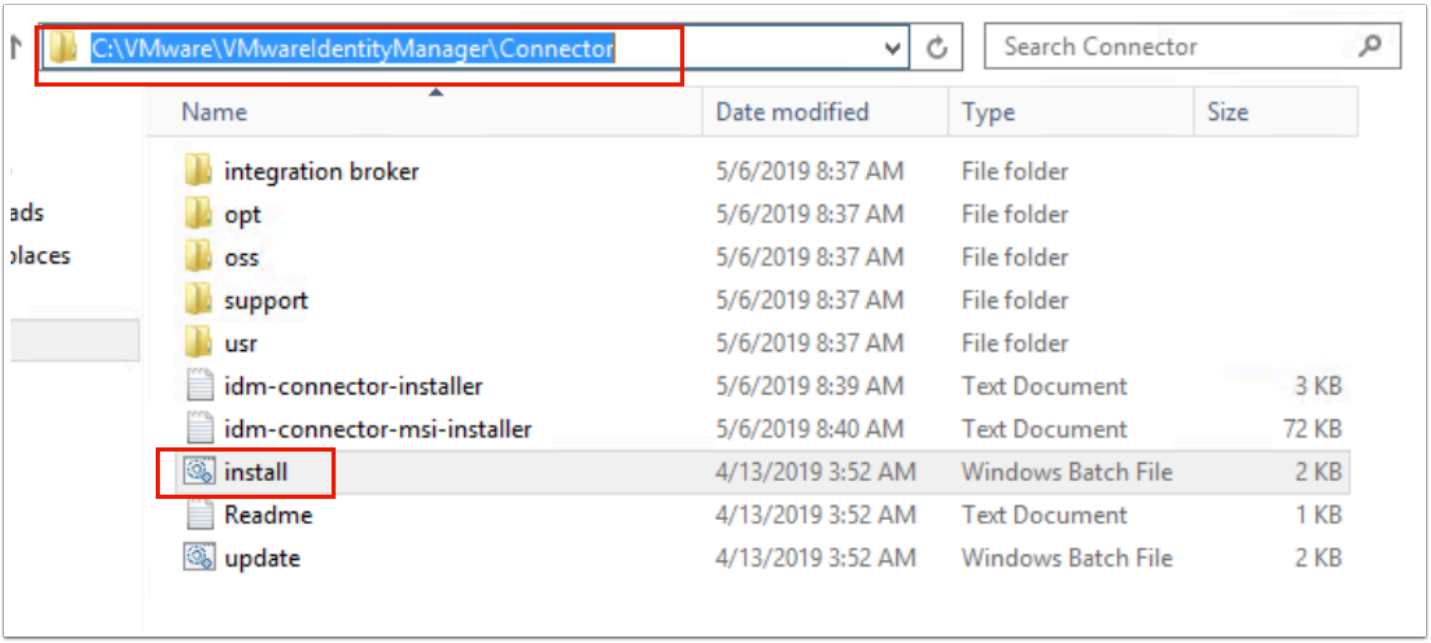
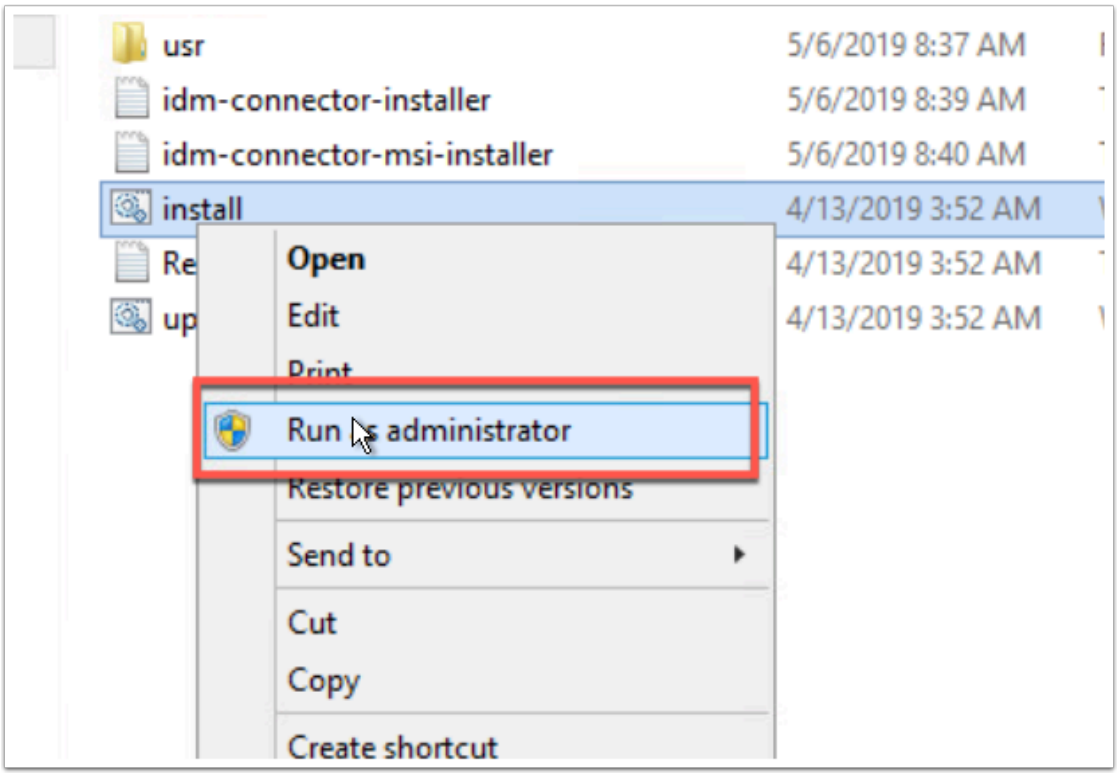
Configuring the Workspace ONE Access Connector

