Certificate Based Authentication 2.0

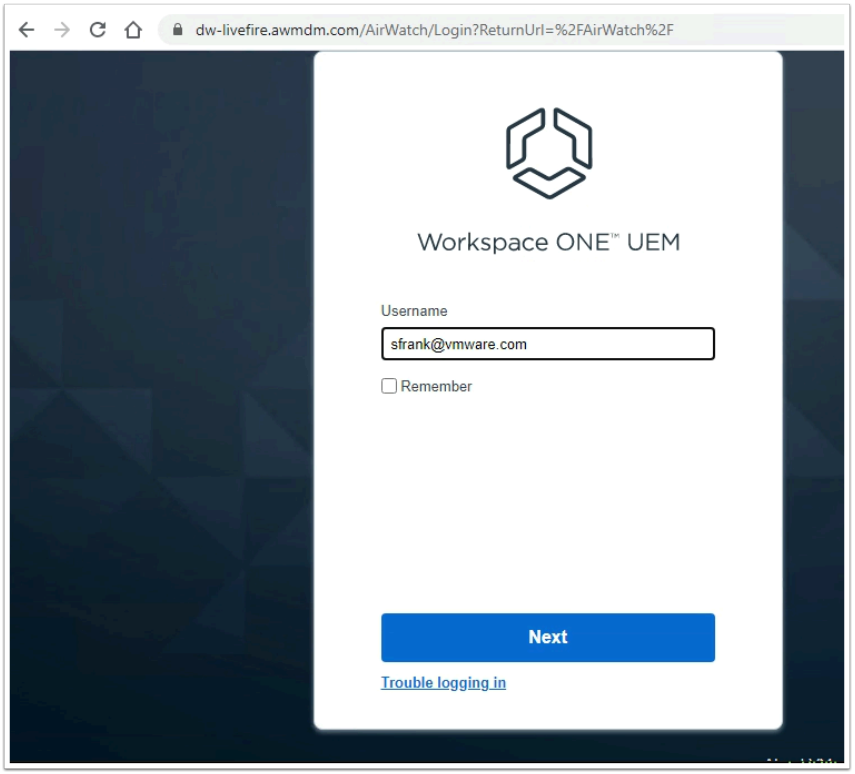
In this lab you will be deploying a certificate to an enrolled Windows 10 virtual machine. This certificate will be generated by the built-in CA in Workspace ONE UEM.

We will later configure Workspace ONE Access to trust certificates issued by UEM and configure the Certificate (Cloud Deployment) authentication adapter.

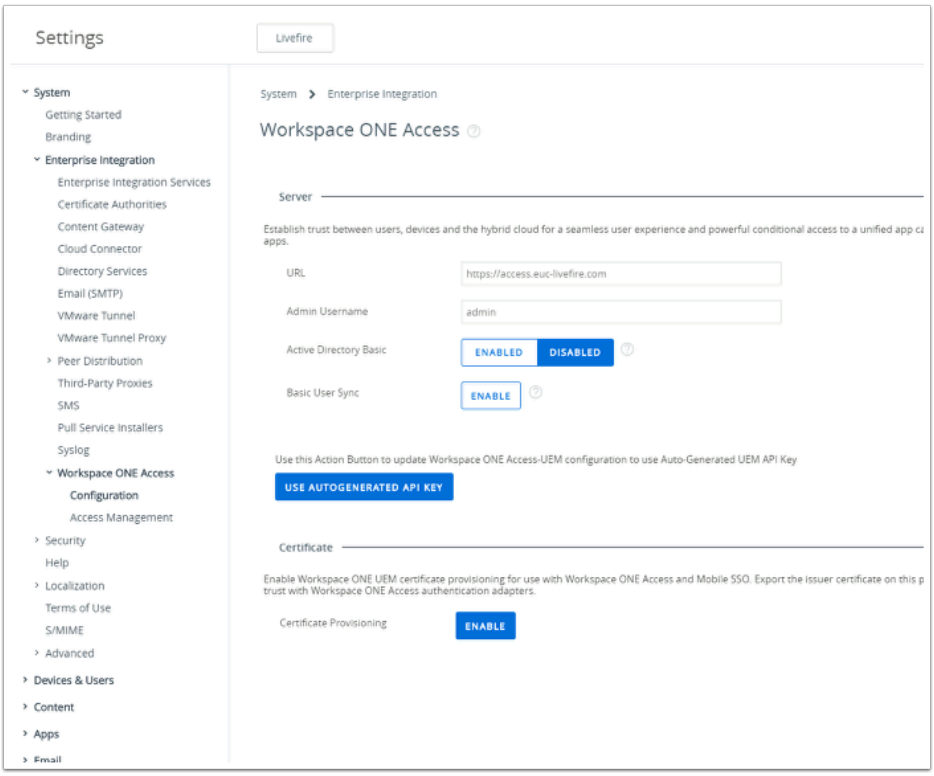
Finally we will test everything on a Windows 10 vm to ensure we are able to have a seamless authentication experience.

Extra Material is optional and will show you how to suppress the pop-up users see in Chrome and to automate this using UEM.

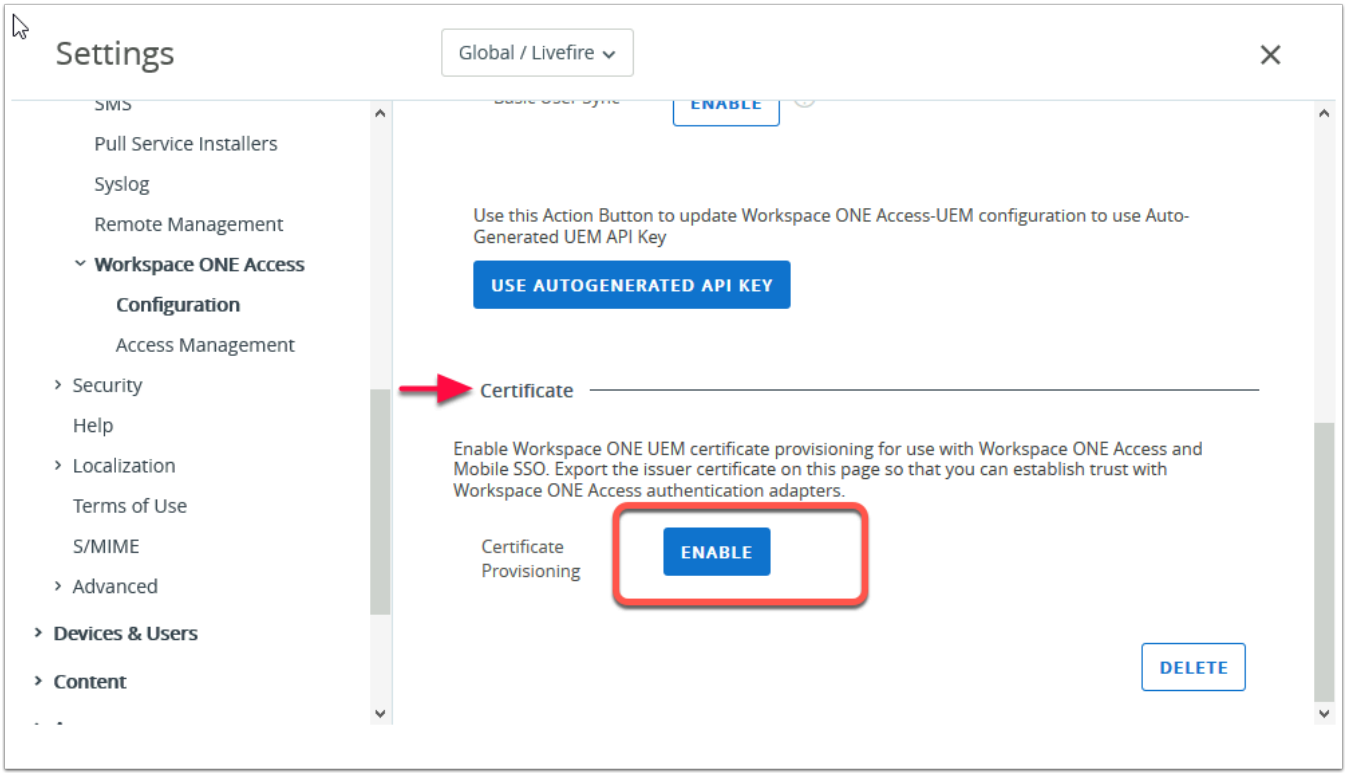
Part 1: WorkspaceOne UEM - Certificate Profile



1. On your **ControlCenter** jumpbox
   1. Open Google Chrome
   2. Navigate to https://cn-livefire.awmdm.com
   3. Authenticate using :
      - Username your **e-mail address**
      - **Password VMware1!** (if you didn't change it from the default)

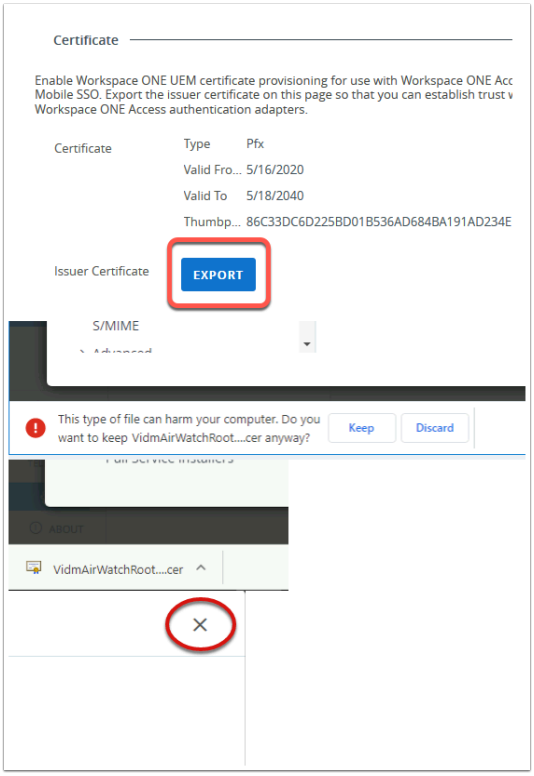


2. In the Workspace ONE UEM Console
   - Navigate to **Groups & Settings** > **All Settings** > **System** > **Enterprise Integration** > **Workspace ONE Access** > **Configuration**

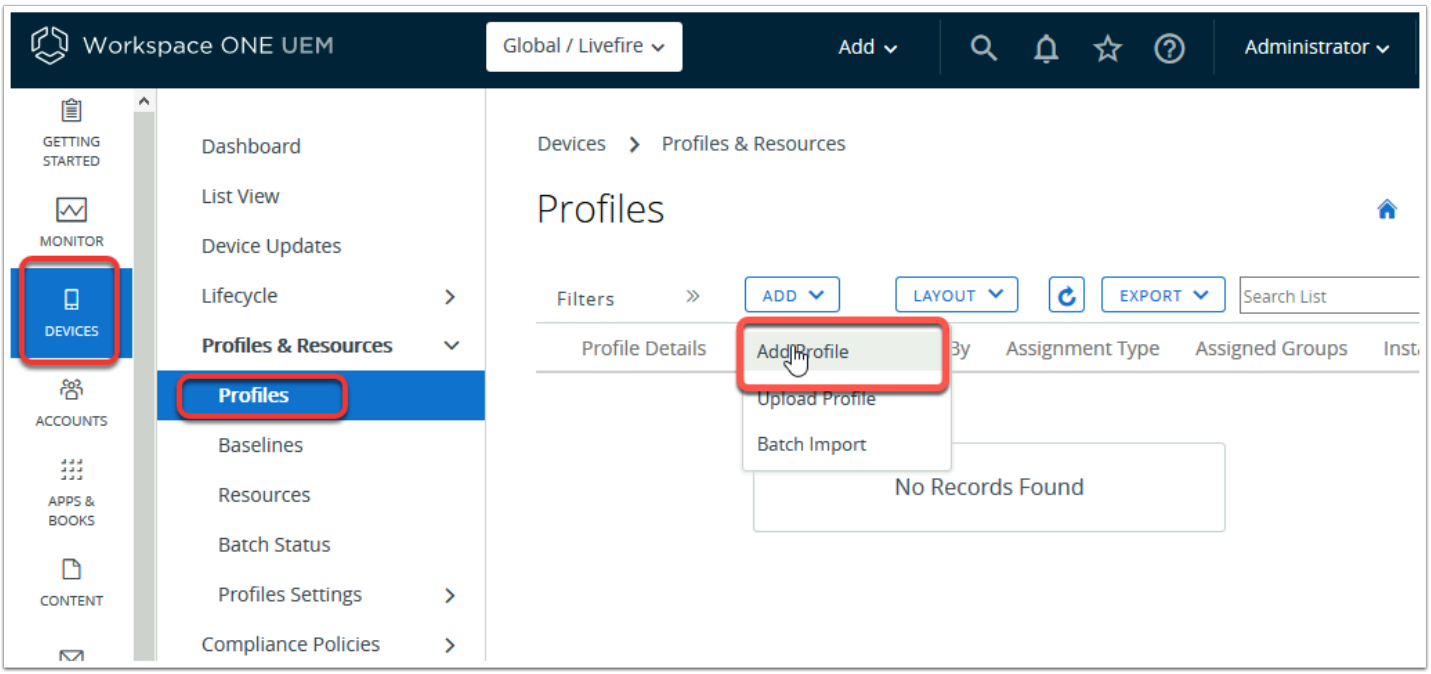


3. In the **Enterprise Integration > Workspace ONE Acces** page
   - **Scroll** down to find the **Certificate** section

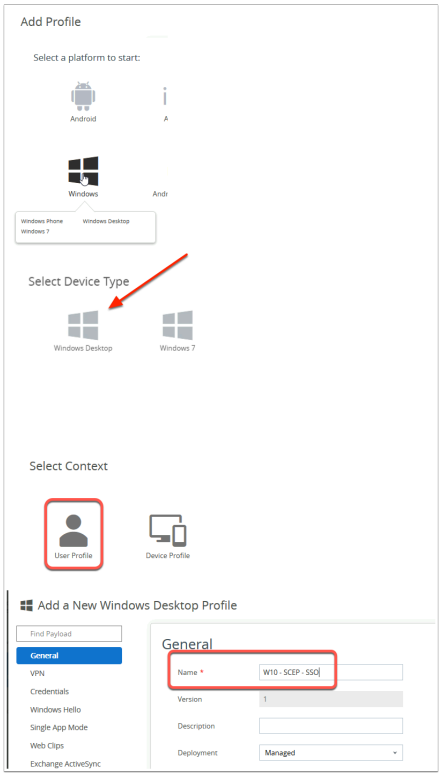
- Under **Certificate** select **ENABLE** (if not already enabled)



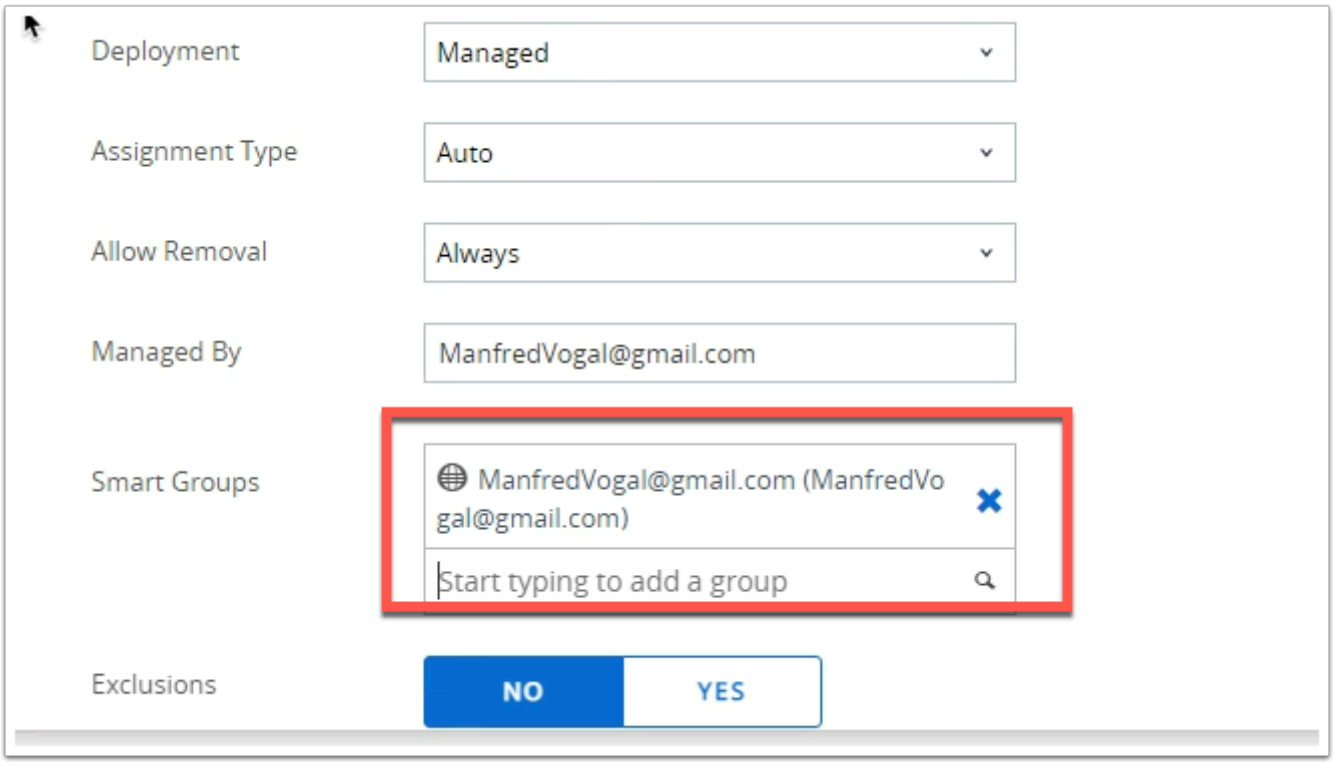
4. In the **Enterprise Integration > Workspace ONE Acces** page
   - In the **Certificates** section
     - Select **EXPORT**
     - When prompted, select **Keep**
     - Note this will download a .cer file (**VidmAirWatchRootCertificate.cer**)
     - Close the **Settings w**indow in the top right-corner, by selecting **x**
     - **NOTE:** You may have downloaded this certificate in a prior lab you can leverage this certificate.



