAMLSP....xml**
  5. Open in **Notepad.** In the Notepad select all or press **CTRL + A** and copy with **CTRL + C.** Now **paste** the **Metadata** in the XML field in **Single Sign-On** page under **URL/XML.**
  6. On the **Single Sign-On** page select **Next**, on the **default Access policies** page accept the default select **Next** and select Save



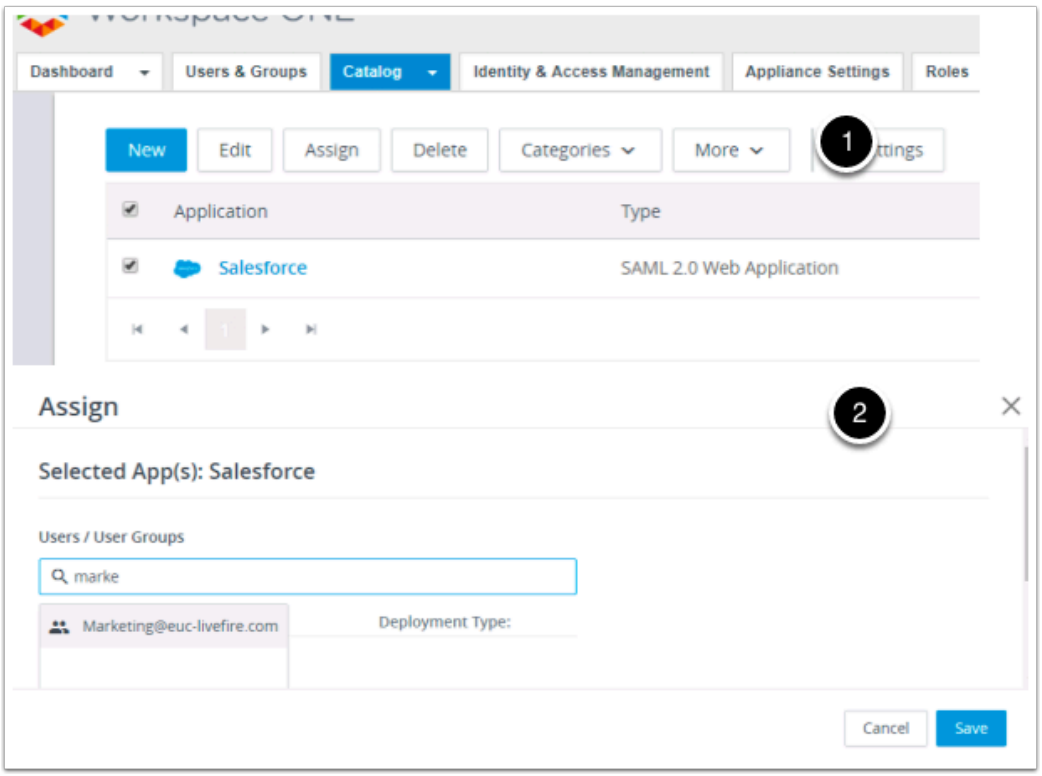

2.8

- On the **Catalog tab**, select **Salesforce** select **Edit**,
  1. Select Configuration, to the right of configuration, **scroll down** to **Username Value** and change **${user.username}** to **${user.email}**.
  2. Select **Next**, on the **Access Policies** page, select **Next**, on the **definition** page, select **Save.**



2.9

1. In the **Catalog** area next to Salesforce, select the **check box** and then select **Assign**
2. In the **Assign** window under **Users / User Groups** box type **marke** and select **Marketing@euc-livefire.com** and select Save



3.0 Testing your custom account with the Salesforce and office 365 Federation

- Open up an Incognito window an alternate browser and login to your SaaS instance of Workspace ONE Access with your custom user account
  - Select and **open** your Salesforce Application
  - Select and **open** one of your Office Applications. NB! Depending on what Microsoft application you might still get messages stating that Office 365 is being setup. At this point all we are concerned is the federation of office 365