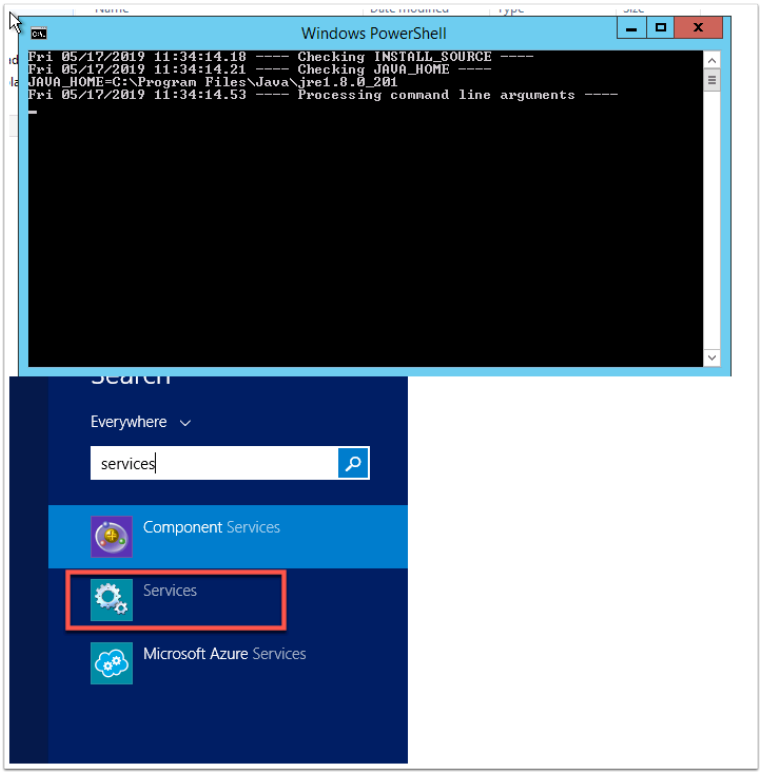
Part 1. Configuring the Workspace ONE Access Connector

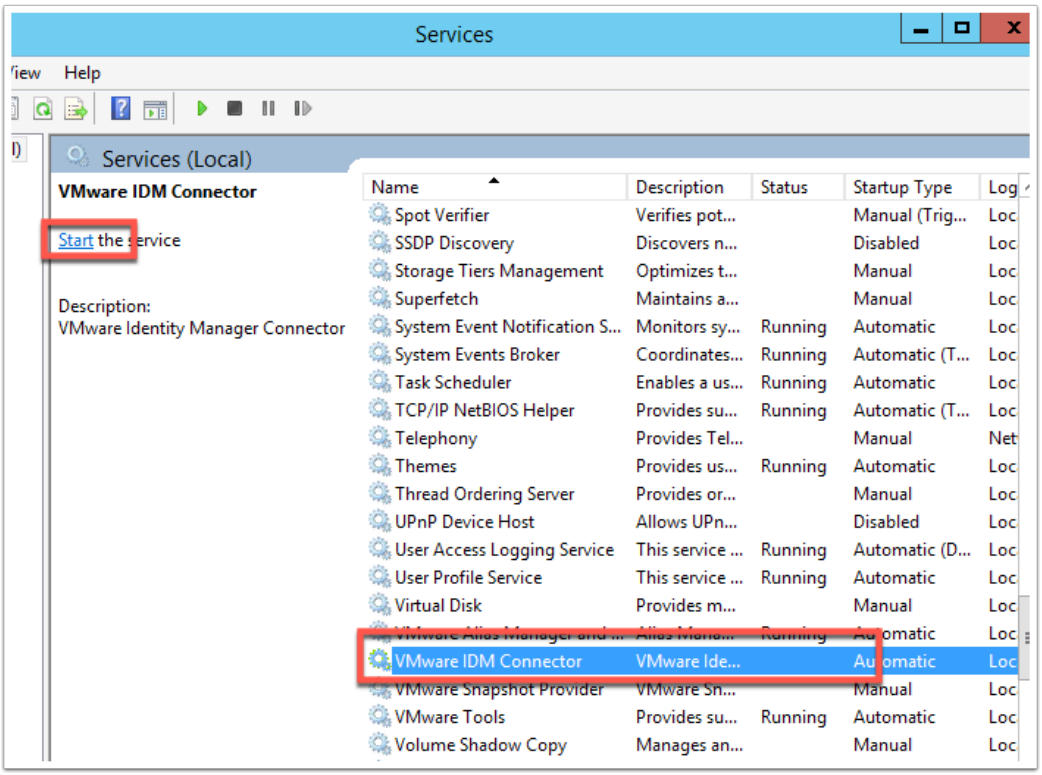
1. We have pre-installed the Workspace ONE Access Connector for you in the Lab environment. However since we have cloned the machine the connector is in an idle state and needs to be re-initiated.