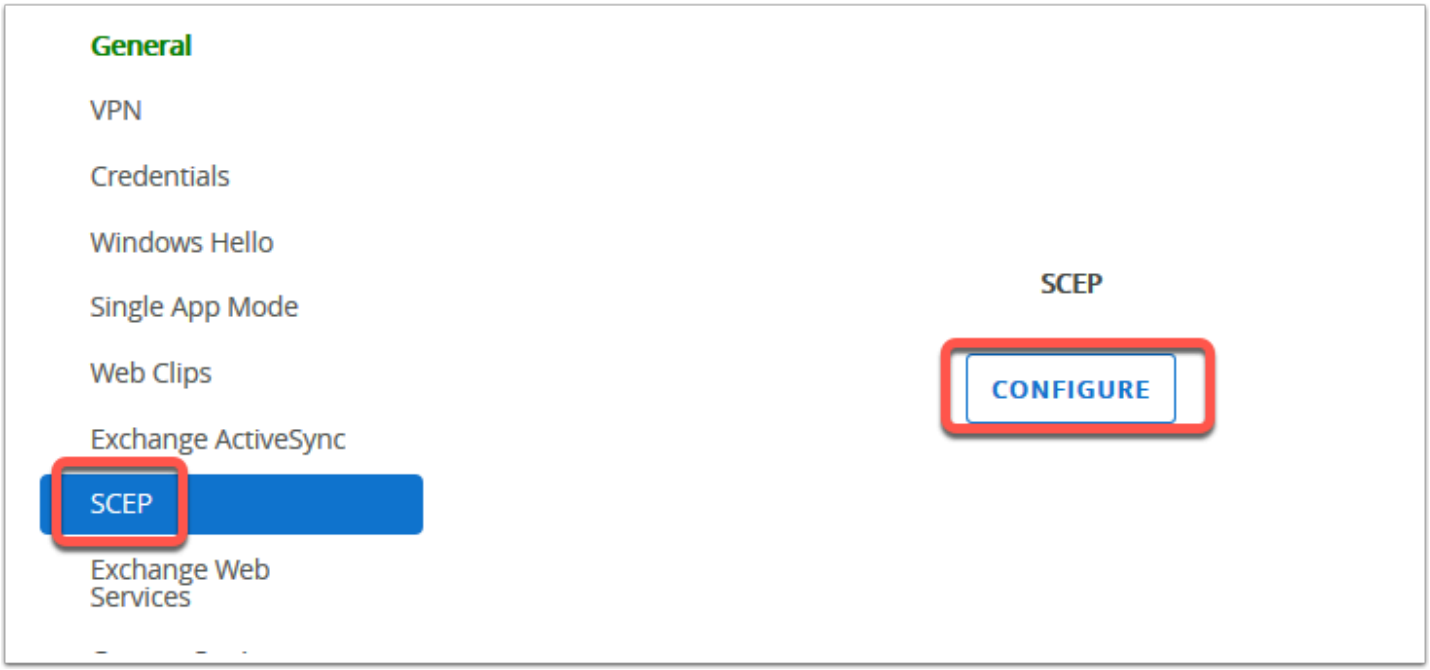
5. In the Workspace ONE UEM admin console
   - Navigate to **Devices** > **Profiles & Resources** > **Profiles** > **ADD** > **Add Profile**



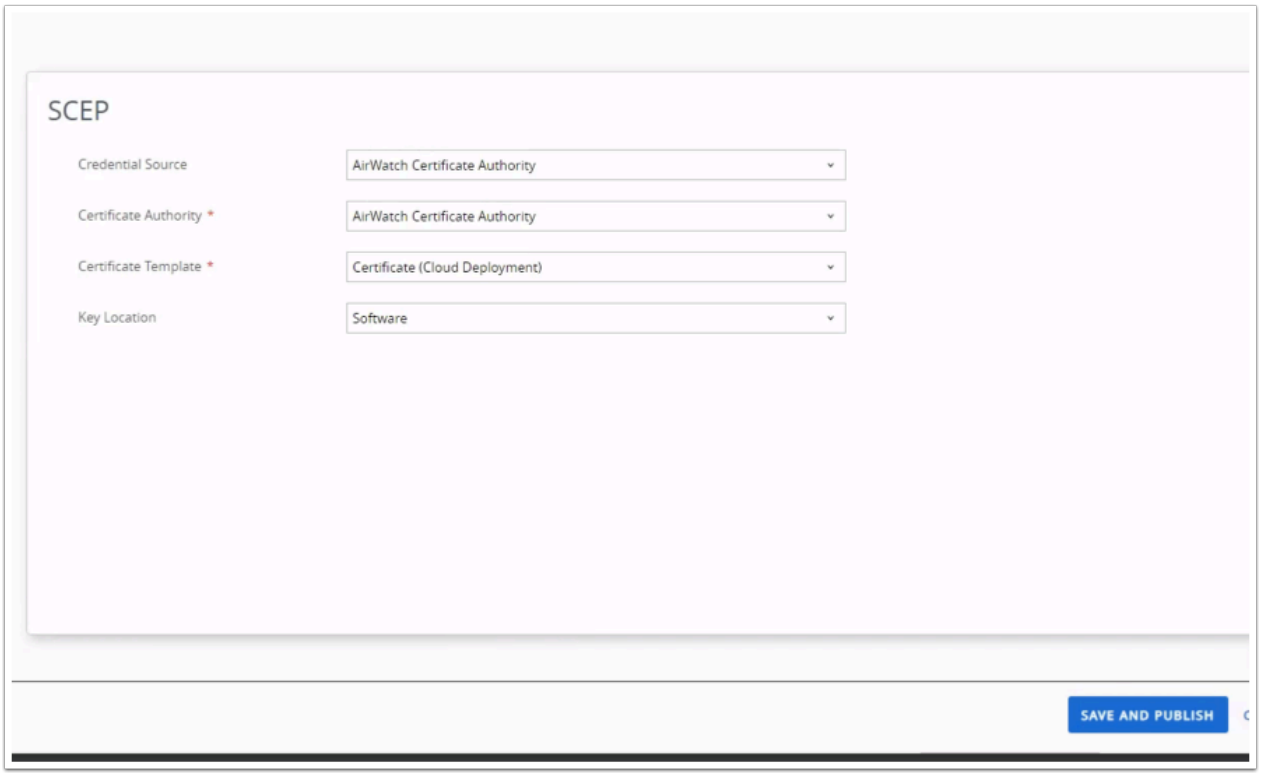
6. In the Add Profile window
   - Select Windows > Windows Desktop > User Profile
   - Under **General**
     - Next to **Name**: type **W10 - SCEP - SSO** .



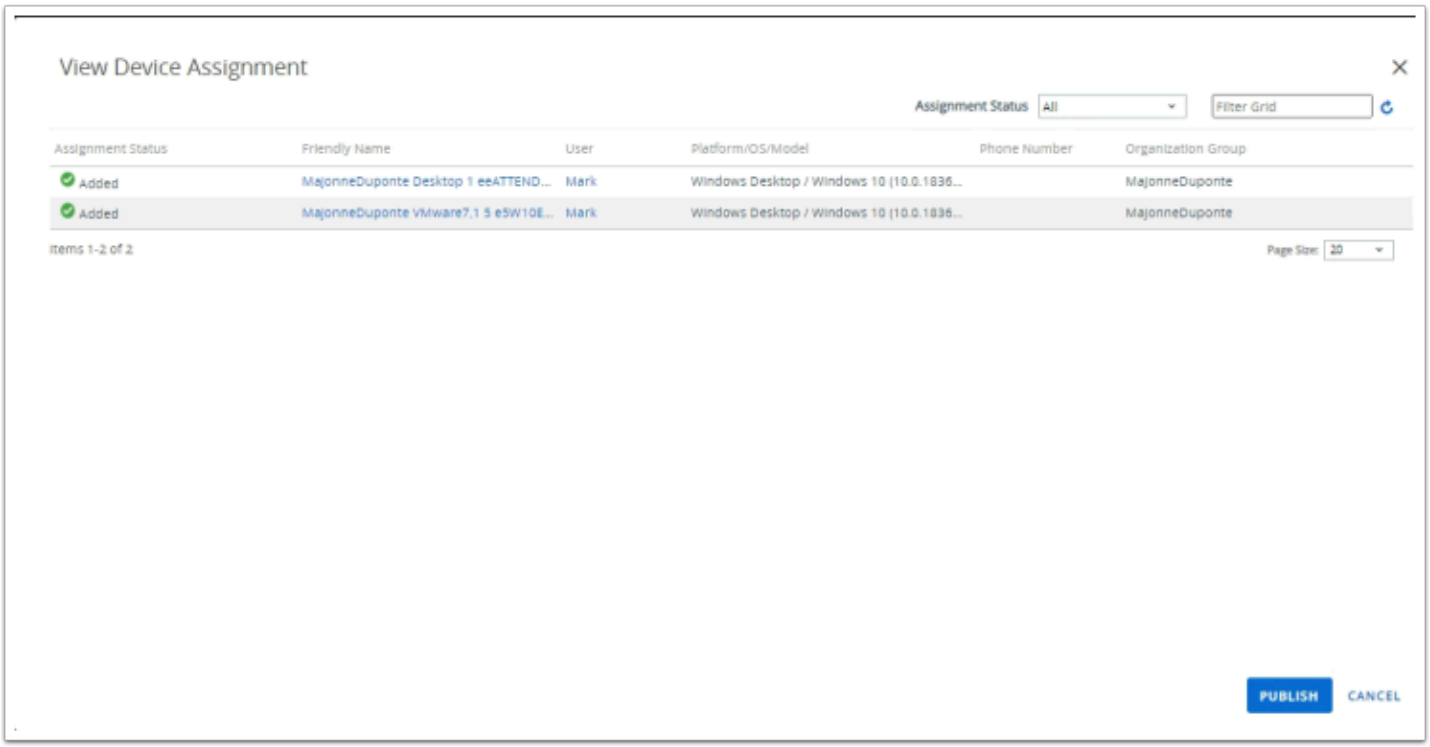
7. In the **Add a New Windows Desktop Profile**
   - In the **General** tab,
     - Scroll down to **Smart Groups**
       - Select you **Organization Group** (This should be your e-mail address) with the **world icon** next to it.



8. In the **Add a New Windows Desktop Profile**
   - In the LEFT MENU, navigate to the **SCEP**
   - Select **CONFIGURE**



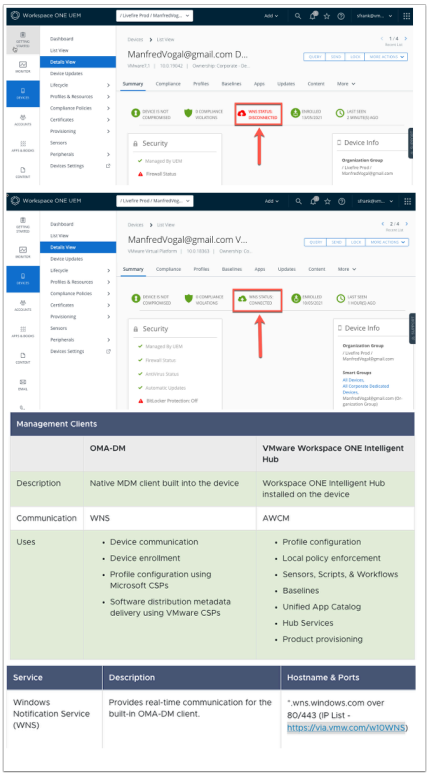
9. In the **Add a New Windows Desktop Profile**
   - Under **SCEP,** Set the following, next to:
     - **Credential Source:** **AirWatch Certificate Authority**
     - **Certificate Template:** **Certificate (Cloud Deployment)**
     - **Key Location:** **Software**
     - Select **SAVE AND PUBLISH** at the bottom right of the window



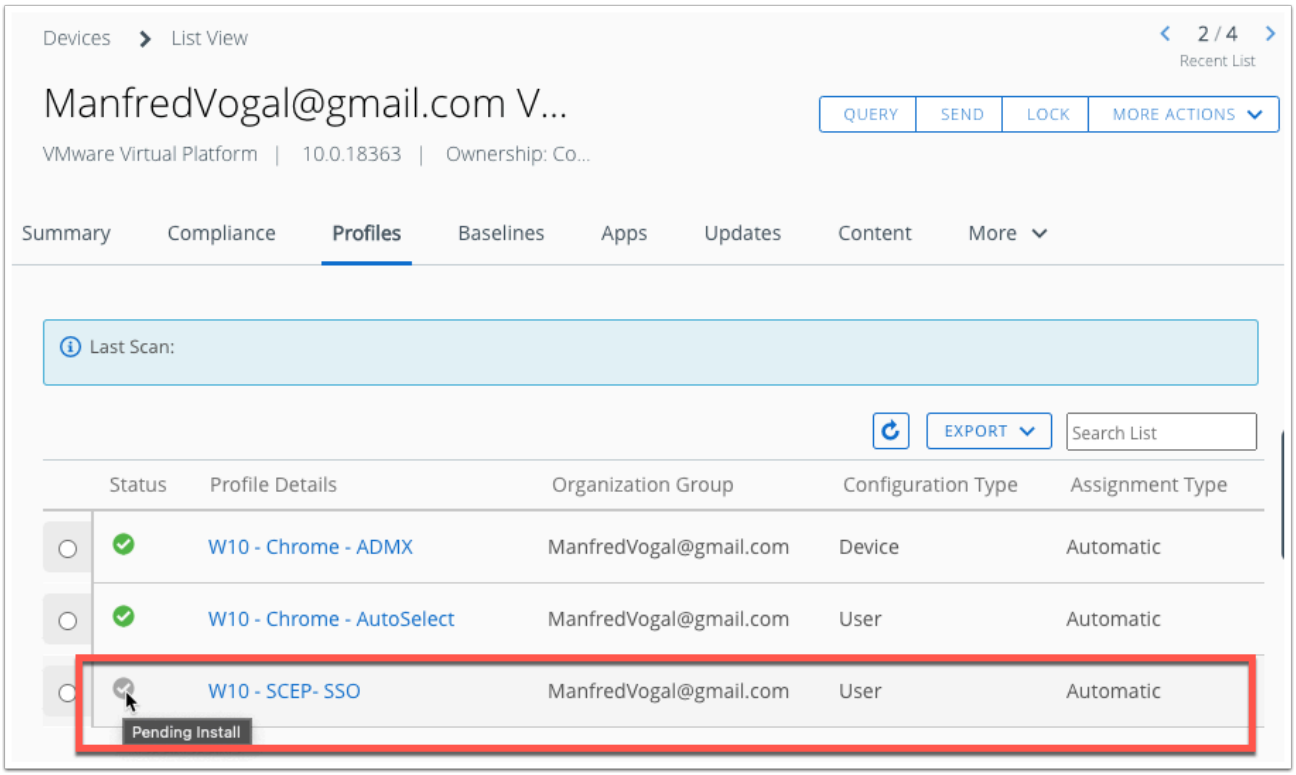
10. On the **View Device Assignment** page
    - Confirm your device is showing
    - Select **PUBLISH**

Troubleshooting Tips

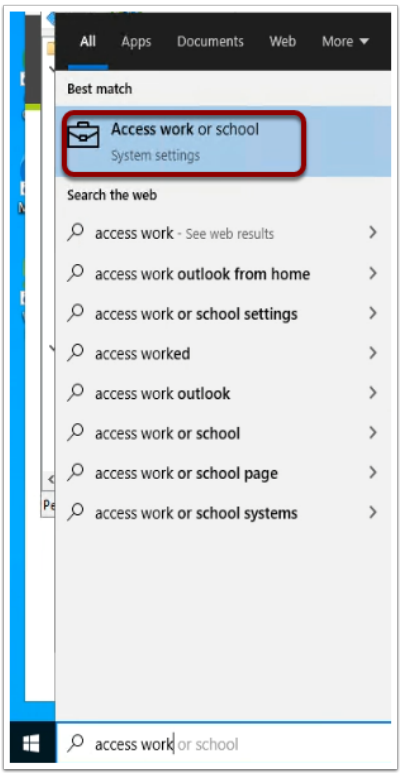
Should the certificate not get deployed please follow the steps below to force the certificate to be pushed.



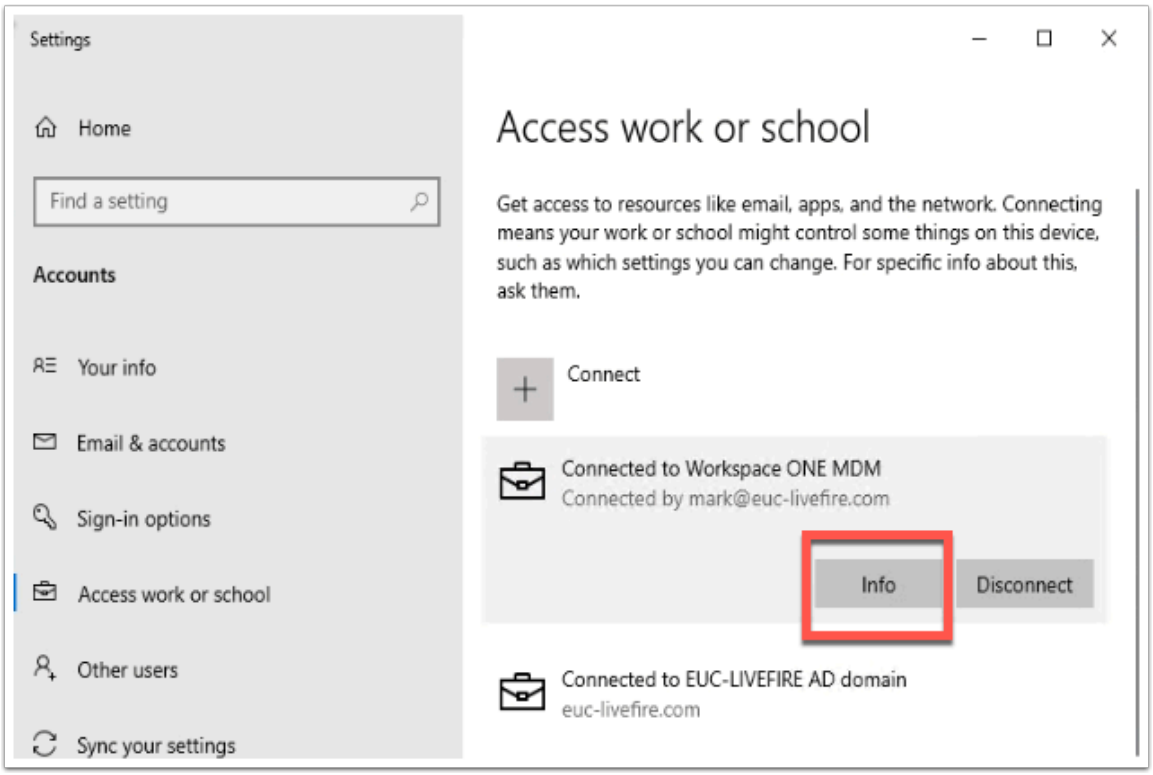
1. We have observed in certain scenarios the device is reporting **WNS STATUS: DISCONNECTED** when it should be **WNS STATUS: CONNECTED**. This can lead to a delay in the client certificate being deployed to the device. In the communication flow WNS (Windows Notification Services) are responsible for triggering a check in between the OMA-DM client and the Workspace ONE UEM Server. Network constraints can sometimes play a role and we recommend seeing Microsoft's guidelines: https://via.vmw.com/w10WNS



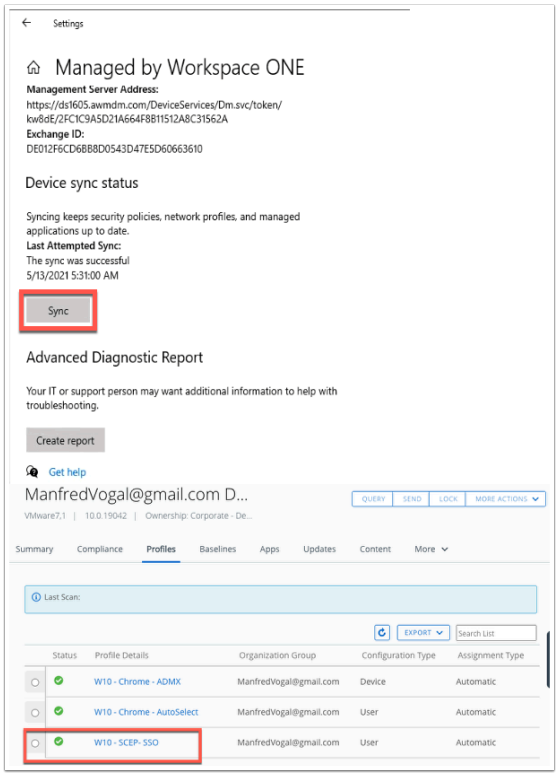
2. In the **WorkspaceONE UEM Console** navigate to **Device** > **List View** > Select the unique VM you are working on (Previously W10Client01).
   - Select the **Profiles** tab.
   - If you are getting a **green** tick the certificate ha been deployed and you can move to part 2 of the lab.
   - However if you are getting a **grey** tick it means the profile is pending install.



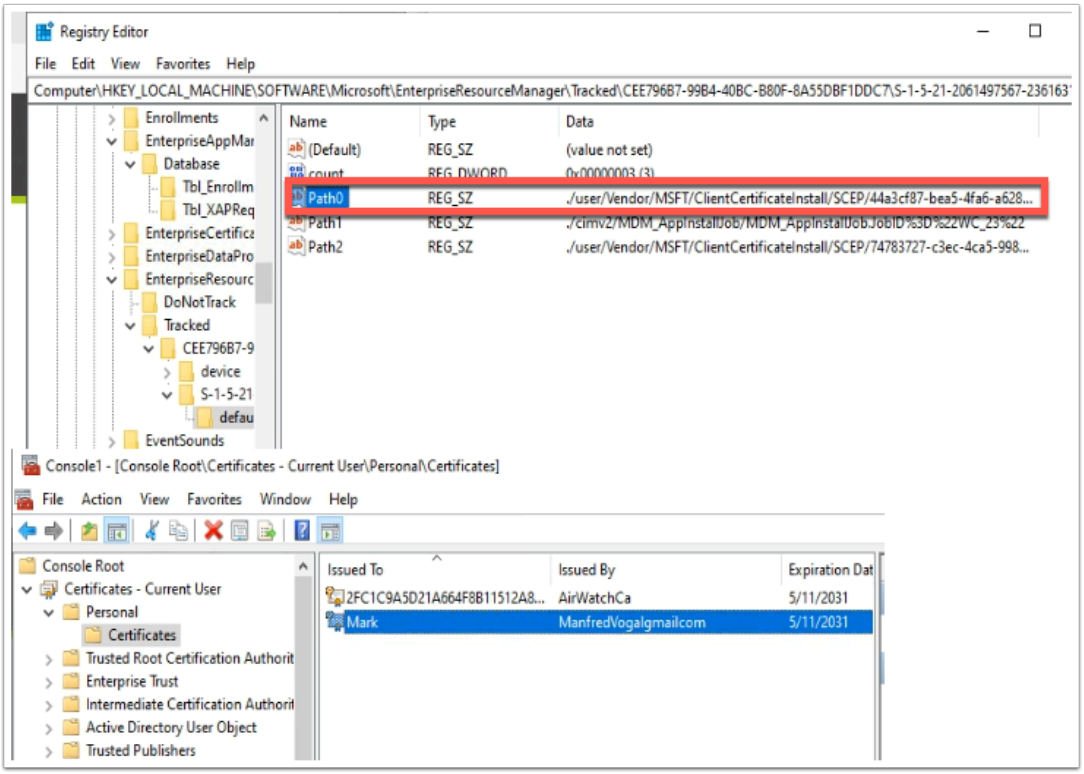
3. Navigate to the Windows 10 VM and type **access work** into the search and click the **Access work or School System settings**



4. Click on **Connected to Workspace ONE MDM**
   - Click on **Info**



5. Scroll to the bottom of the page and click **Sync**
   - This should trigger a manual check in with **WorkspaceONE UEM** and trigger the deployment of the certificate. Allow for a few minutes while this process takes place.
   - Double check in the WorkspaceONE UEM console to make sure that there is now a **Green** tick next to the **W10 - SCEP - SSO** profile.