- Log into your ControlCenter2 server with username **administrator@euc-livefire.com** and password **VMware1!**
  1. On your **ControlCenter2** server desktop select your **Remote Desktops** folder and select and launch your **WS1-Connector.RDP** shortcut.
  2. When prompted log in as username **administrator@euc-livefire.com** with the password **VMware1!**
  3. On the **WS1-Connector** server open the **File Explorer** to the following path **C:\VMware\VMwareidentityManager\Connector**
  4. Right Click the **install.bat** file and click **Run as Administrator**
  5. This will launch a PowerShell window that will clear out the state of the connector. Wait till the Powershell Window closes which confirms it has run successfully.
  6. Open **services.msc** and **start** the **VMware IDM Connector** service
  7. Wait for a few minutes till all the services have launched and move on to the next part of the lab.



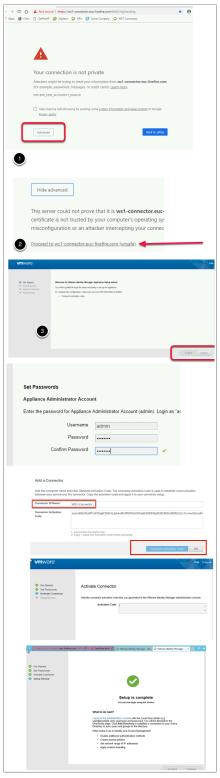

usr
5/6/2019 8:37 AM
idm-connector-installer
5/6/2019 8:39 AM
idm-connector-msi-installer
5/6/2019 8:40 AM
install
4/13/2019 3:52 AM
Re
4/13/2019 3:52 AM
up
4/13/2019 3:52 AM
Open
Edit
Print
Run as administrator
Restore previous versions
Send to
Cut
Copy
Create shortcut


Windows PowerShell
Fri 05/17/2019 11:34:14.18 ---- Checking INSTALL_SOURCE ----
Fri 05/17/2019 11:34:14.21 ---- Checking JAVA_HOME ----
JAVA_HOME=C:\Program Files\Java\jre1.8.0_201
Fri 05/17/2019 11:34:14.53 ---- Processing command line arguments ----
Everywhere
services
Component Services
Services
Microsoft Azure Services



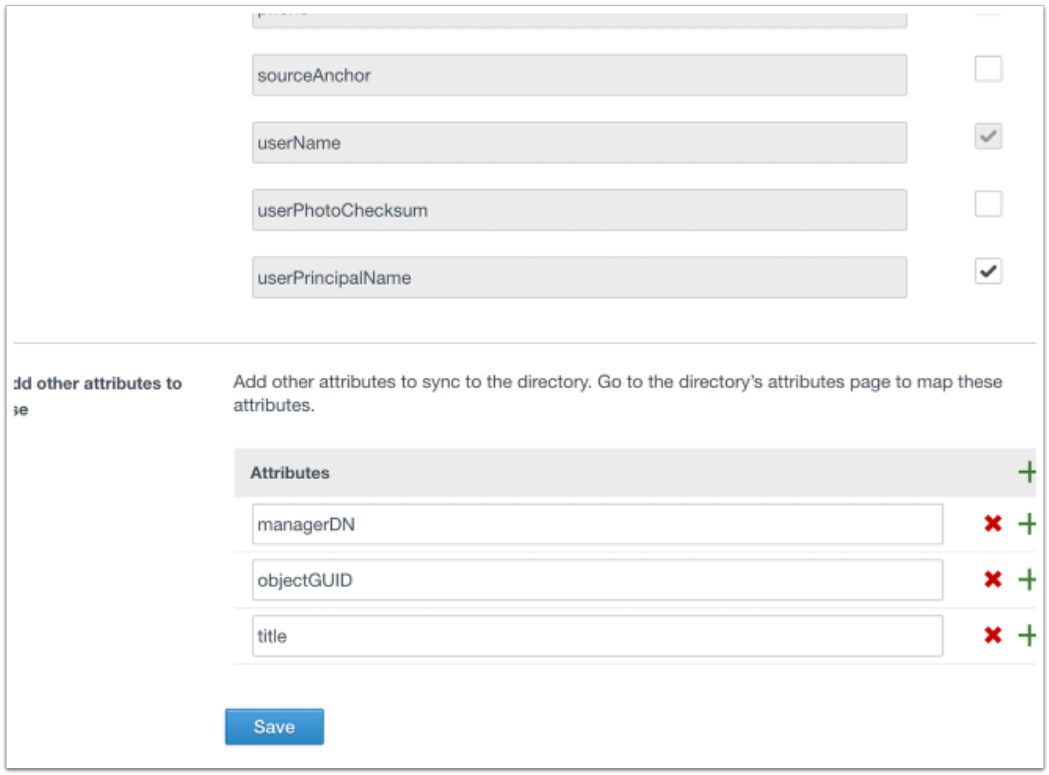
1. Our objective is to associate our on-premise connector instance with our SaaS instance of Workspace ONE Access.

- Log on to your **Control Center2** server in your Lab use your **Google Chrome browser**.
  1. On your chrome select the **WS1-connnector** shortcut or type **https://ws1-connector.euc-livefire.com:8443/cfg in the address bar**
  2. On the Your Connection is not private page, select **Advanced** and select **Proceed to ws1-connector.euc-livefire.comue.**
  3. On the **Get Started** Window select **Continue**
  4. In the **Set Passwords** section next to **Username** type **admin** next to **password** type **VMware1!** next to **Confirm Password** type **VMware1!** select **Continue** at the bottom of the page.
  5. On your browser, open up a **second Tab**, navigate to your unique **Workspace ONE Access Tenant** and if you have not done so login as **Administrator** with your **unique password**, that your received in your e-mail login
  6. Navigate to **Identity & Access Management** > **Setup** > **Connectors** Select **Add Connector**
  7. Next to **Connector ID Name:** type **WS1-Connector.** Next select **Generate Activation Code** . Next **copy** this code
  8. **Revert back** to your **WS1-Connector Server** setup: On the **activate connector page** **Paste** this code into the **Activation Code** box of your **Connector configuration** setup, select **Continue**
  9. You should get a **setup is complete** page inside the Workspace ONE Access Console.



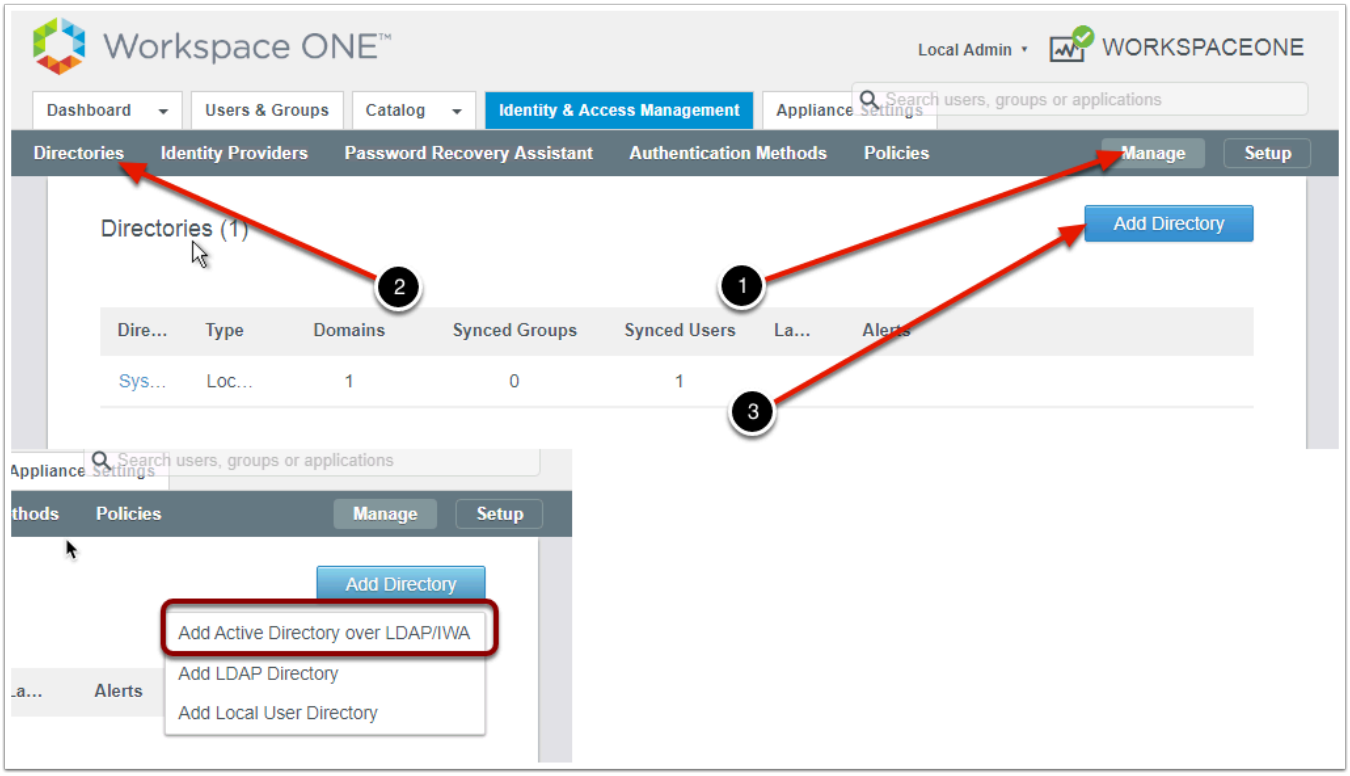
2. We will now configure and synchronise Active Directory to the Workspace ONE Access server using the external connector.