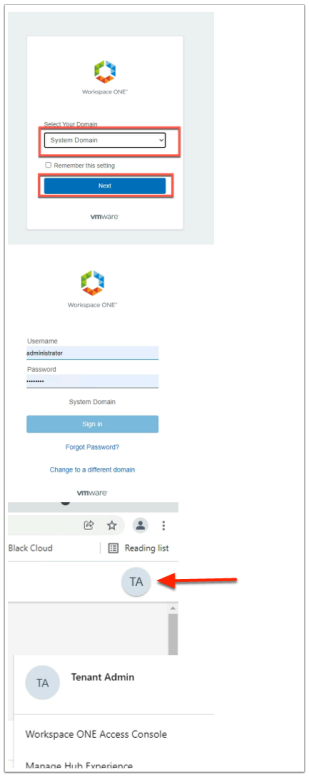


6. Should you require further troubleshooting check this registry key for installed profiles -

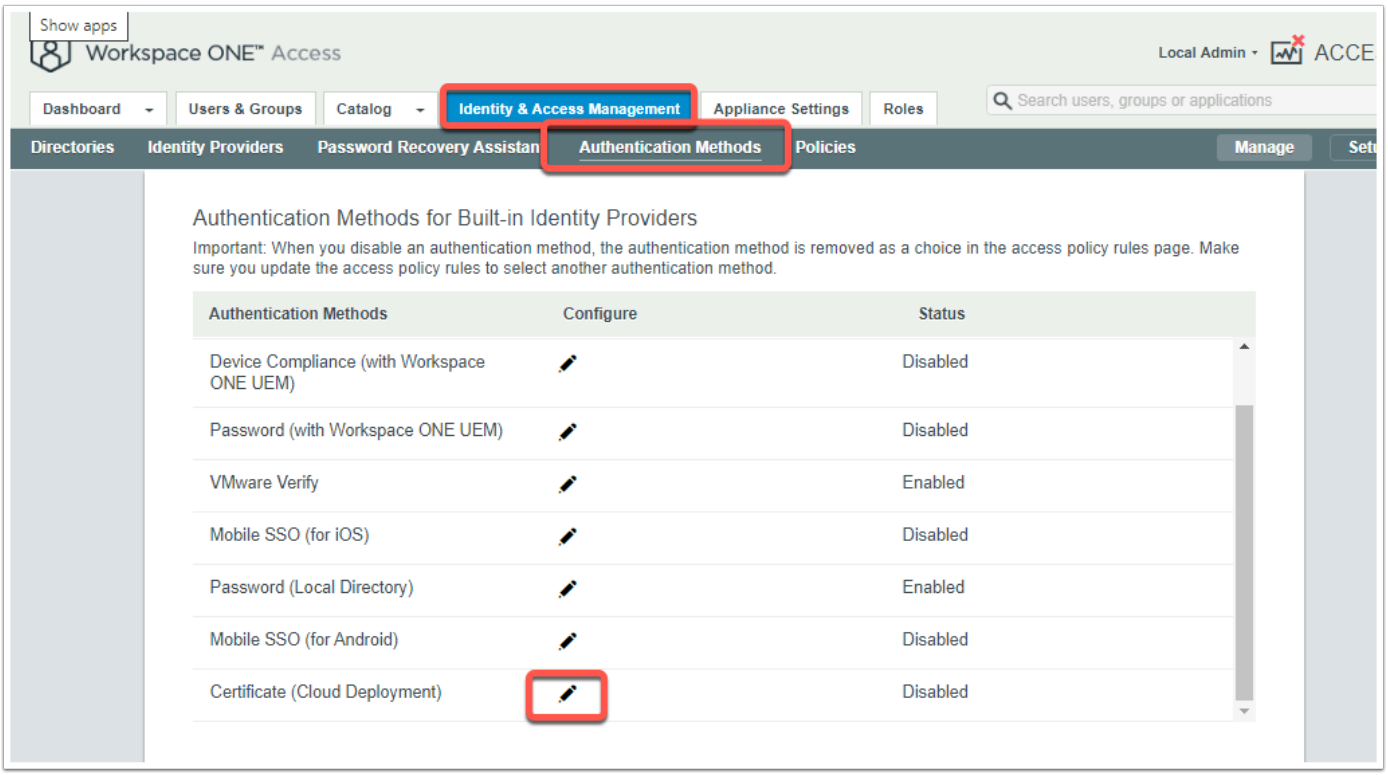
`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseResourceManager\Tracked`

You can also check the Certificate store in MMC under **Personal** > **Certificates** to ensure you have the client certificate installed.

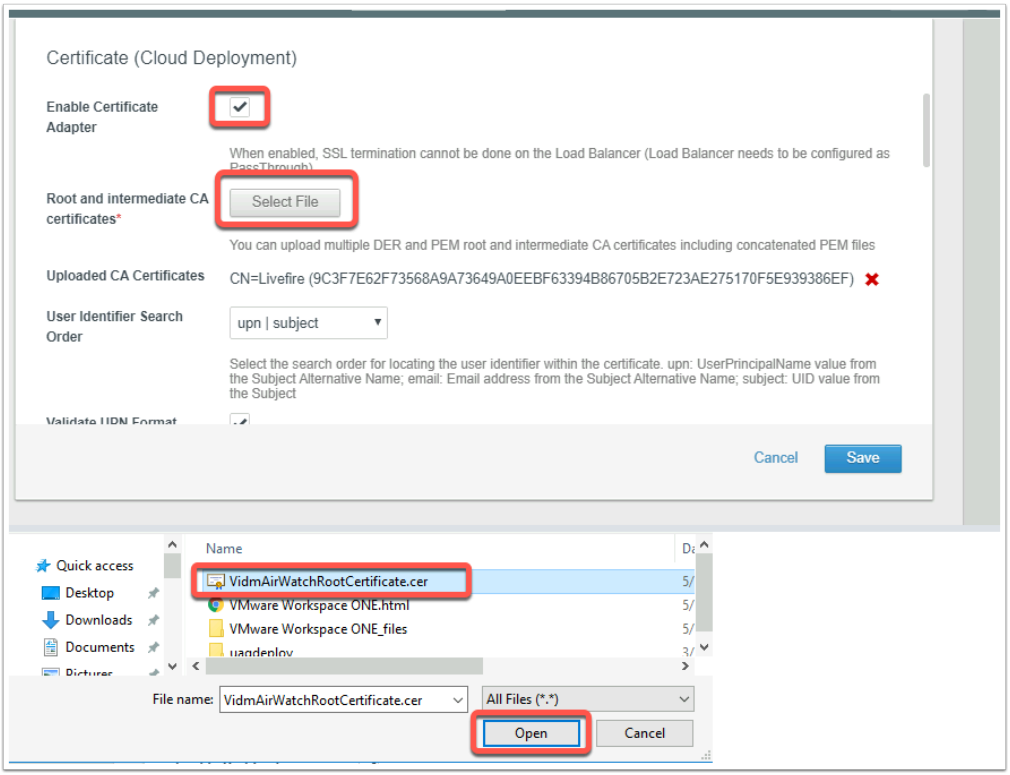
Part 2 : Configure Workspace ONE Access



1. On your **ControlCenter** server
   - In the Chrome browser
   - Navigate to your unique Workspace ONE Access tenant.
   - Authenticate using **System Domain**
     - username: **Administrator**
     - password: **VMware1!**
   - In the Web Intelligent Hub
     - In the top right corner, select the **TA** Icon
     - In the **Tenant Admin** interface
       - Select **Workspace ONE Access Console**

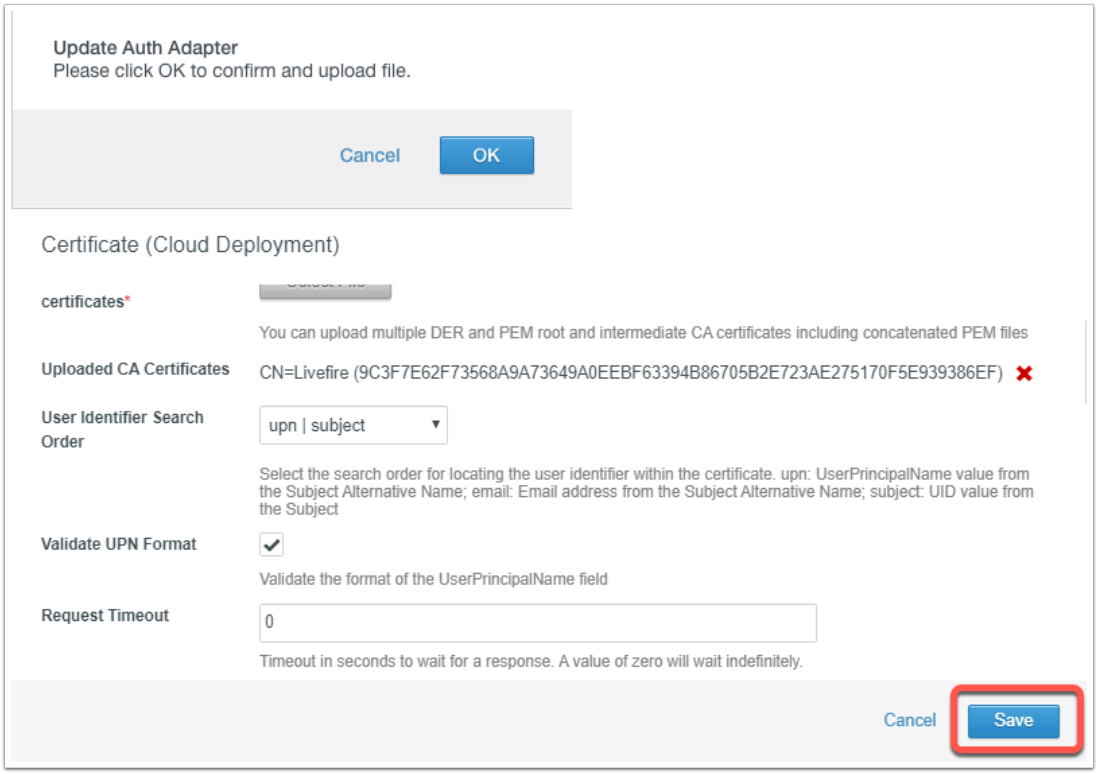


2. In the Workspace ONE Access admin console
   - Navigate to **Identity & Access Management** > **Authentication Methods**.
   - Select the **pencil** **icon** next to **Certificate (Cloud Deployment)**



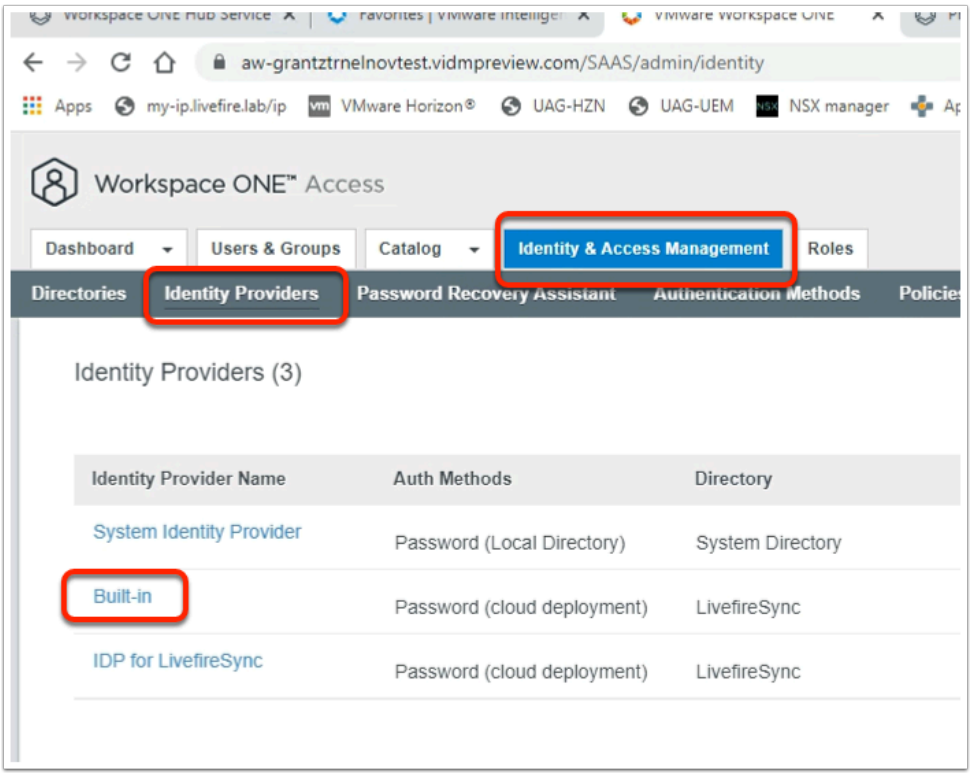
3. In the **Certificate (Cloud Deployment)** page
   - Select the **tickbox** to **Enable Certificate Adapter**

- Select **Select File** for the **Root and Intermediate CA Certificates**
- Select the **certificate** we have downloaded from the UEM console earlier
- Select **Open**

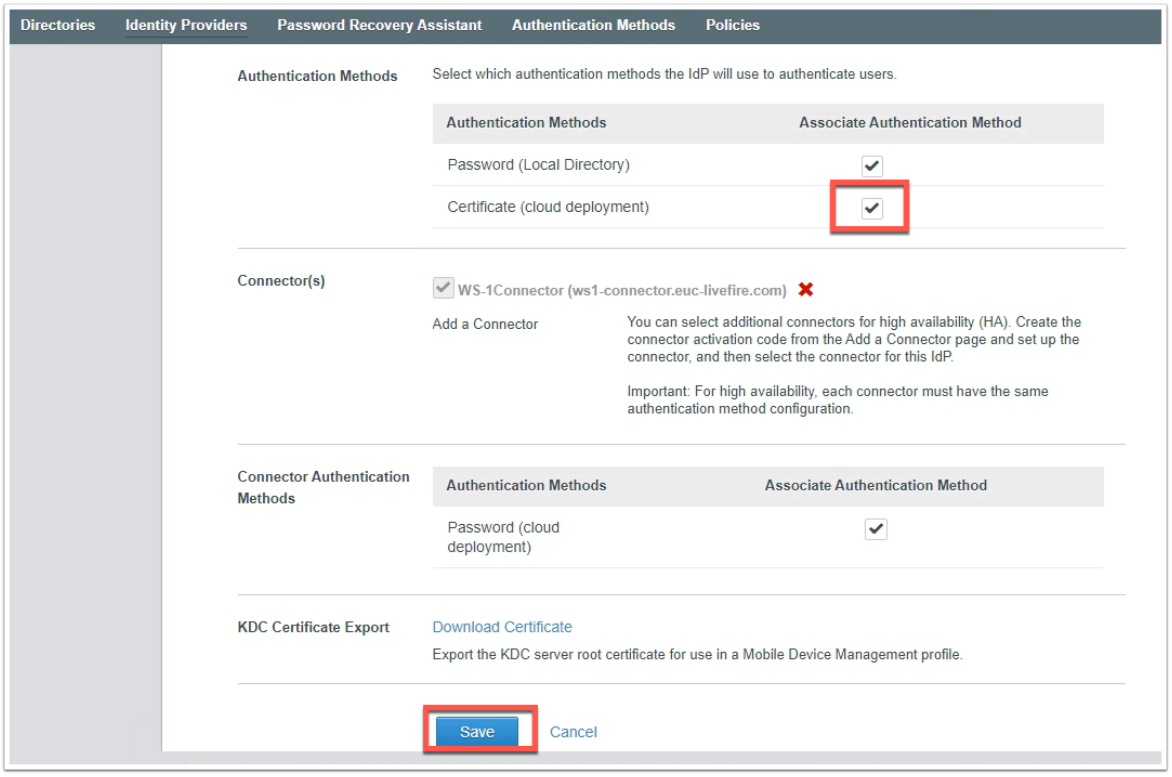


4. In the **Update Auth Adapter** window
   - Select **OK**.

- In the **Certificate (Cloud Deployment)** window
  - At the bottom of the page, select **Save**

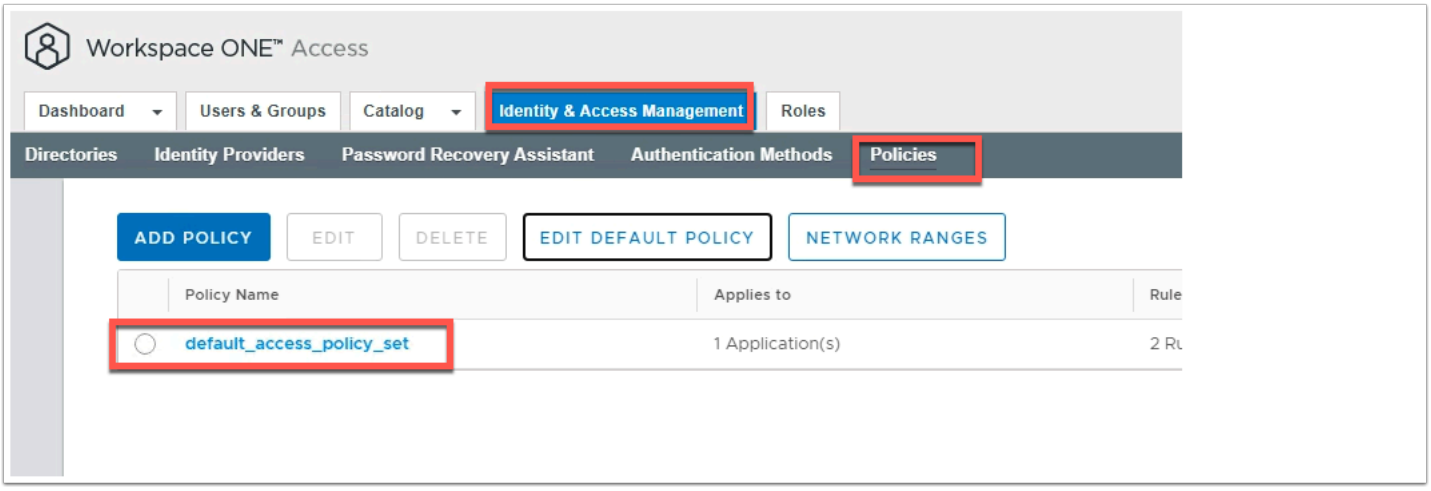


5. In the **Workspace ONE Access** Console
   - Navigate **Identity Providers**
   - Under **Identity & Access Management, s**elect on **Built-in**

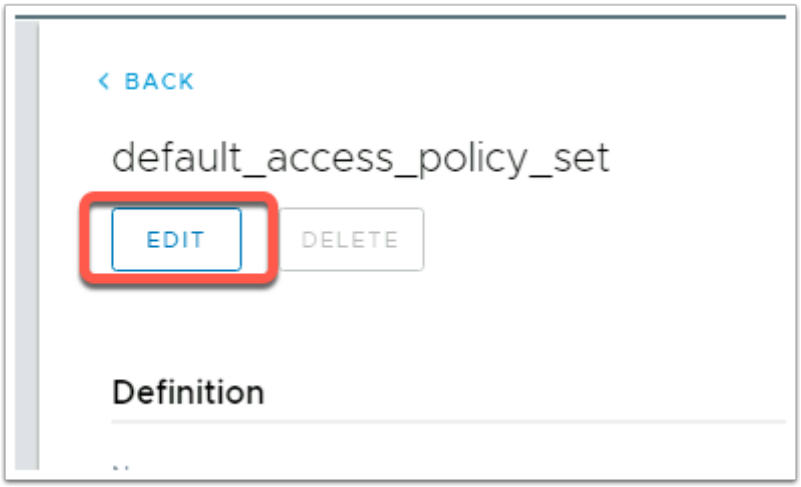


6. In the **Built-In** page
   - Navigate to the **Authentication Methods** area

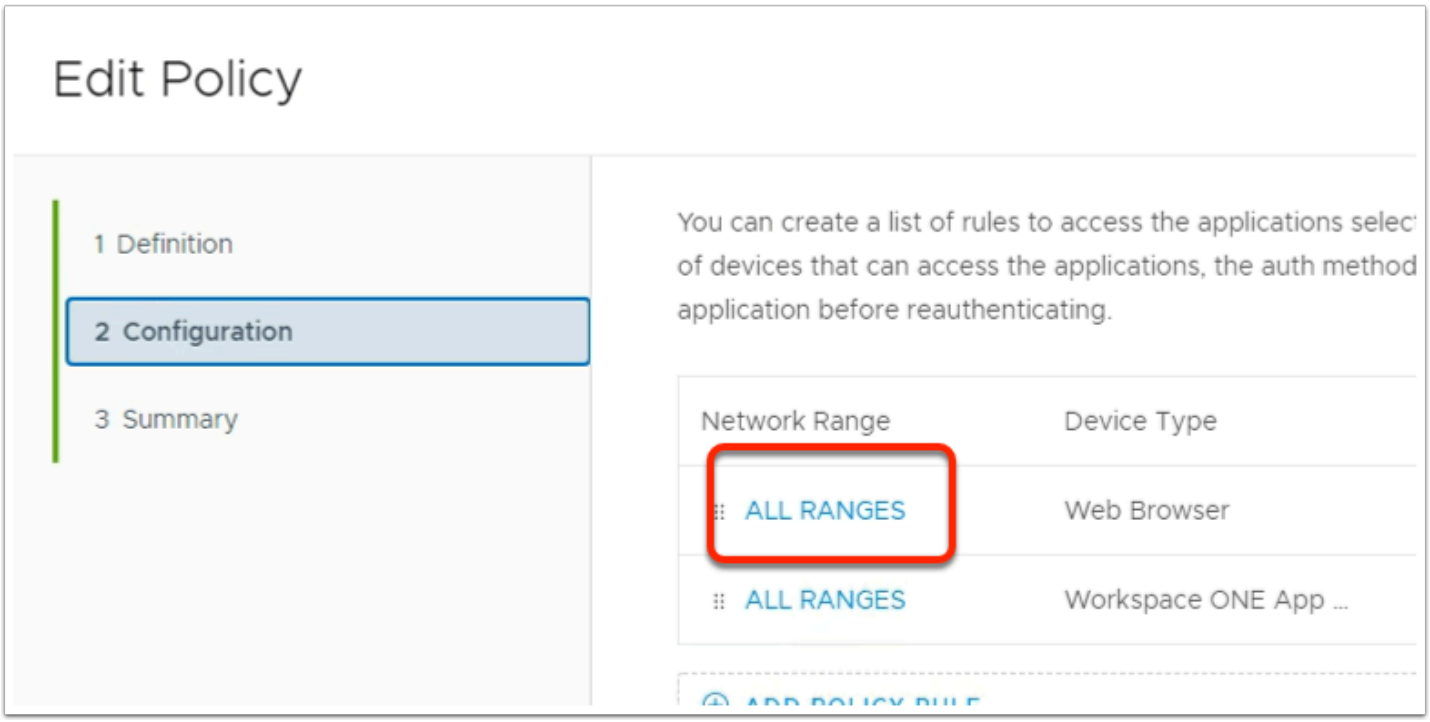
- Select the **check box** next to **Certificate (Cloud Deployment)**
- Select **Save** at the bottom of the page.



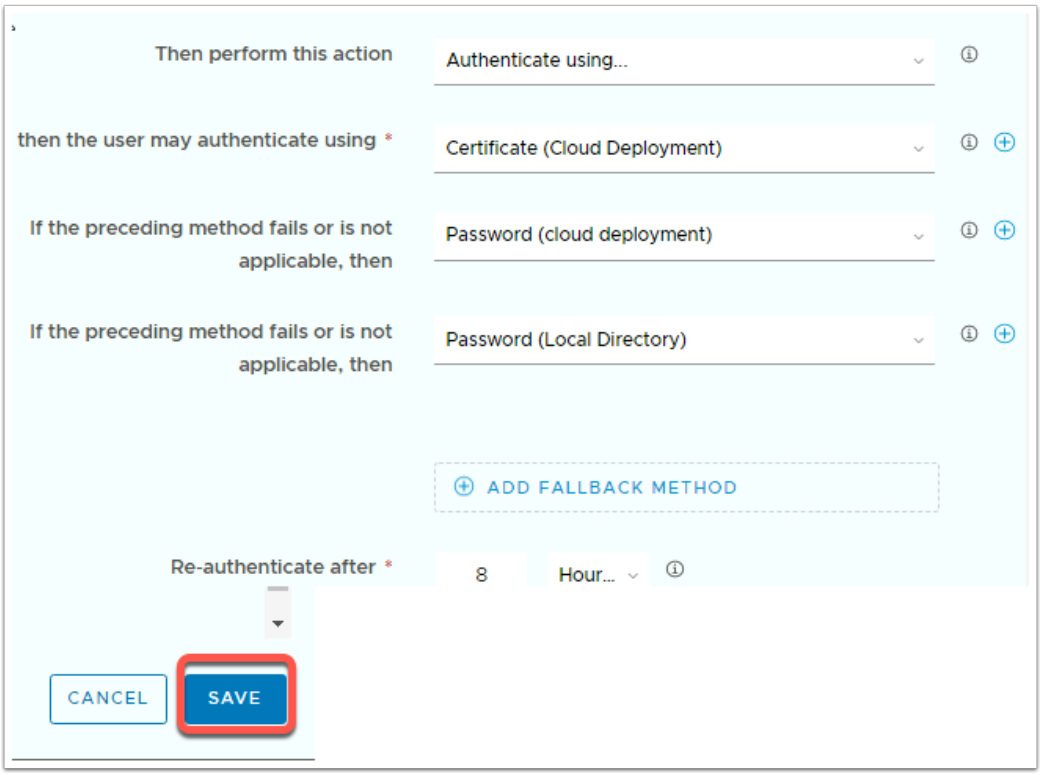
7. In the **Workspace ONE Access** console
   - Navigate to **Identity & Access Management** > **Policies**
   - Select **default_access_policy_set**



8. **Under Policies \ default_access_policy_set**
   - Select **EDIT**

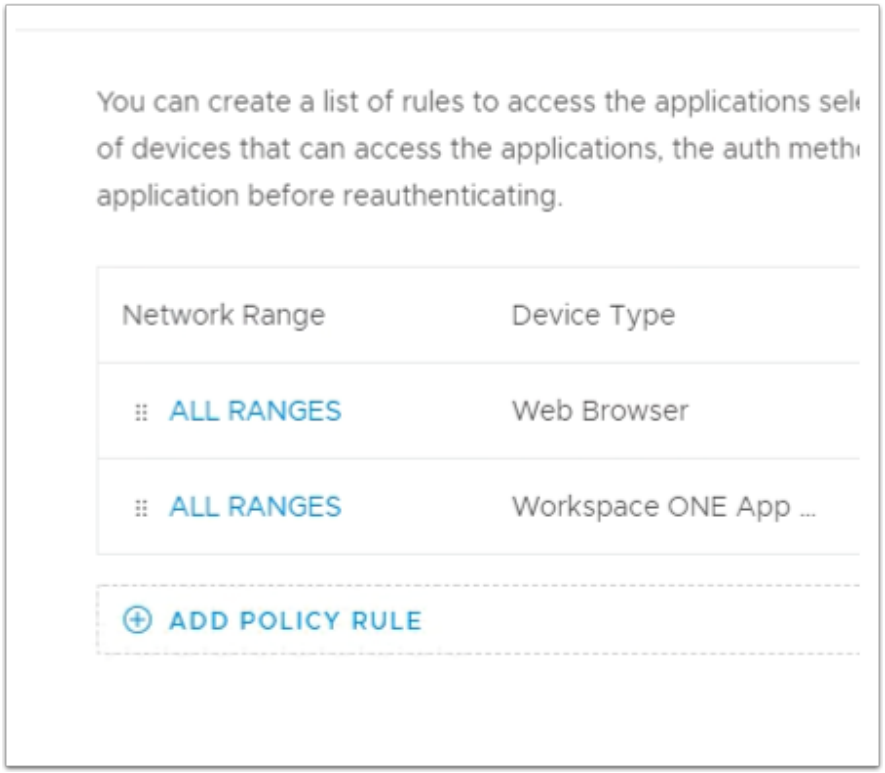


9. In the **Edit Policy** page
   - Select the second tab from the left column **Configuration**
   - Select **All Ranges** next to **Web Browser** in the Device **Type Category**

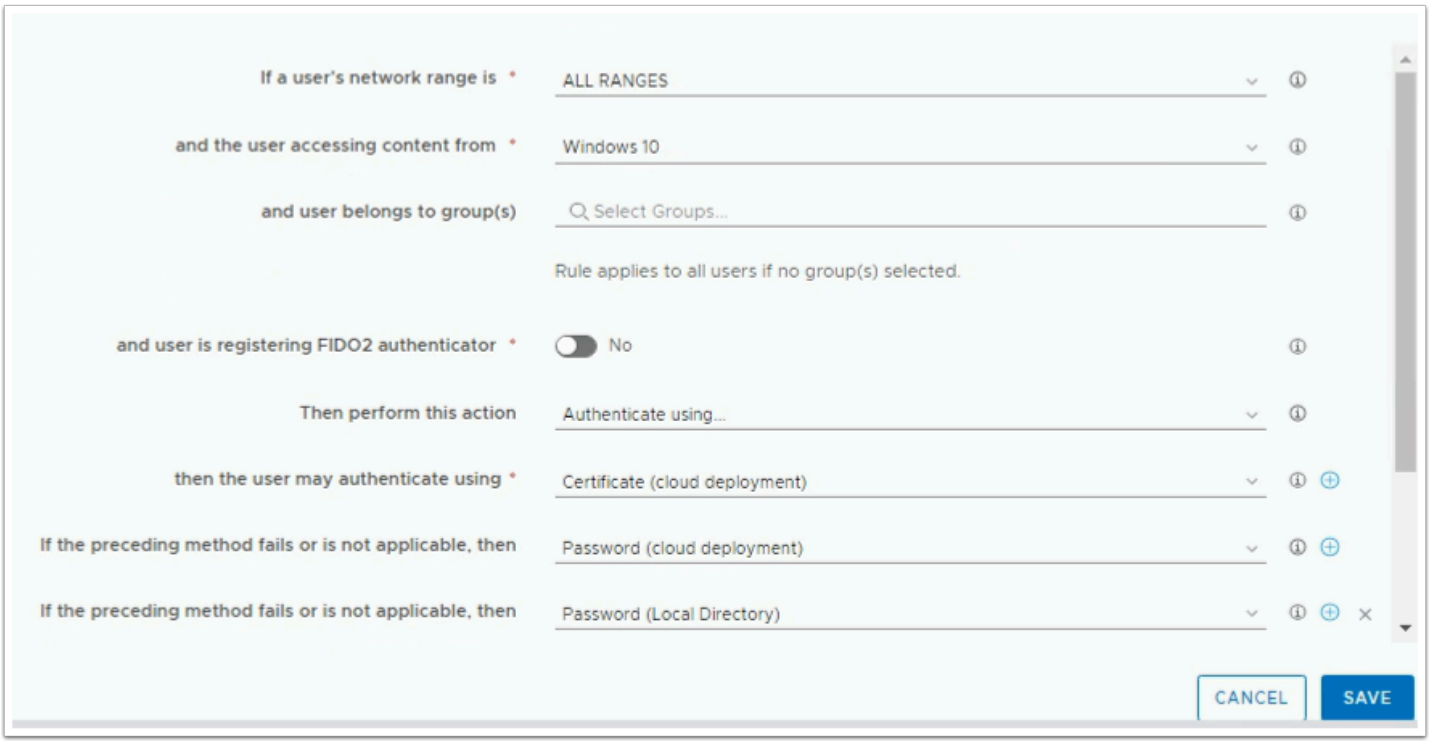


10. In the **Edit Policy Rule** page, edit the following next to:
    - **then the user may authenticate using *** change to : **Certificate (Cloud Deployment)**

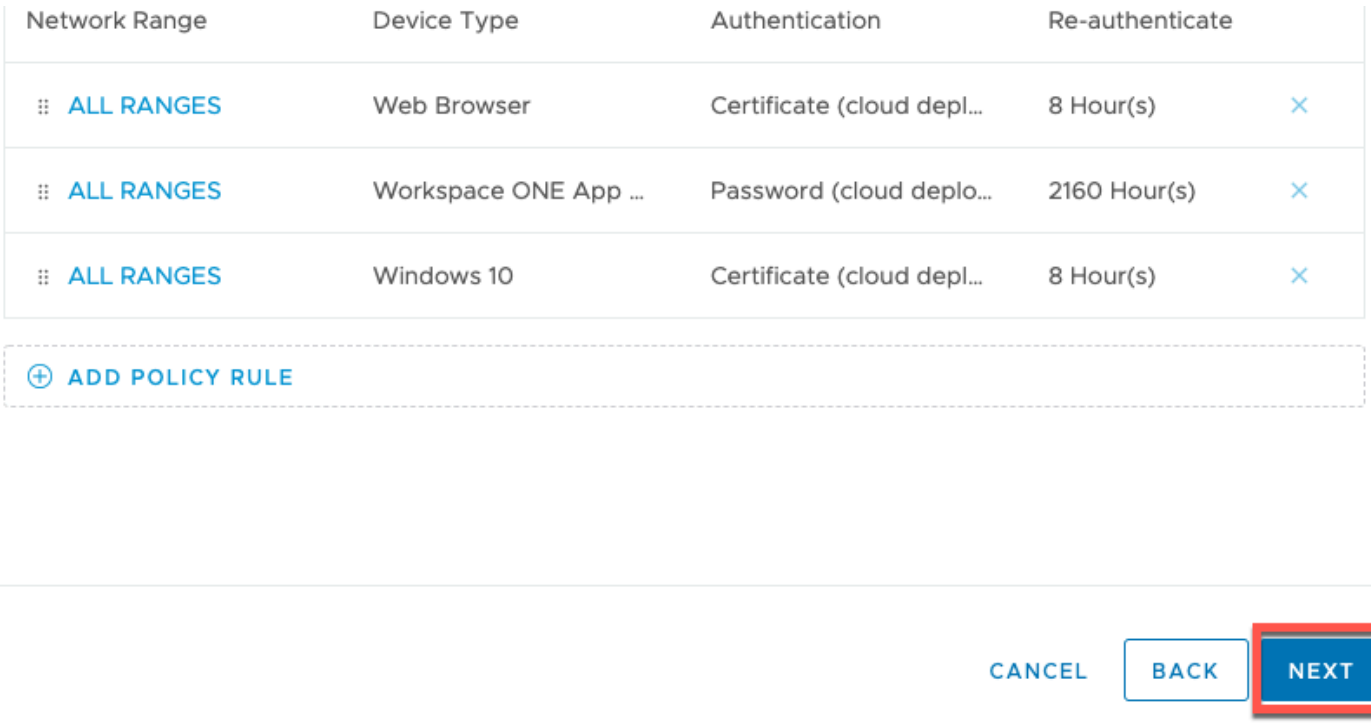
- **if preceding method fails or is not applicable then** change to **Password (Cloud Deployment)**,
- then Select **ADD FALLBACK METHOD**
- Select **Password (Local Directory)** as the third authentication option.
- Select **SAVE** at the bottom of the window



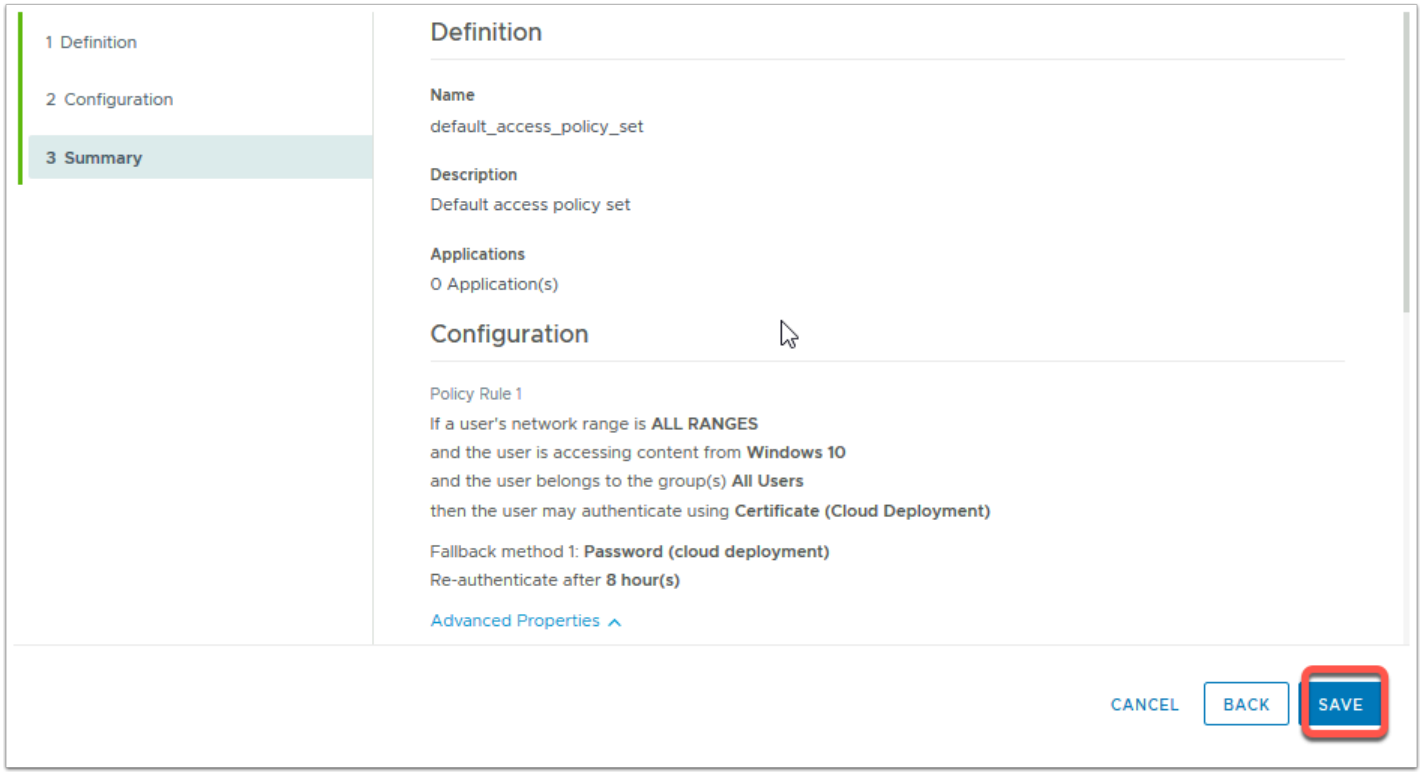
11. In the **Edit Policy \ Configuration** page
    - Select **ADD POLICY RULE**



12. In the **Add Policy Rule** page, add the following next to :
    - **and user accessing content from :** from the *drop down* select:- **Windows 10**
    - **then the user may authenticate using:** from the *drop down* select:- **Certificate (Cloud Deployment)**
    - **If the preceding method fails or is not applicable, then** : from the *drop down* select:- **Password (cloud deployment)**
    - Select **+ADD FALLBACK METHOD**
    - **If the preceding method fails or is not applicable, then** : from the *drop down* select:- **Password (Local Deployment)**
    - Select **SAVE**