- First we will configure the Attributes. Note! Every organisation will need to research their requirements when deciding whether or not to set attributes to **required.** For specific applications where this needs to be considered, if the associated user object does not have the attribute, authentication might fail.
  1. Navigate to **Identity & Access Management** > **Setup** > **User Attributes**
     Notice the attributes that are available and the option available to set these to **Required**.
     IMPORTANT NOTE: The attributes set to required **cannot** be changed after a directory sync has taken place.
  2. Set the attribute **distinguishedName** and **userPrincipalName** to Required
  3. Under Attributes to the right select the **Green Plus** (+) Add the following additional attributes (case sensitive) :
     - **objectGUID**
     - **title**
     - **managerDN**
  4. Select **Save**



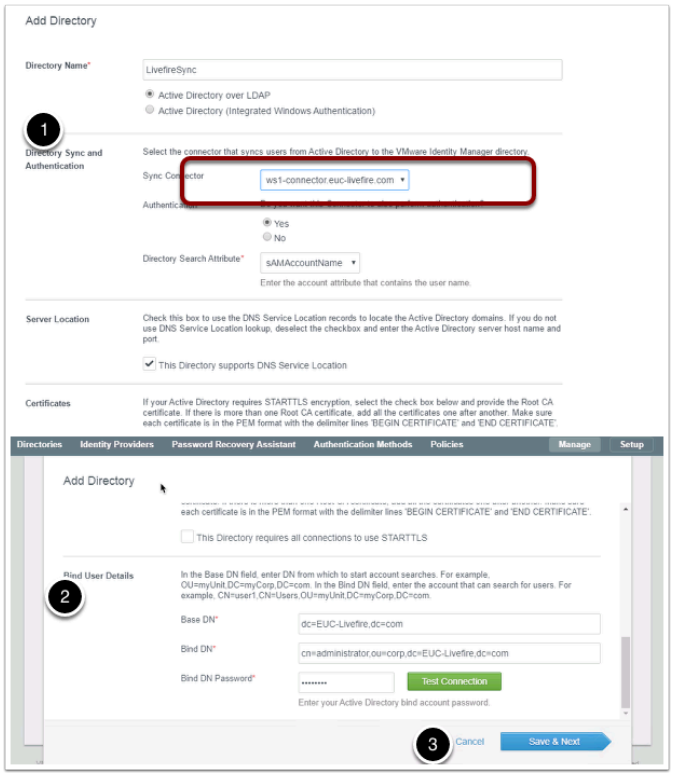
3. Configure our AD-sync configuration with Workspace ONE Access.

1. To the right of the screen select **Manage**, select **Directories**
2. Select **Add Directory** > **Add Active Directory over LDAP/IWA**



4. Configure our AD-sync configuration with Workspace ONE Access....continued

- In **Add Directory** Page, configure the following
  1. **Directory Name: LivefireSync**
  2. Ensure the **Active Directory over LDAP radio button** is selected
  3. The **Sync Connector** select the external connector **ws1-connector.euc-livefire.com**
  4. **Directory Search Attribute**: **sAMAccountName**
  5. **Base DN: dc=EUC-Livefire,dc=com**
  6. **Bind DN: cn=administrator,ou=corp,dc=EUC-Livefire,dc=com**
  7. **Bind DN Password: VMware1!**
  8. Select Test Connection
  9. Select **Save & Next**