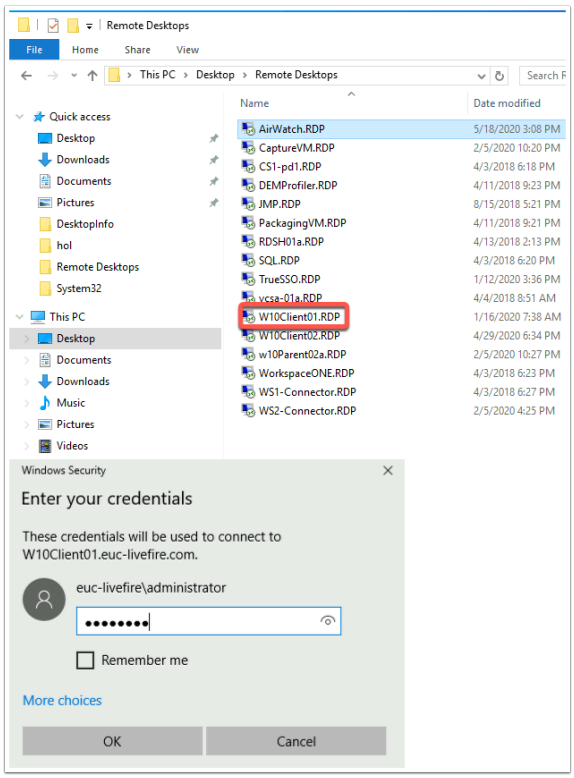


13. Select **NEXT** on the **Edit Policy Page**

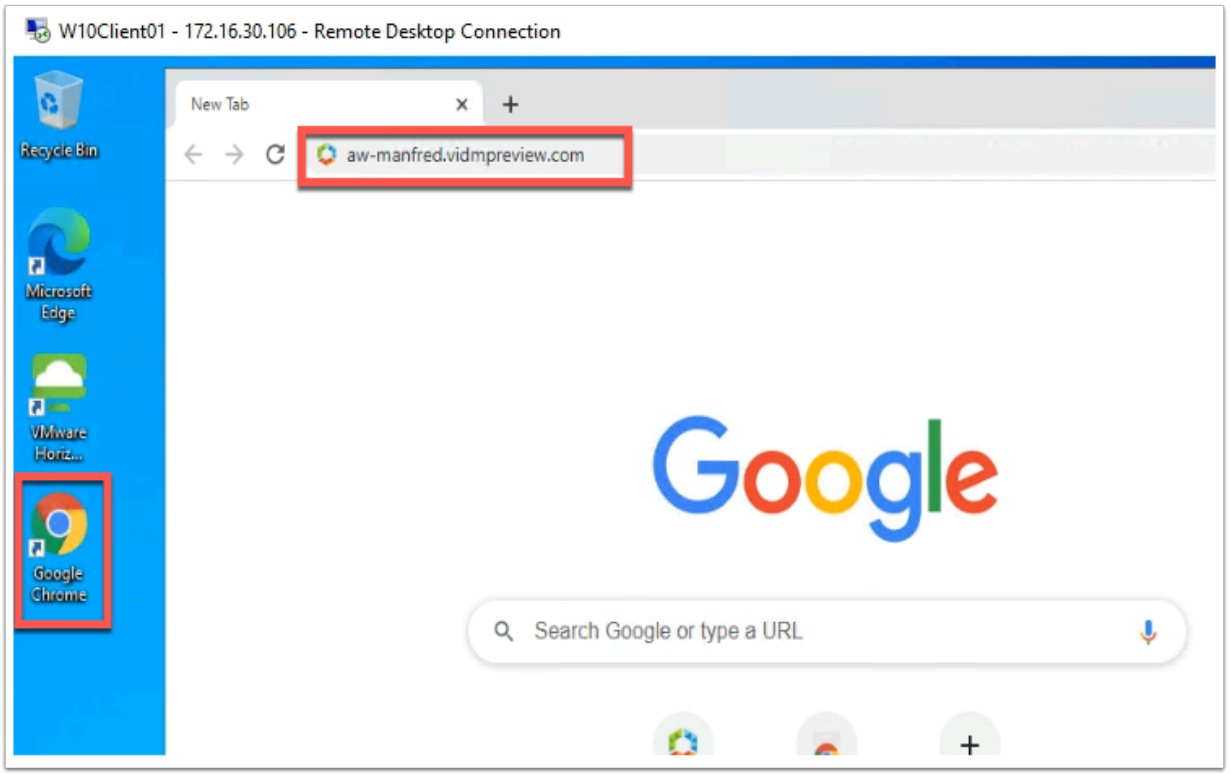


14. On the **Edit Policy \ Summary** page
    - Select **SAVE** .
        - You have now enabled Certificate (Cloud Deployment) as an authentication method on the default access policy.
        - Our next step is to ensure this implementation is working.

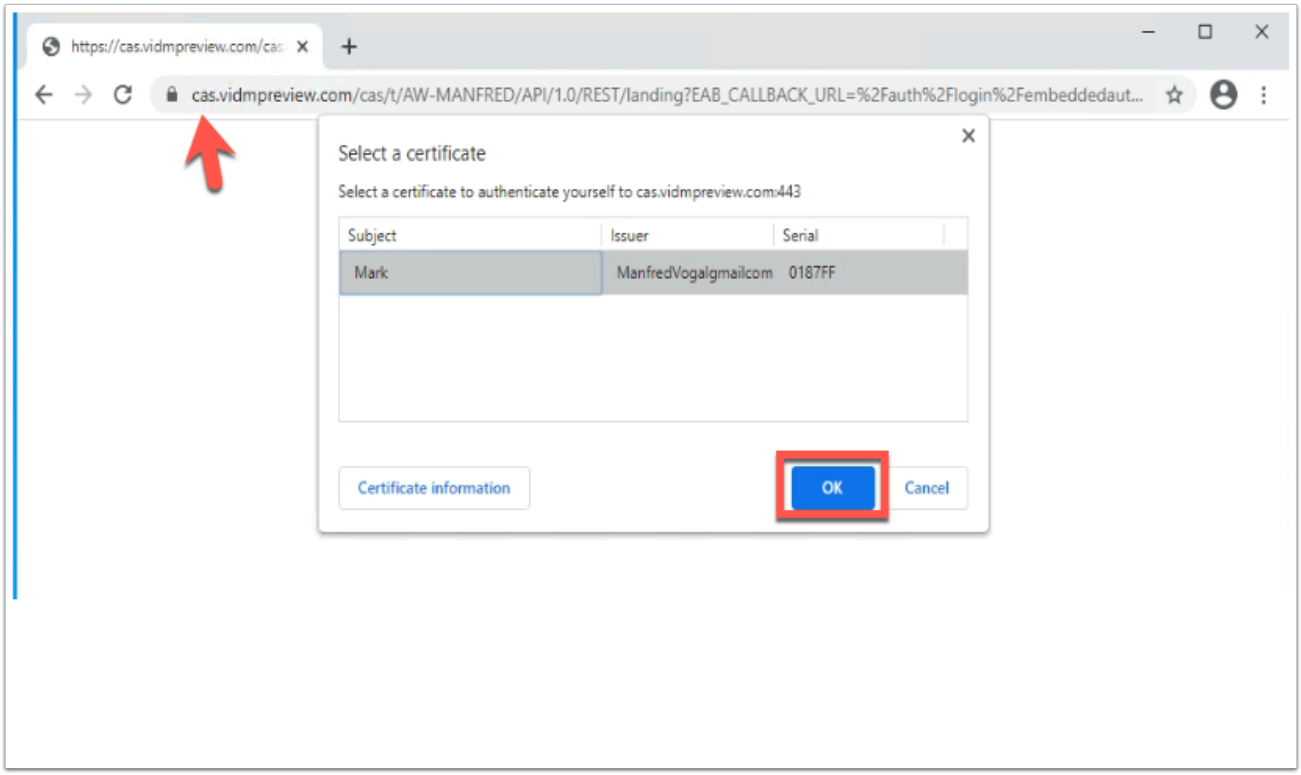
Part 3: Windows 10 Single Sign-On using Certificates



1. On the Desktop of **ControlCenter**
   - Open your **Remote Desktops** folder
   - RDP to your **Windows 10 Client (W10Client01.RDP)**
   - Authenticated using :
     - Username **euc-livefire\administrator**
     - Password **VMware1!**



2. On your **W10Client01**
   - Open the **Chrome Browser**
   - Navigate to Your unique **Workspace ONE Access Tenant**

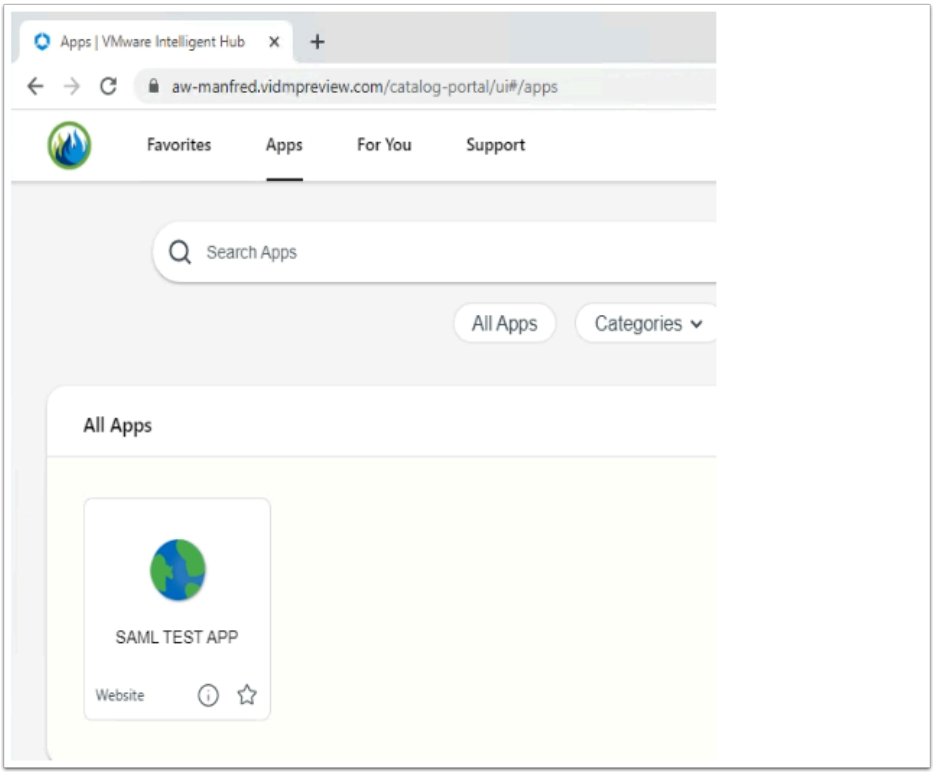


3. On your **W10Client01**

- You will within a second get a prompt from Chrome to confirm the use of the installed client certificate
- Notice the URL has **/cas** which is the certificate authentication service that will validate that certificate.

- Select **OK** to confirm the use of the certificate.

NOTE: If you do not see the Certificate pop-up window, instead you are directed to the normal Access authentication page. Go back to Part 1 in UEM and ensure the Certificate profile we have published has been installed on the device.



4. You should now be authenticated to the Intelligent Hub on the Chrome browser.

This concludes the Certificate-Based authentication lab, allowing users to authentication to corporate resources securely from a managed Windows 10 device.

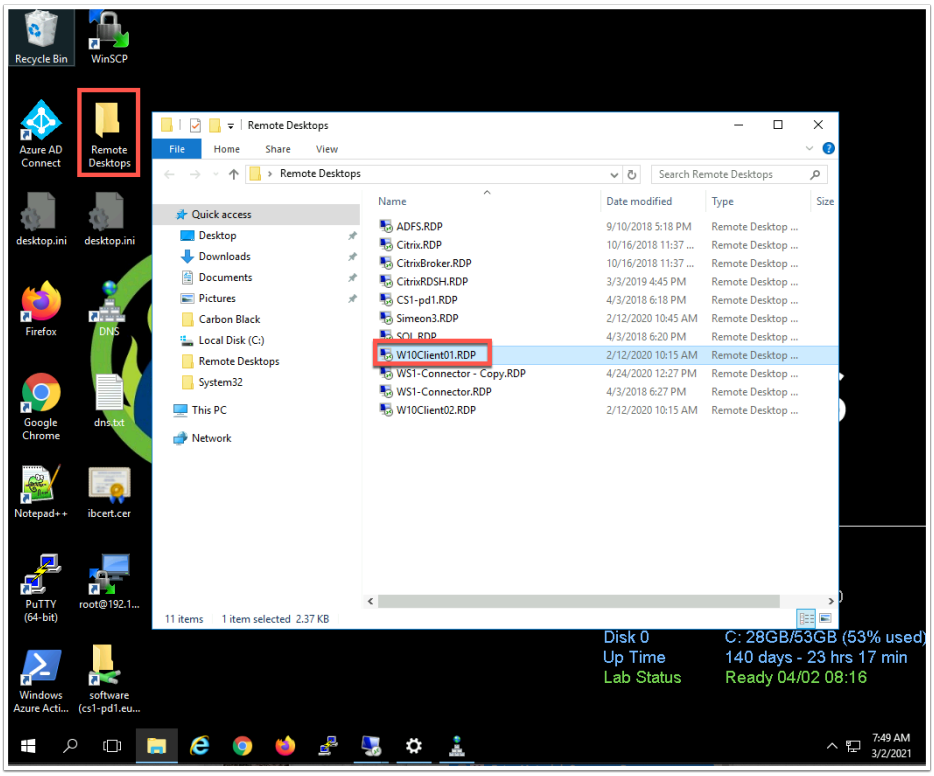
Extra Material: Suppress Pop-up on Chrome Part 1

In the flow above the user's experience is not ideal requiring the user to manually select the certificate from the prompt during authentication.

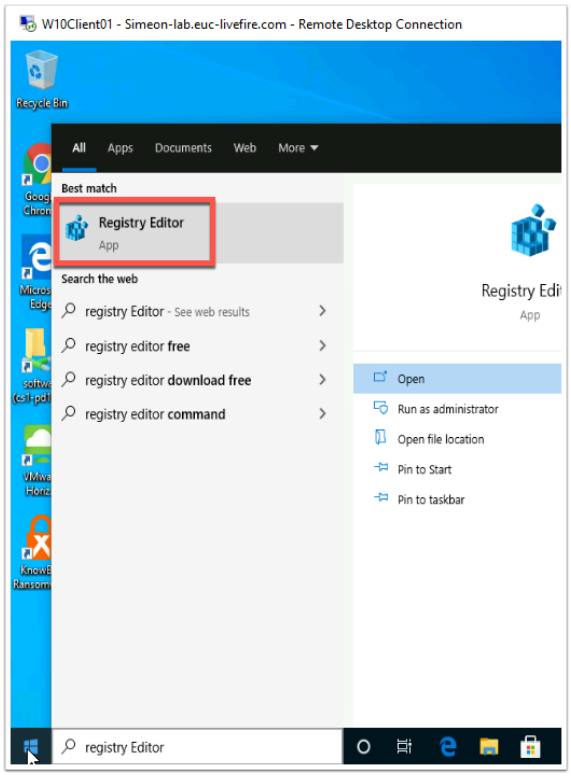
The various browsers handle the rules to auto-select certificates differently. In Chrome you can do this either through registry files or Chrome ADMX policies as per this article. https://www.chromium.org/administrators/policy-list-3#AutoSelectCertificateForUrls

In this lab we will show you both, first you will use the **registry option** and later we will use the **ADMP policy option** using UEM.

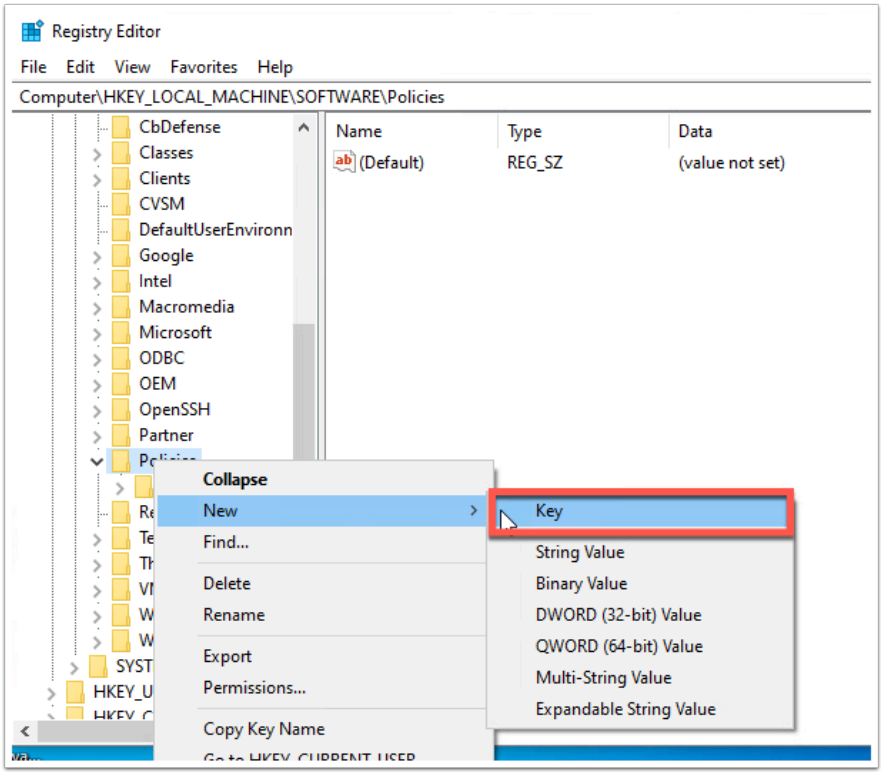
Alternatively you can download the Chrome Policy templates here: http://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip



1. On the **Controlcenter** base navigate to the **Remote Desktops** folder on the **desktop** and RDP to **W10Client01**

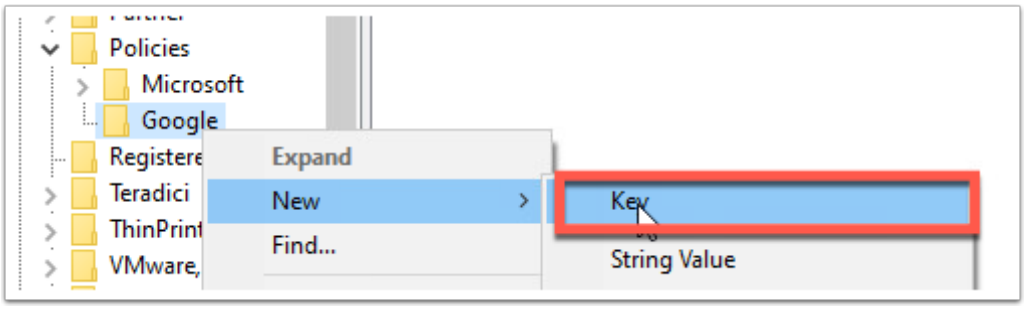


2. On the W10Client01 click **Start** and type **registry editory** and click on the **Registry Editor**

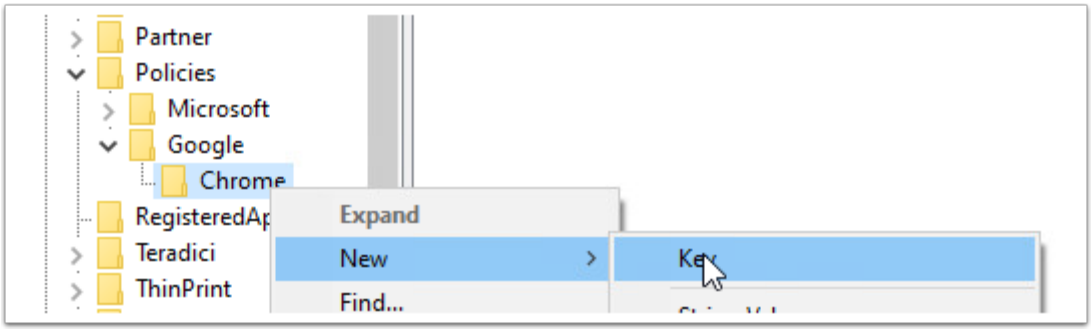


3. Navigate to **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies**

Right click **Policies** and click **New** > **Key**. Then Type **Google**.