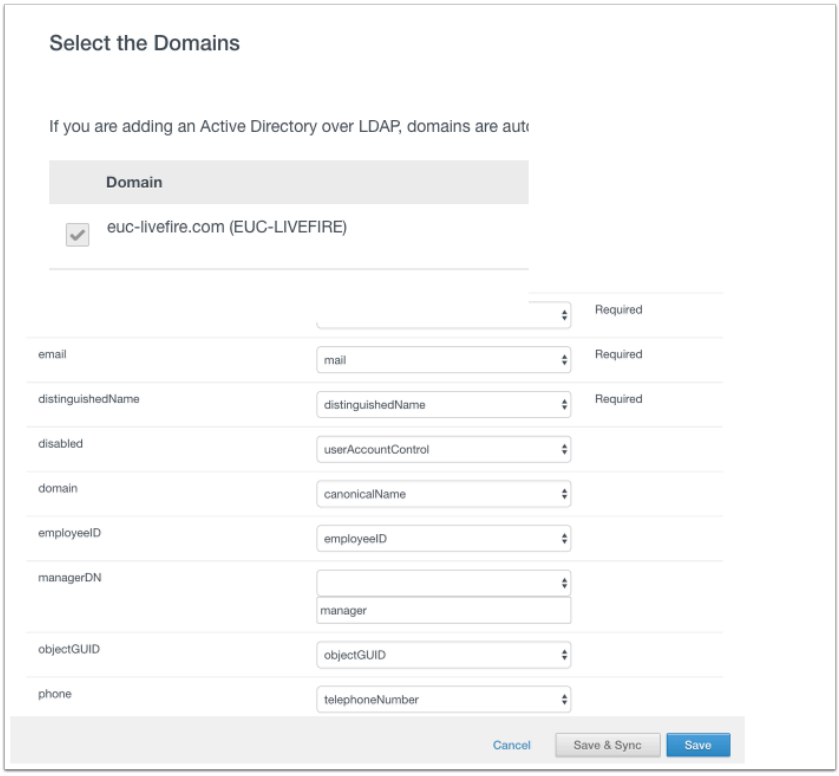
5.

- Configure our AD-sync configuration with Workspace ONE Access….continued
  1. On the **Select the Domains** page, select **Next. euc-livefire.com** should be discovered.
  2. On the **Map User Attribute** page scroll down to **objectGuid** and select the **drop down** arrow select **objectGUID.**
     Since this is the attribute we setup earlier in User Attributes we will also need to map it to an AD attribute.
  3. Next to **managerDN** select ***custom input*** and type **manager** in the dropdown
  4. Next to **title** select **title** in the dropdown
  5. Select **Next**

Note of interest

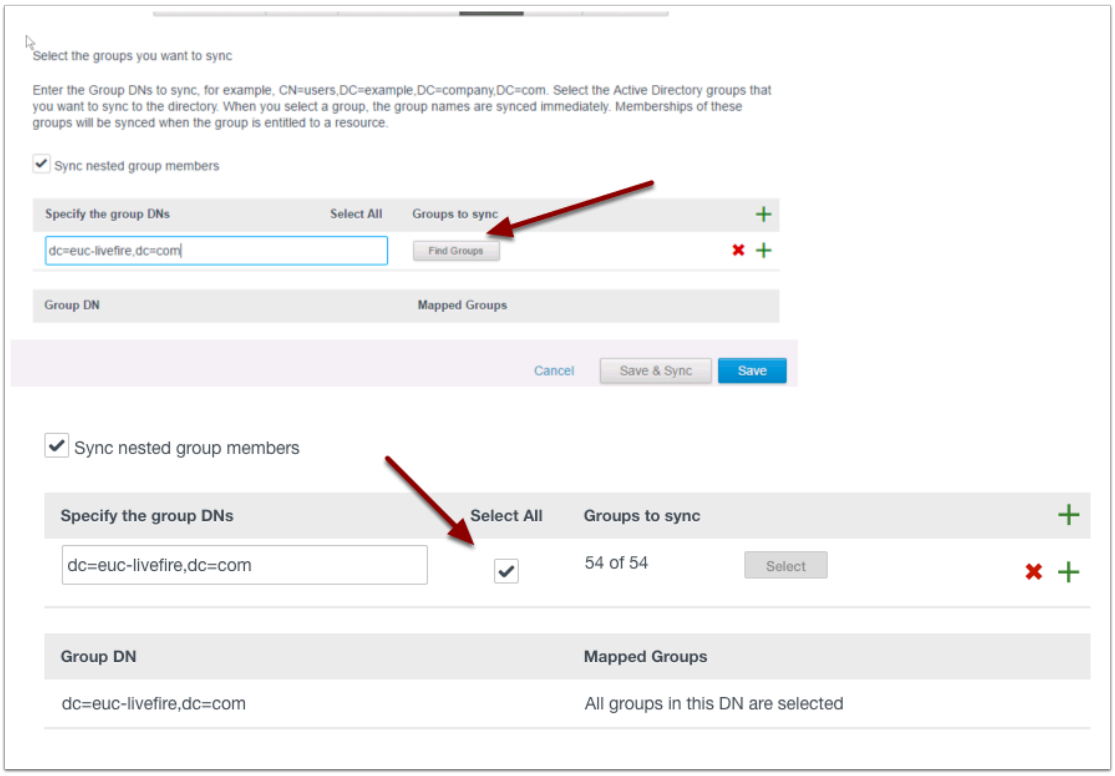
From version **Workspace ONE Access 1903** of , an attribute has been added which is **sourceanchor** set this also to **ObjectGUID**. Sourceanchor is the attribute often used for when

federating Azure. (Note: Some large customers may decide to use an alternative value such as ms-ds-consistenctguid for this attribute)



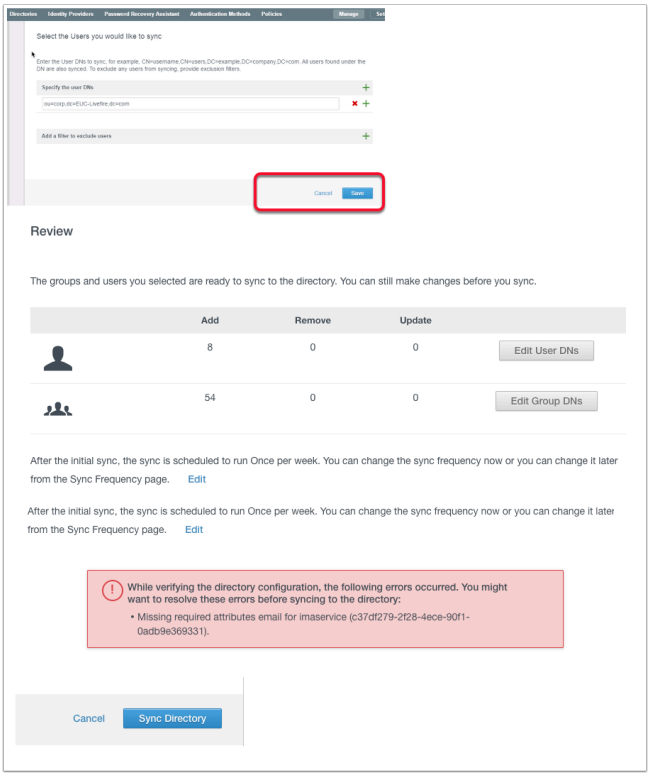
6.

- Configure our AD-sync configuration with Workspace ONE Access....continued
  1. On the **Select the Groups you want to sync** page, select the green plus (+) to the right of the page,
  2. Under **Specify the group DNs** type the following **dc=euc-livefire,dc=com** next to the distinguished name you added, select Find Groups then the **Select All** check box
  3. select **Next**.



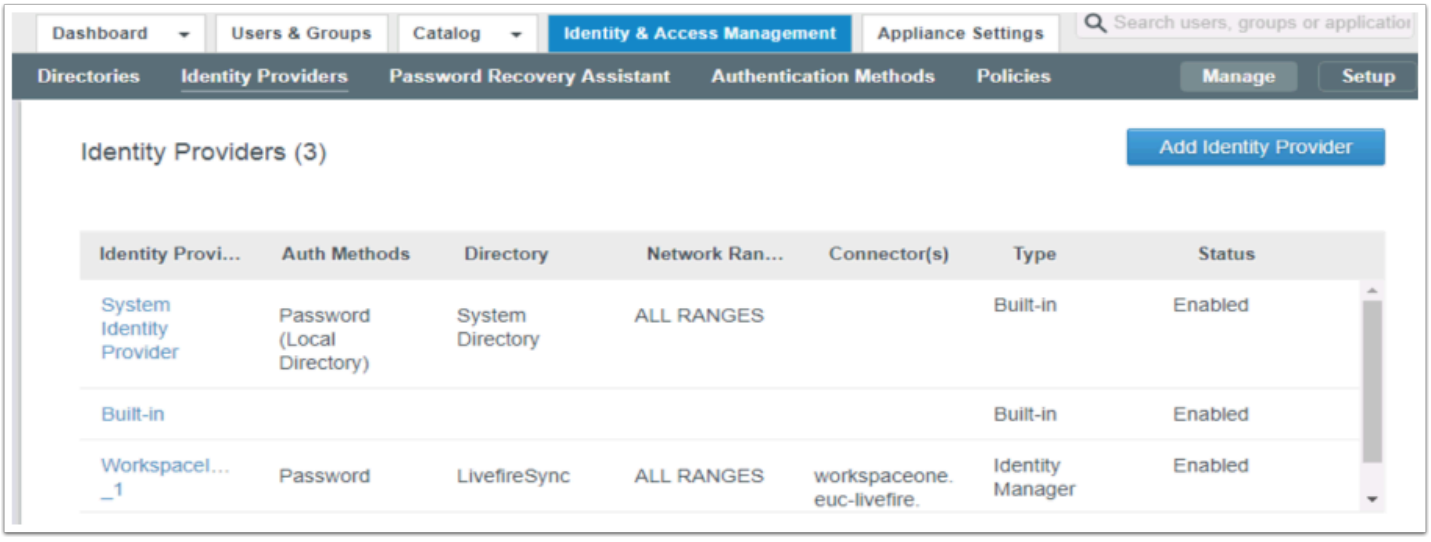
7.