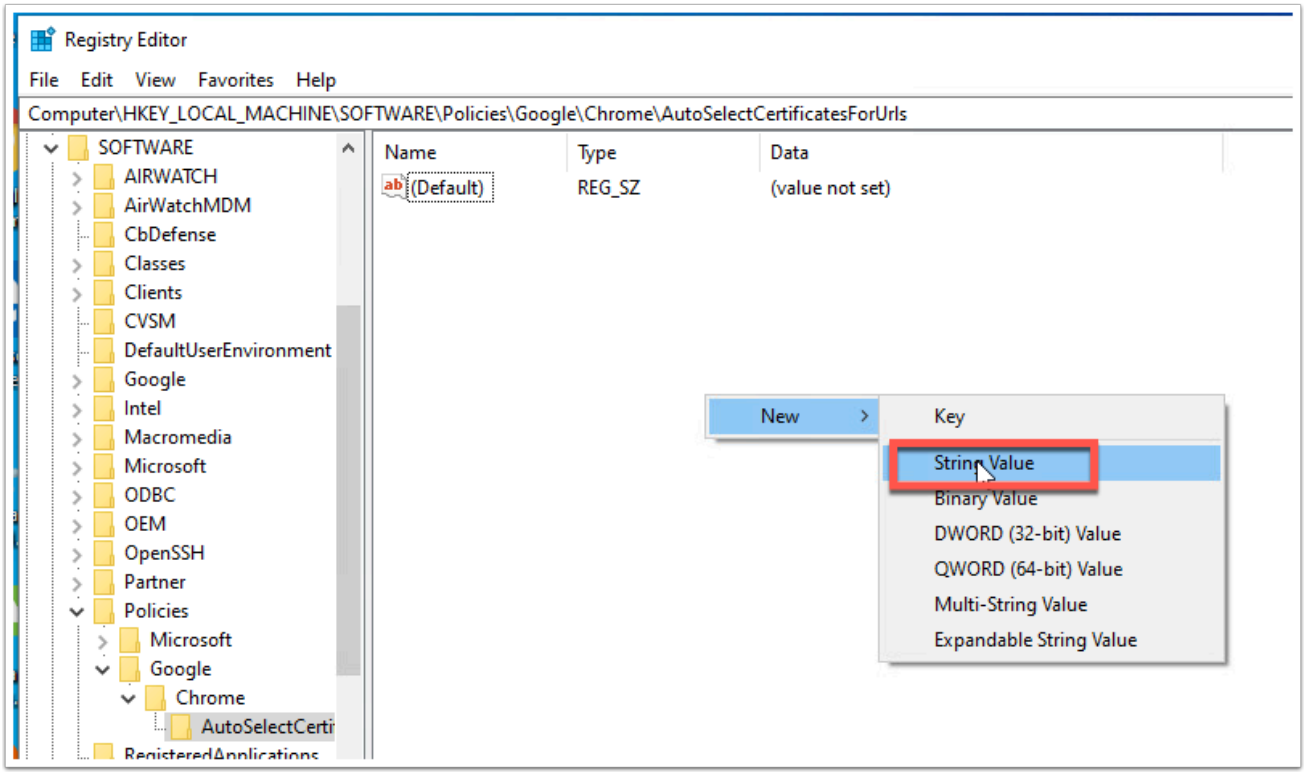


4. Right Click on the **Google** and click **New** > **Key.** Then type **Chrome**.

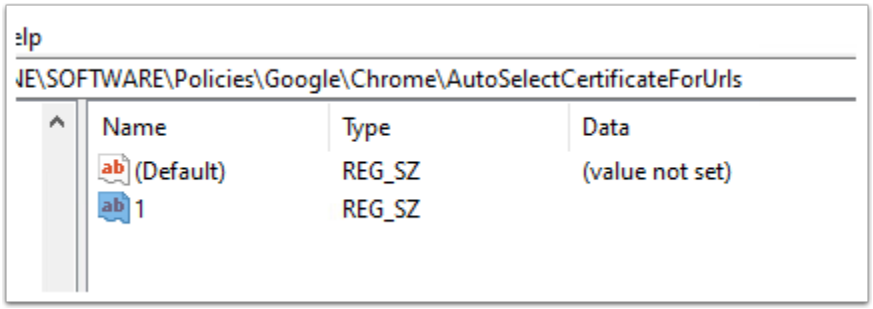


5. Right Click on **Chrome** and click **New** > **Key**. Then type **AutoSelectCertificateForUrls**

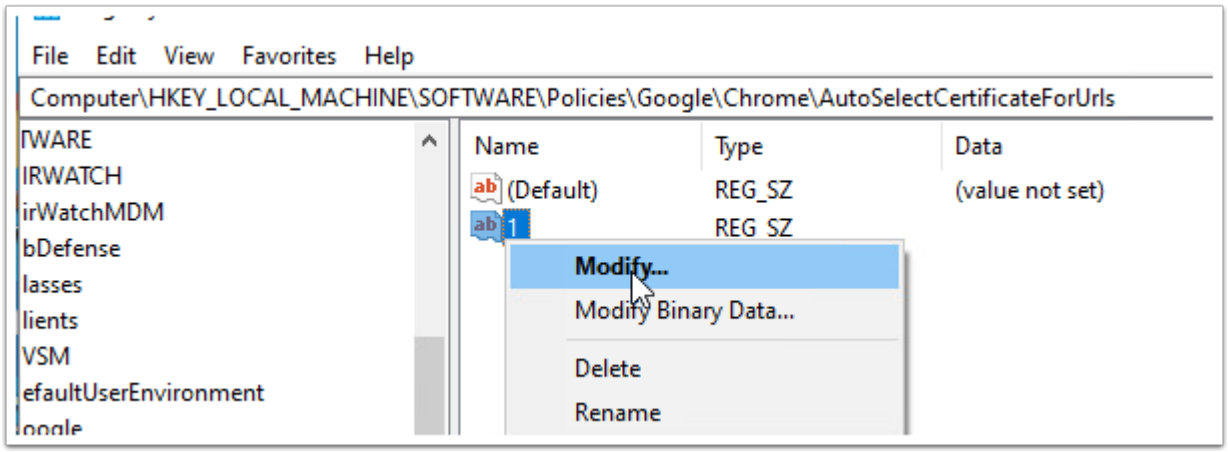
You should now have: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AutoSelectCertificateForUrls



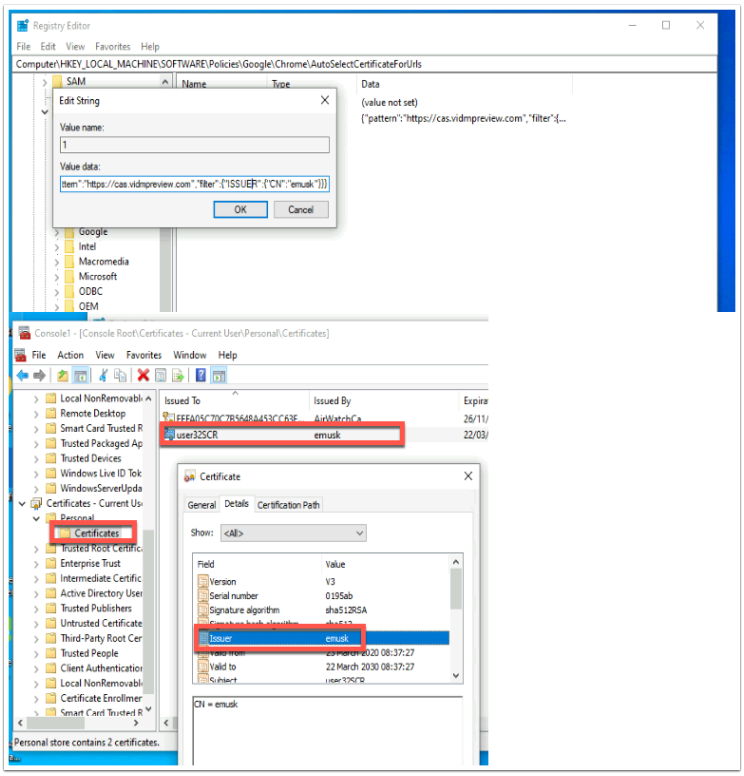
6. Right-Click in the white space inside the key **AutoSelectCertificateForUrls** and click **New** > **String Value**



7. Give the key the name **1**



8. Right-click on the **1** and click **Modify...**



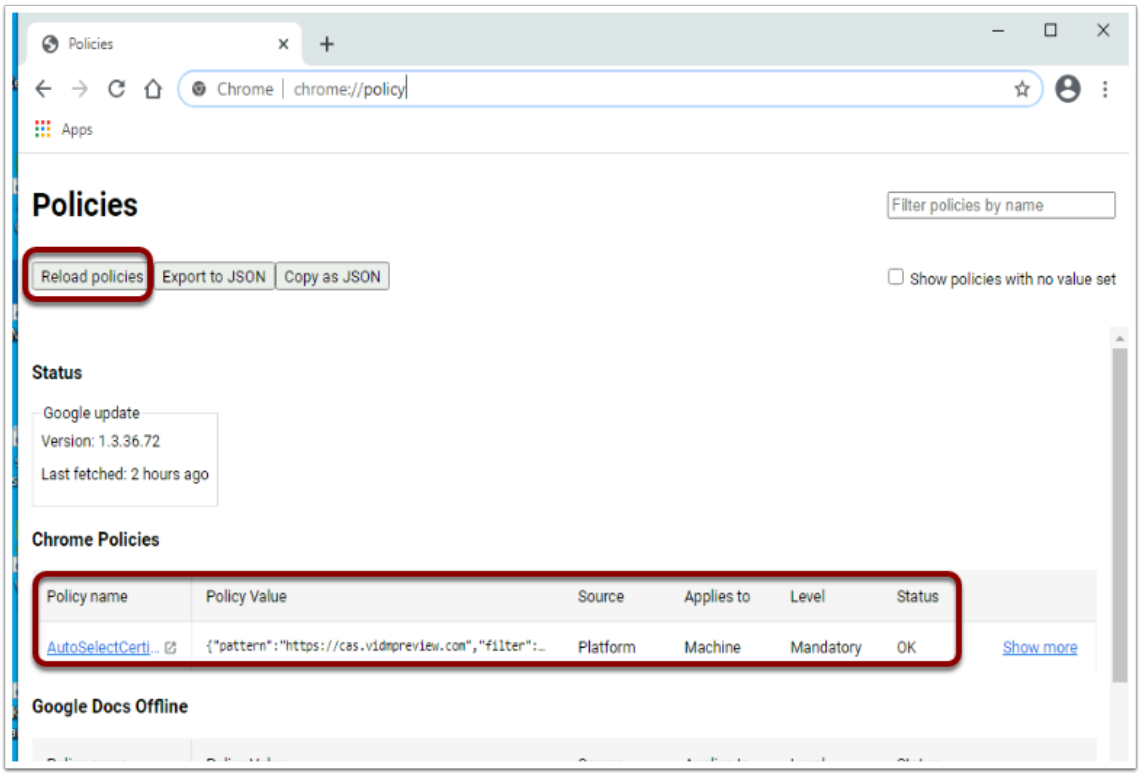
9. Fill in the Value data with the following replacing the highlighted text with the issuer value from your certificate. This is the certificate issuer name. When using **UEM certificates** this is the name of the Organization group from which the Certificate profile has been created.

{"pattern":"https://cas.vidmpreview.com","filter":{"ISSUER":{"CN":"emusk"}}}

Note: Some organizations may have multiple certificates issues by the same CA and will require more detail in that scenario reference link at the top of the lab

EXAMPE:

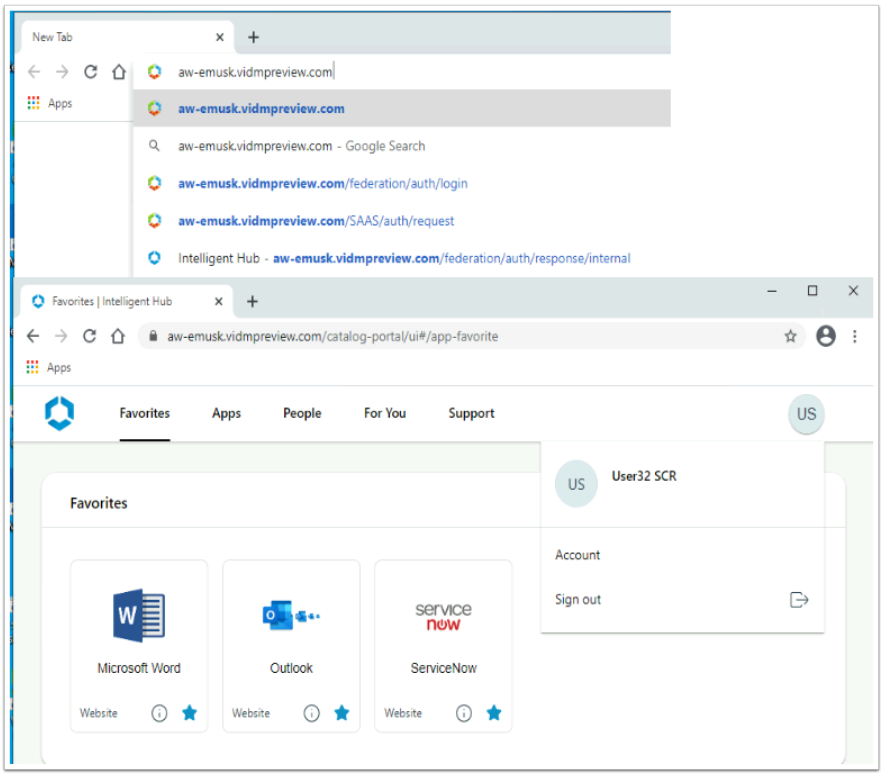
Software\Policies\Google\Chrome\AutoSelectCertificateForUrls\1 = "{"pattern":"https://www.example.com","filter":{"ISSUER":{"CN":"certificate issuer name", "L": "certificate issuer location", "O": "certificate issuer org", "OU": "certificate issuer org unit"}, "SUBJECT":{"CN":"certificate subject name", "L": "certificate subject location", "O": "certificate subject org", "OU": "certificate subject org unit"}}}"



10. Open **Chrome** on **W10Client01** and browse to **chrome://policy**

You should now notice that you have a Chrome Policy **AutoSelectCertificateForUrls**. This is a sanity check to make sure that the Registry entry has been successfully created.

NOTE: if you do not see the policy. Click **Reload policies** in the top left at which point you should see the policy appear.



11. In the navigation bar type the **Workspace ONE Access URL** and hit enter. You will be authenticated and land on the **Intelligent hub page.**

You will notice a in the URL a redirect to cas.vidmpreview.com at which point the certificate gets presented and validated, however the user is not prompted to select the certificate.

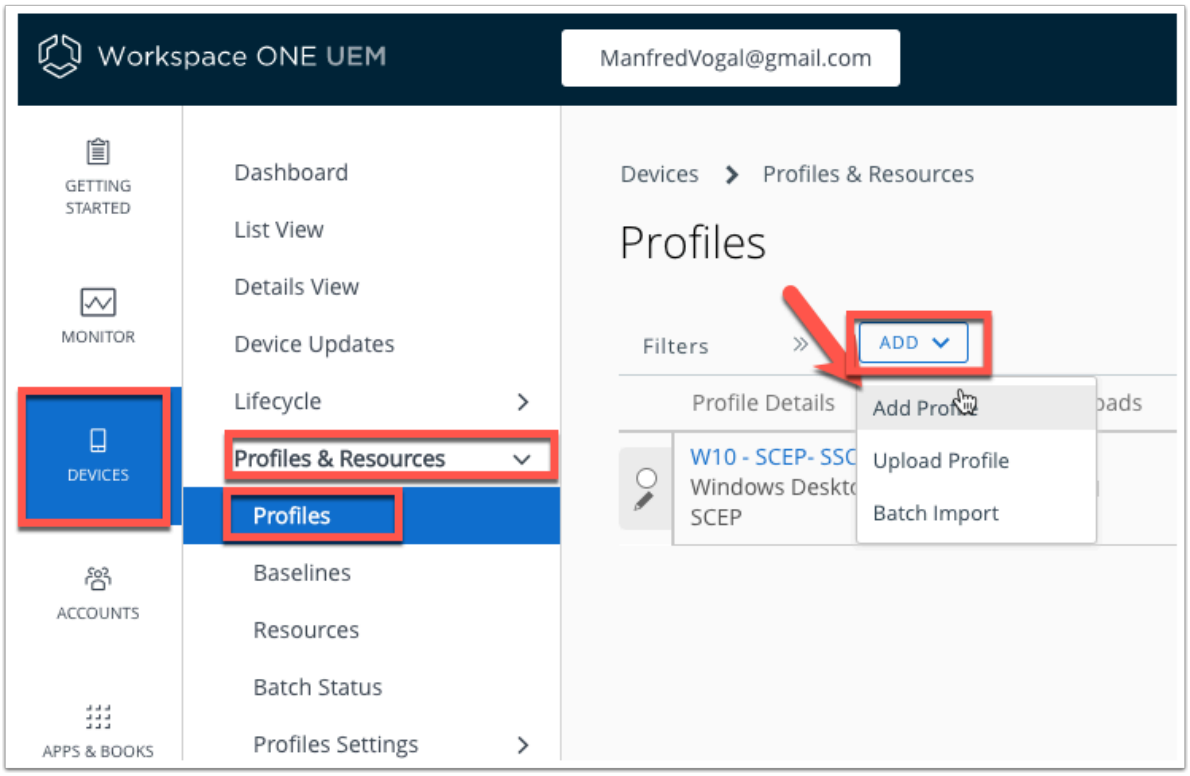
Extra Material: Suppress Pop-up on Chrome Part 2

In this part we will look at how we can automate the process so our entire fleet of Windows 10 managed devices will get the chrome policy to auto-select the appropriate certificate for SSO in the Chrome browser.

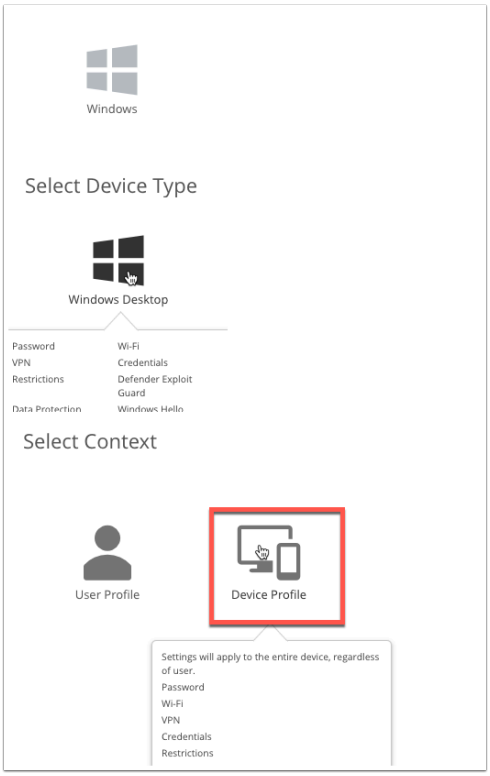
We again have two options to realize this. One is to use the above registry option. Export the registry, create a .bat file that installs the registry key and upload to UEM as Files/ Actions part of Product Provisioning.

The second option and the one we will use (just to change it up:) is to configure ADMX template using CSP. We can do this using custom profiles as described here: https://code.vmware.com/en/samples/3329/windows-10---chrome-admx#

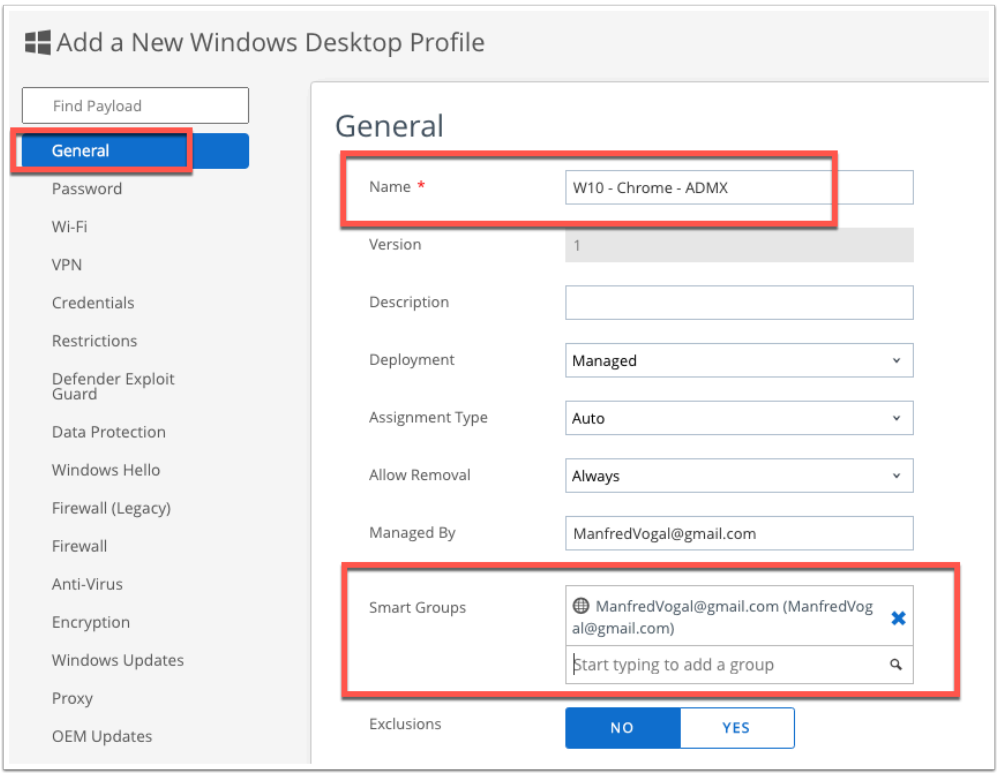
First we will deploy the ADMX policy as part of a custom profile, then we will create a policy that configures the "AutoSelectCertificateForURL"



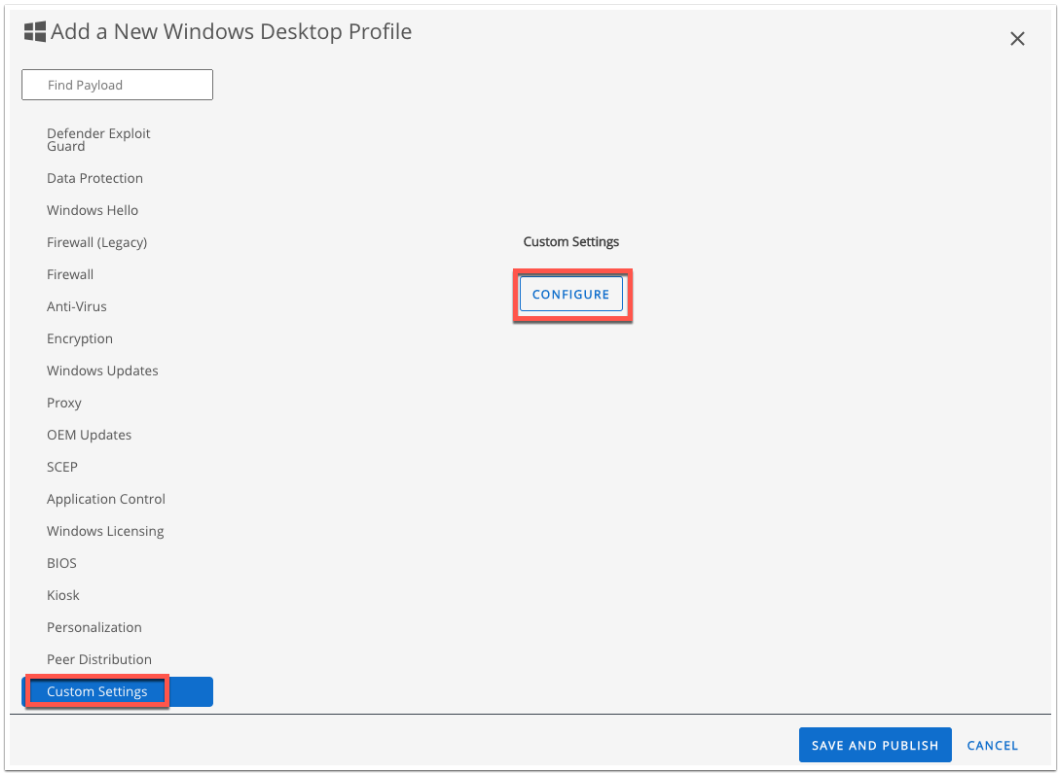
1. Open the **Workspace ONE UEM** admin console and navigate to **Devices** > **Profiles & Resources** > **Profiles** > **ADD** click **Add Profile**



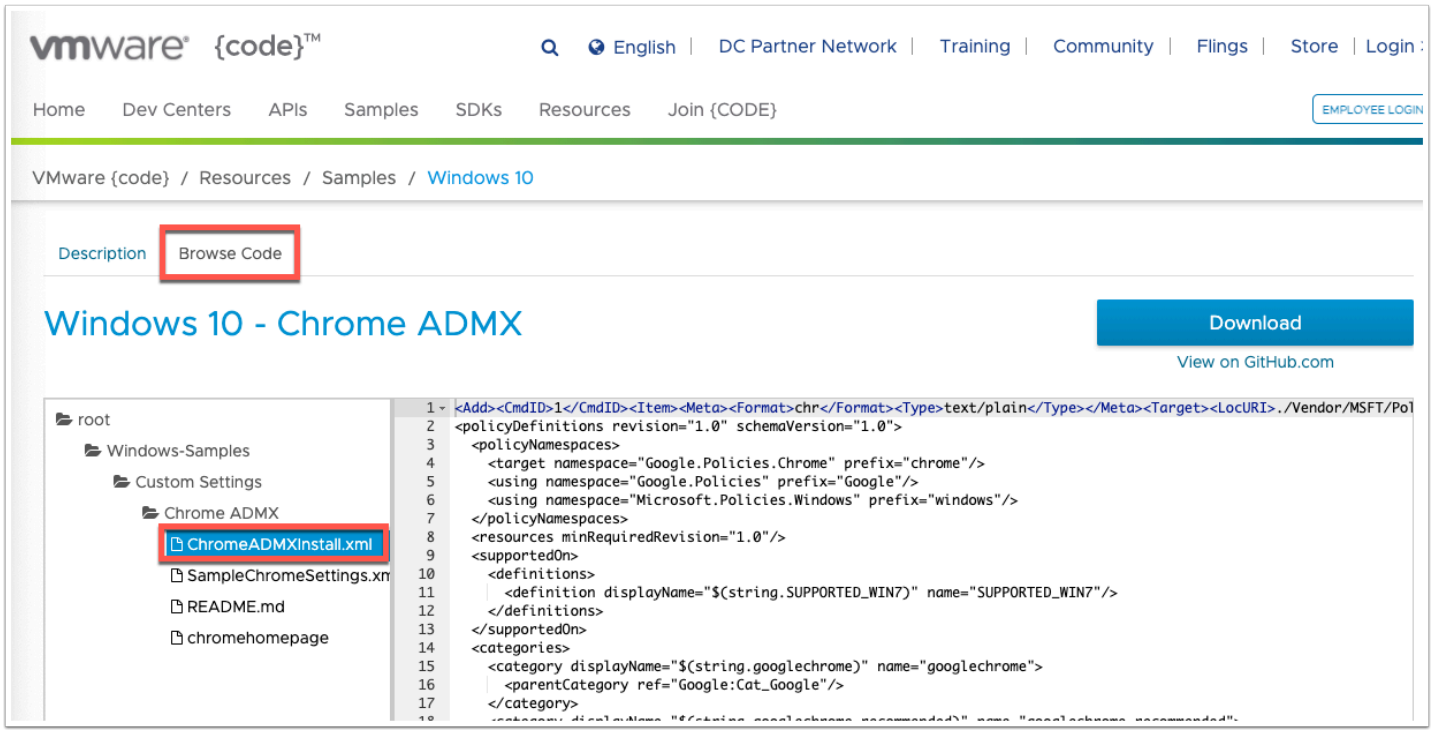
2. In the **Add Profile** window Select **Windows** > **Windows Desktop** and **Device Profile**



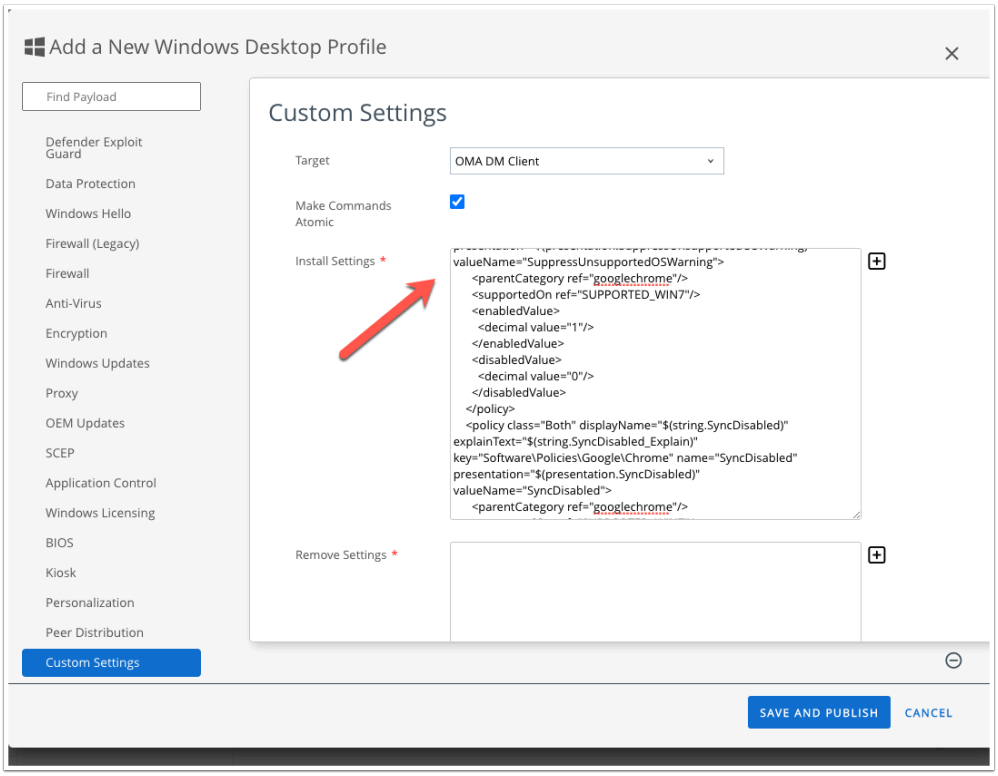
3. In the **General** payload fill in the following:
   - Name : **W10 - Chrome - ADMX**
   - Smart Groups - Select the World Icon for **your Organization Group** {should be you e-mail address}



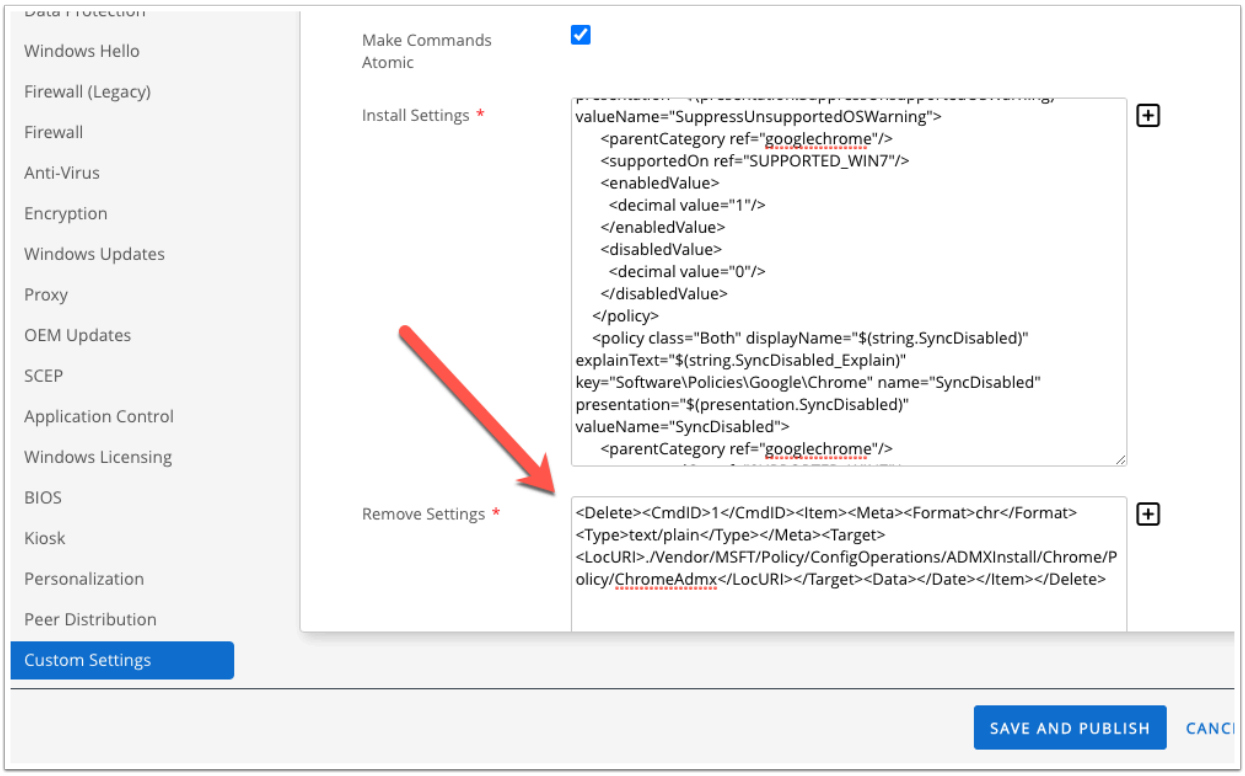
4. On the left find **Custom Settings** payload and click **CONFIGURE**



5. Open a **new tab** and navigate to https://code.vmware.com/en/samples/3329/windows-10---chrome-admx#code
   - Click on **Browse Code** and Drill down to the **ChromADMXinstall.xml**
   - **Copy** the entirety of the XML

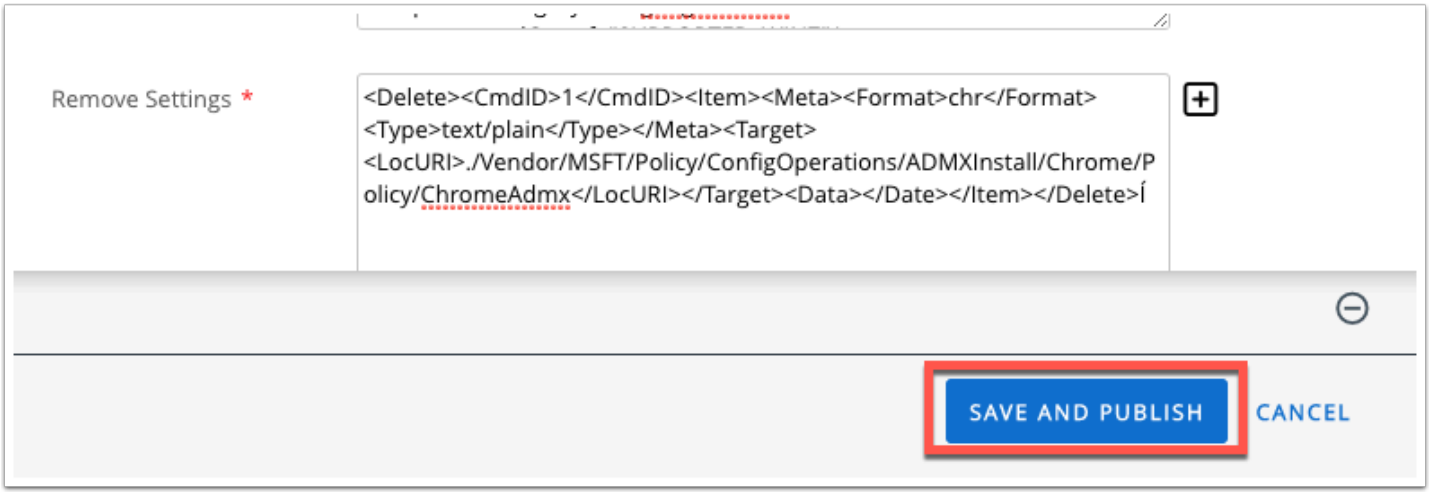


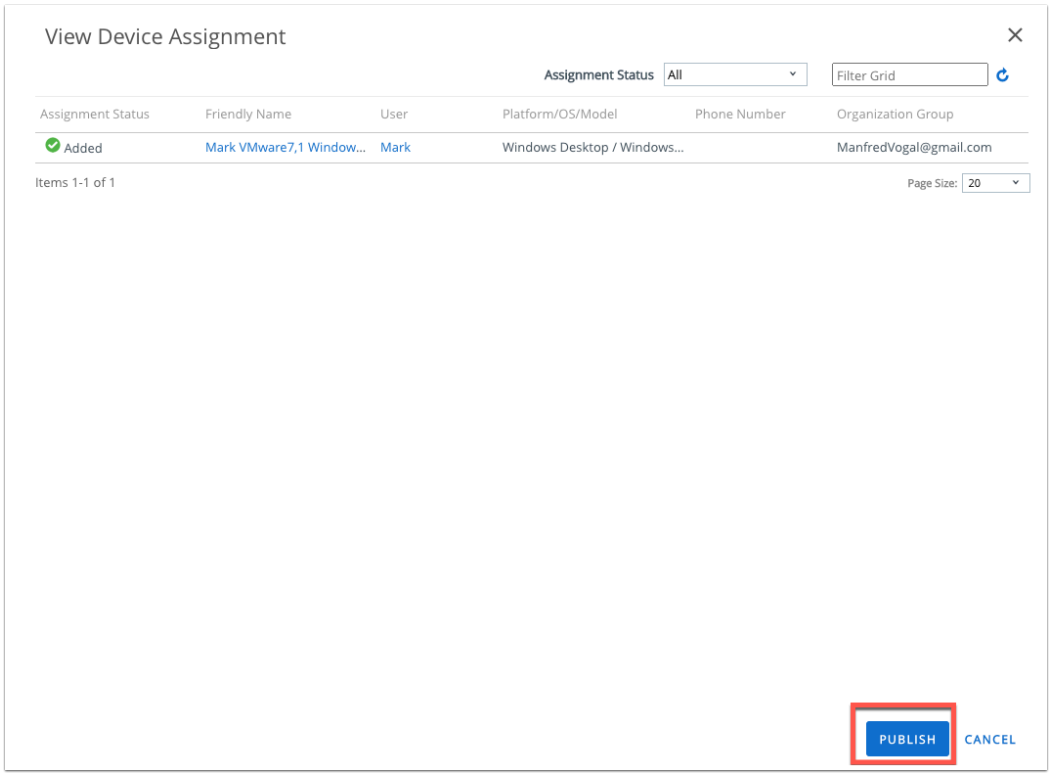
6. Navigate back to the **Workspace ONE UEM** Console and **paste** the XML into the **Install Settings** box of Custom Settings.



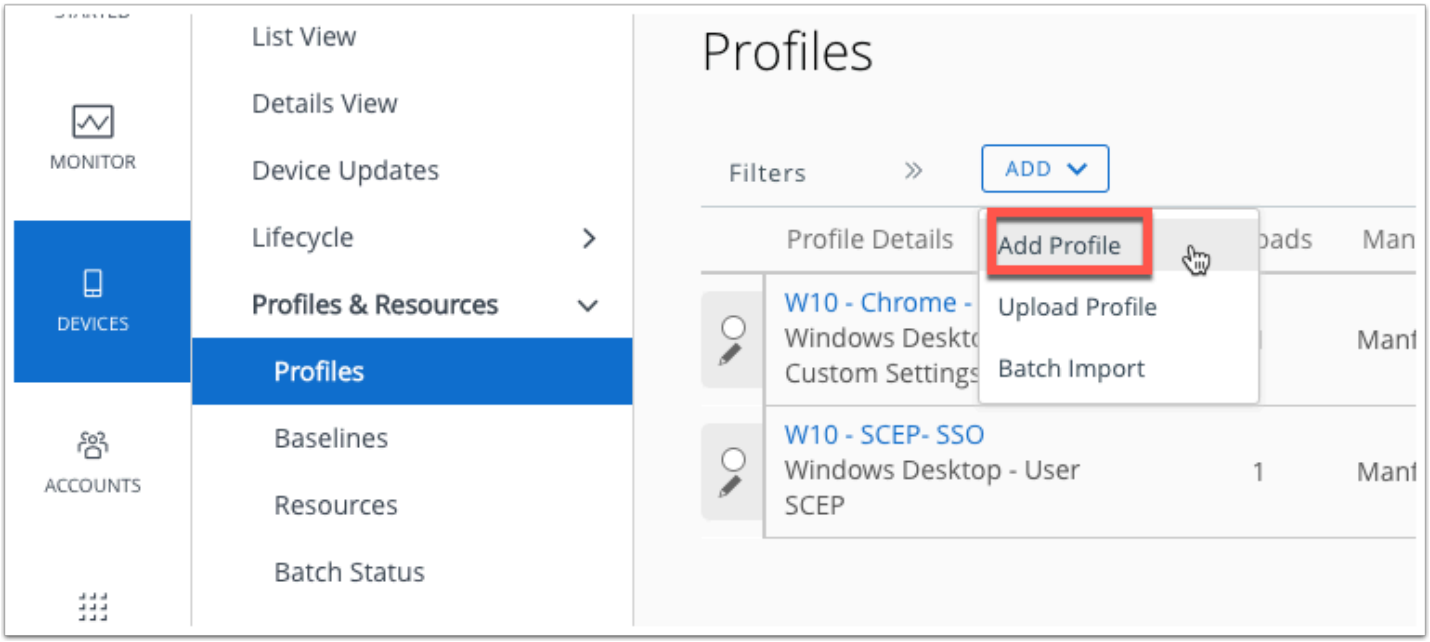
7. **Paste** the below XML into the **Remove Settings** box of the Custom Settings payload.

```
<Delete><CmdID>1</CmdID><Item><Meta><Format>chr</Format><Type>text/
plain</Type></Meta><Target><LocURI>./Vendor/MSFT/Policy/ConfigOperations/
ADMXInstall/Chrome/Policy/
ChromeAdmx</LocURI></Target><Data></Date></Item></Delete>
```