- Configure our AD-sync configuration with Workspace ONE Access....continued
  1. On the **Select the Users you would like to sync page,** under **specify the user DNs** type **ou=corp,dc=EUC-Livefire,dc=com**
  2. Select **Next**, notice the objects to sync in the Review page.
  3. There may be an error, "Missing required attributes email for imaservice" Disregard this error. The sync will stil work.
  4. Select **Sync Directory**



8. Configuring the Built-in IDP in Workspace ONE Access

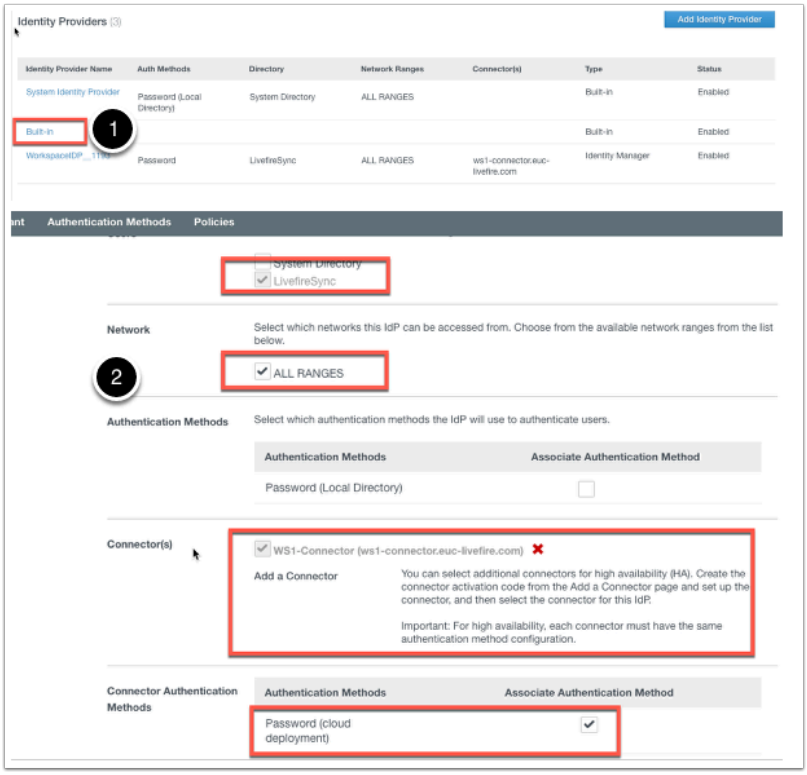
- Navigate to and select **Identity & Access Management** > **Manage**, select **Identity Providers**. Notice you now have an additional Identity Provider which is a Workspace IDP called **WorkspaceIDP_1xxx** which is associated with the LiveFireSync directory we just created above. This is an automatic process whereby when the built in connector is associated with Active Directory this Identity Provider gets created.



9. Configuring the Built-in IDP in Workspace ONE Access...continued

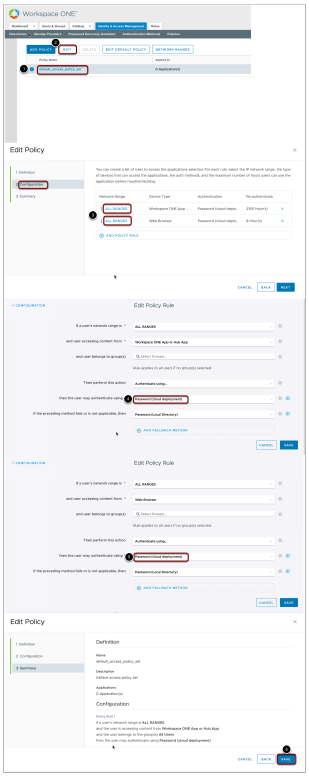
- Let's associate the Built-In iDP with the AD and the external connector to ensure **Password (Cloud Deployment)** can be used as an authentication method.

1. Select **Built-In**.
2. In the **Built-in IDP** windows select the following:
    1. Select **LivefireSync** under Users
    2. **All Ranges** under Network
    3. **Add** the **WS1-Connector.euc-livefire.com** to the connector section
        1. Click **Add Connector** to confirm
    4. Select **Password (Cloud Deployment) checkbox**
    5. Select **Save** at the bottom of the page.



10. Configuring the Built-in IDP in Workspace ONE Access...continued

- We need to ensure that our default access policy has **Password (Cloud Deployment)** set as the authentication method for enrollment to work. Note, Workspace ONE enrollment uses this access policy.
    1. Navigate to **Identity & Access Management** > **Manage** > **Policies** . Select **dafault_access_policy_set** and select **EDIT** (this will edit the default Access Policy Set)
    2. Select **Configuration** on the left navigation and **Workspace One App Policy** and select **Password (Cloud Deployment)** as the first authentication form. Select **SAVE** at the bottom of the page.
        1. **NOTE**: Be sure to leave Password (Local Directory) as the fallback method as seen in the screen shot below.
    3. Now Select the **Web Browser** and do the same by changing the primary authentication method to **Password (Cloud Deployment)** and select **SAVE** at the bottom of the page.
        1. **NOTE**: Be sure to leave Password (Local Directory) as the fallback method
    4. Select **NEXT** on the **Policy Page** and **SAVE** on the final page of the wizard.



This section of the lab is completed. We will not install and configure the ACC as a later lab will look at SCIM provisioning users in the WorkspaceOne UEM.