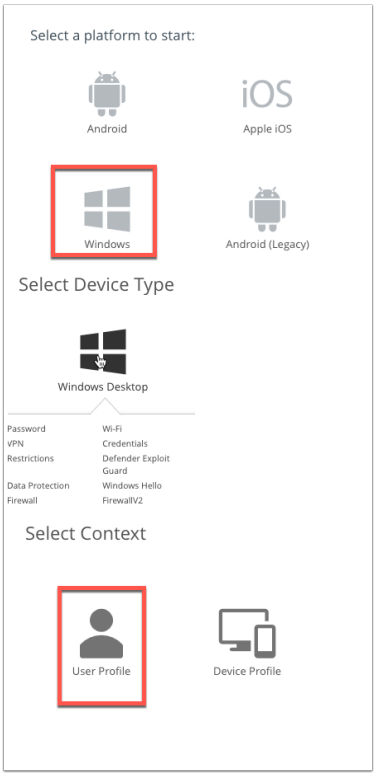




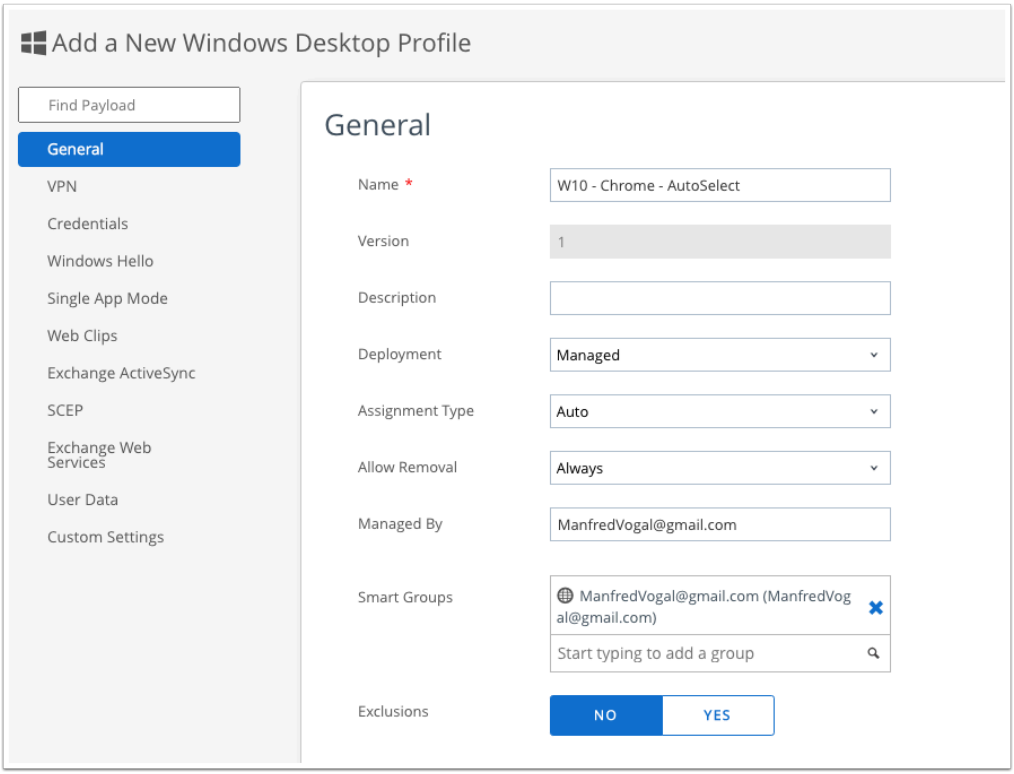
8. Click **SAVE AND PUBLISH** and **PUBLISH** on the View Device Assignment window.



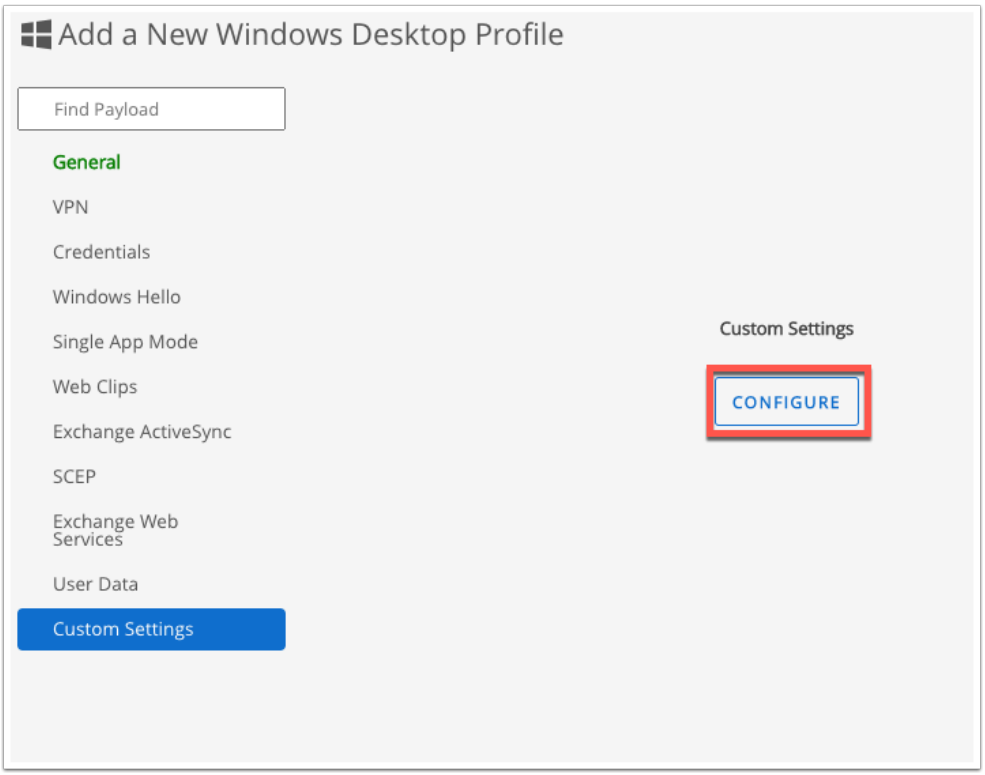
9. Click **ADD** and **Add Profile** in the **Profiles** page.



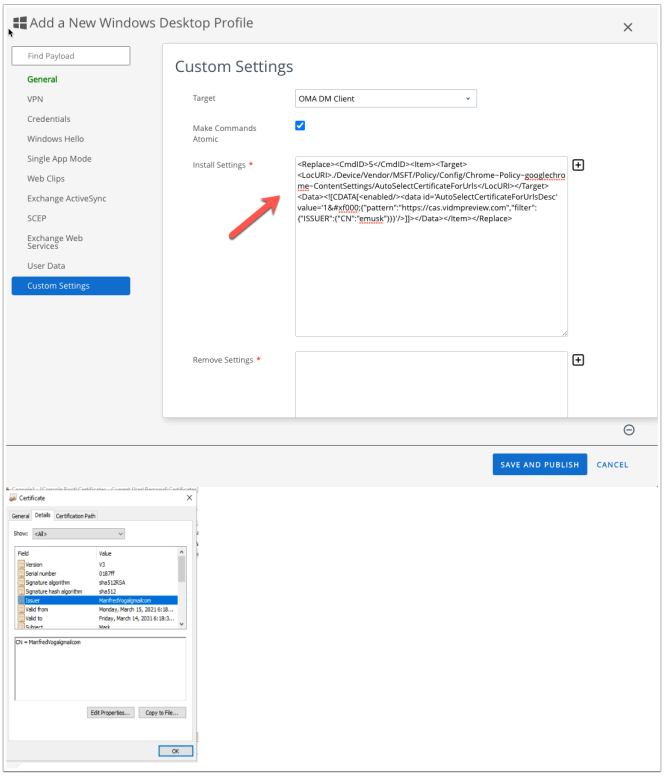
10. Select **Windows** > **Windows Desktop** > **User Profile**



11. In the General payload set the following:
    - Name: **W10 - Chrome - AutoSelect**
    - Smart Groups: Select the World Icon for **your Organization Group** {should be you e-mail address}

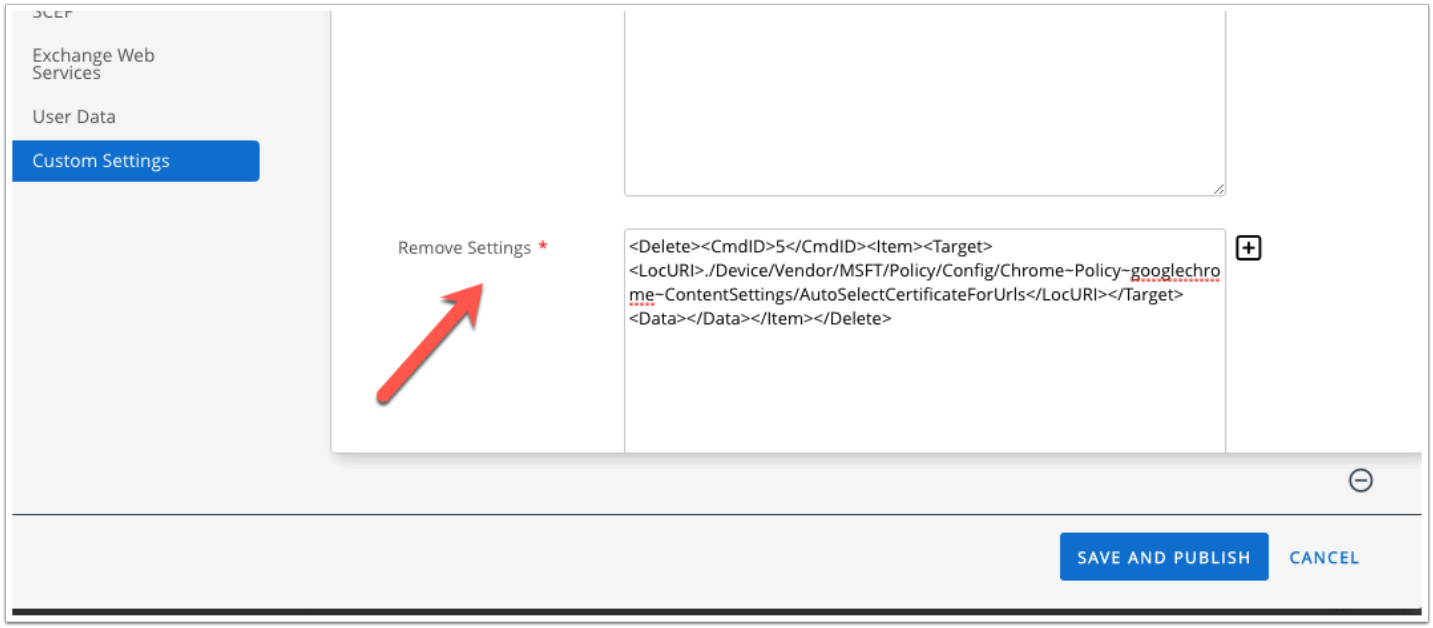


12. Go to the **Custom Settings** payload and click **CONFIGURE**



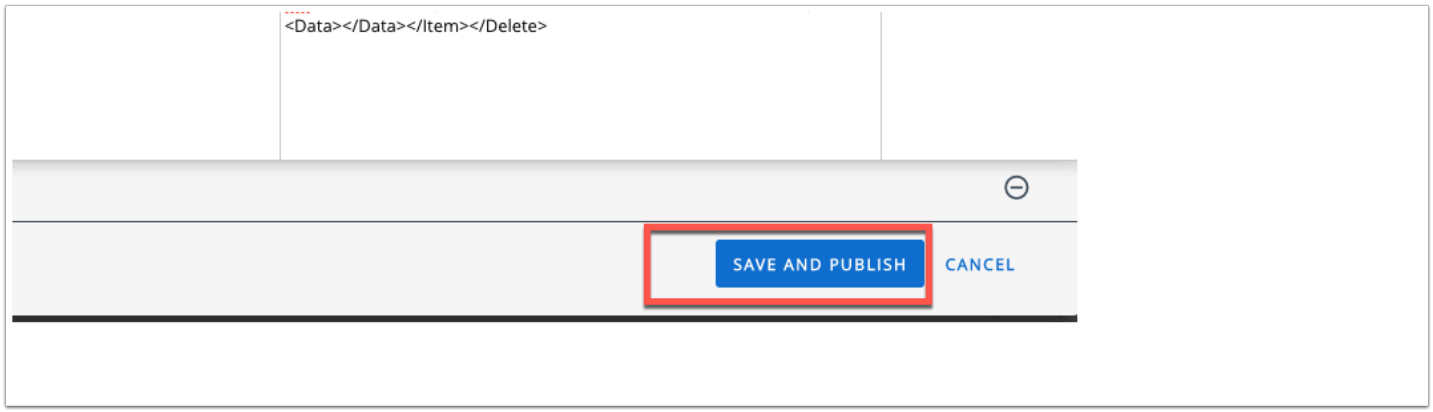
12. **Paste** the following XML into the **Install Setting**s section of **Custom Settings**. Replacing the **CN value** (Highlighted) with your **OrganisationGroup** name without punctuation. (Eg. ManfredVogalgmailcom) This is the **Issuer value** if you would like to double check on you W10Client01 certificate.

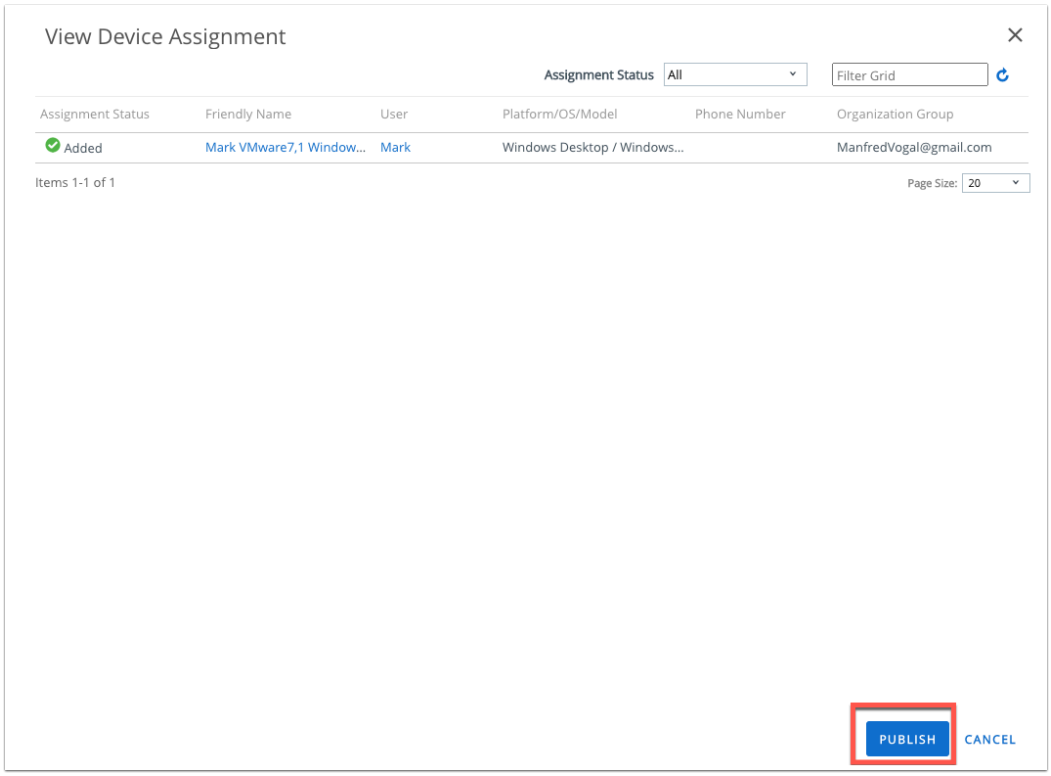
<Replace><CmdID>5</CmdID><Item><Target><LocURI>./Device/Vendor/MSFT/Policy/Config/Chrome~Policy~googlechrome~ContentSettings/AutoSelectCertificateForUrls</LocURI></Target><Data><![CDATA[<enabled/><data id='AutoSelectCertificateForUrlsDesc' value='1{"pattern":"https://cas.vidmpreview.com","filter":{"ISSUER":{"C



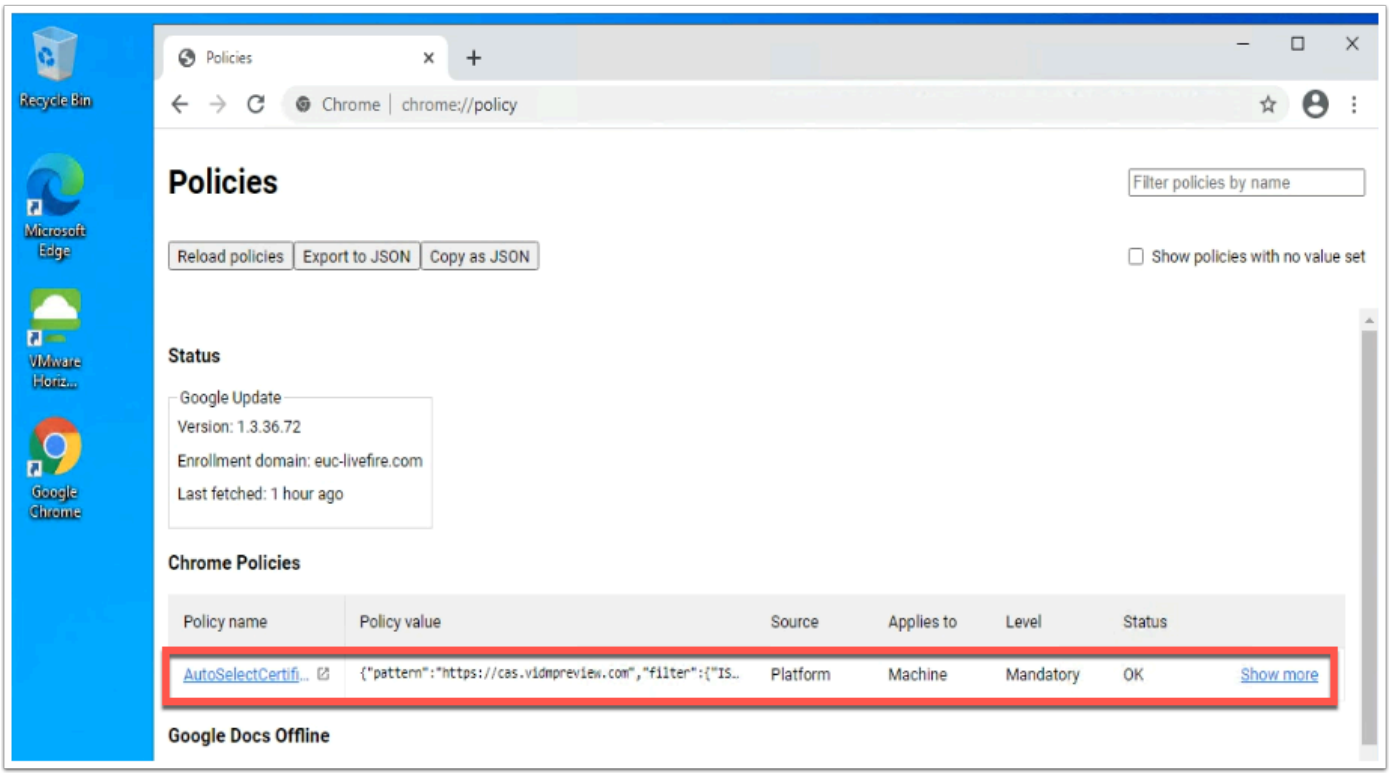
13. **Paste** the following XML into the Remove Settings section of the Custom Settings.

<Delete><CmdID>5</CmdID><Item><Target><LocURI>./Device/Vendor/MSFT/Policy/Config/Chrome~Policy~googlechrome~ContentSettings/AutoSelectCertificateForUrls</LocURI></Target><Data></Data></Item></Delete>





14. Click **SAVE AND PUBLISH** and **PUBLISH** on the View Device Assignment window.



15. On the **W10Client01** VM close **Chrome** and Re-open it. **Navigate** to Chrome://policy you should see the AutoSelectCertificate policy there. Navigate to your unique WorkspaceONE Access URL you should not be prompted for a certificate but it should be a seemless single-sign-on experience.

This concludes the Certificate-Based Authentication on Windows 10 and the configuration of the end-points to auto-select the appropriate certificate for single-sign on.

Author: Simeon Frank