

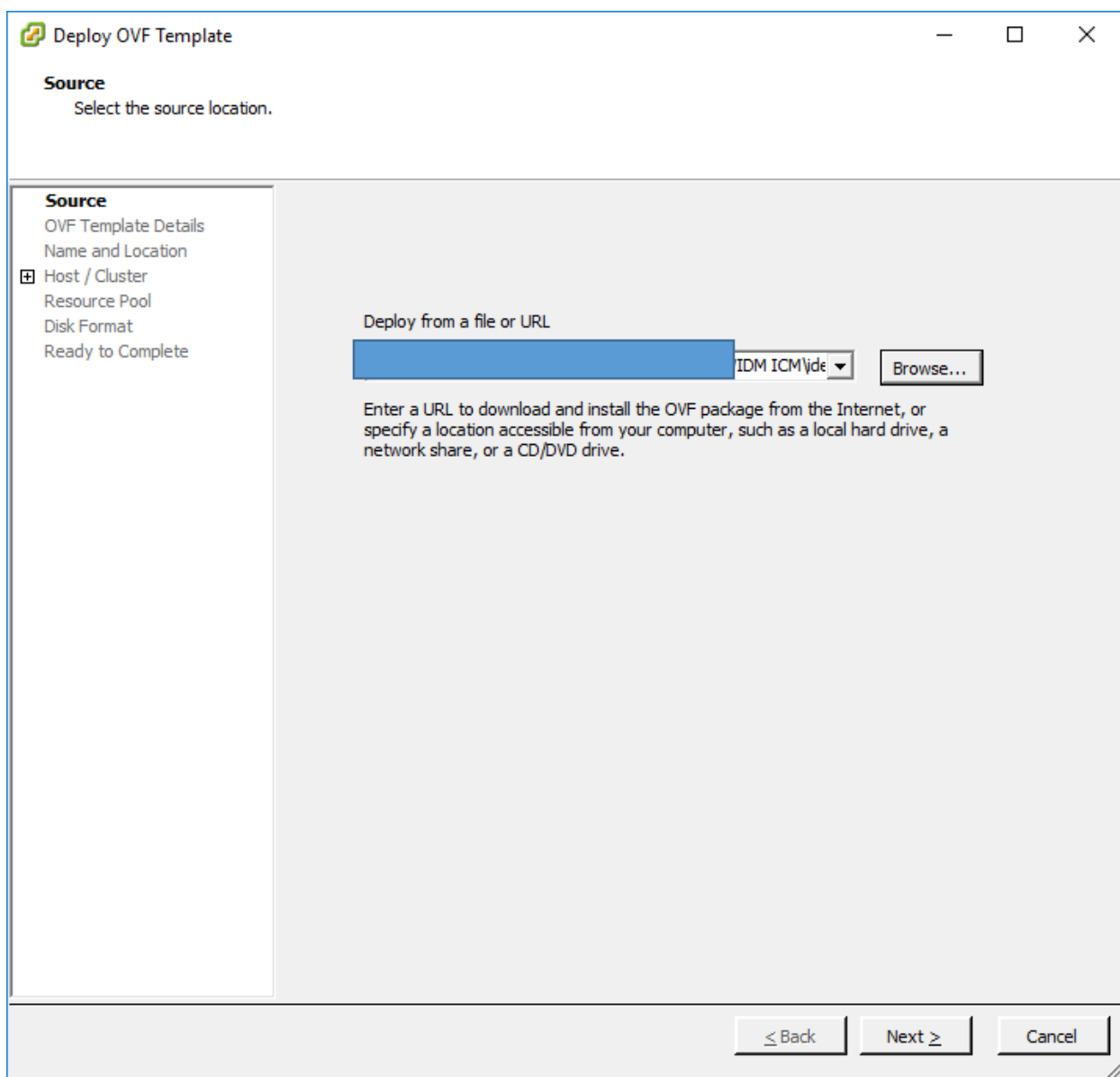
How to install /configure Workspace One ?

Our setup will have one UI (user interface server with database) and two connector servers

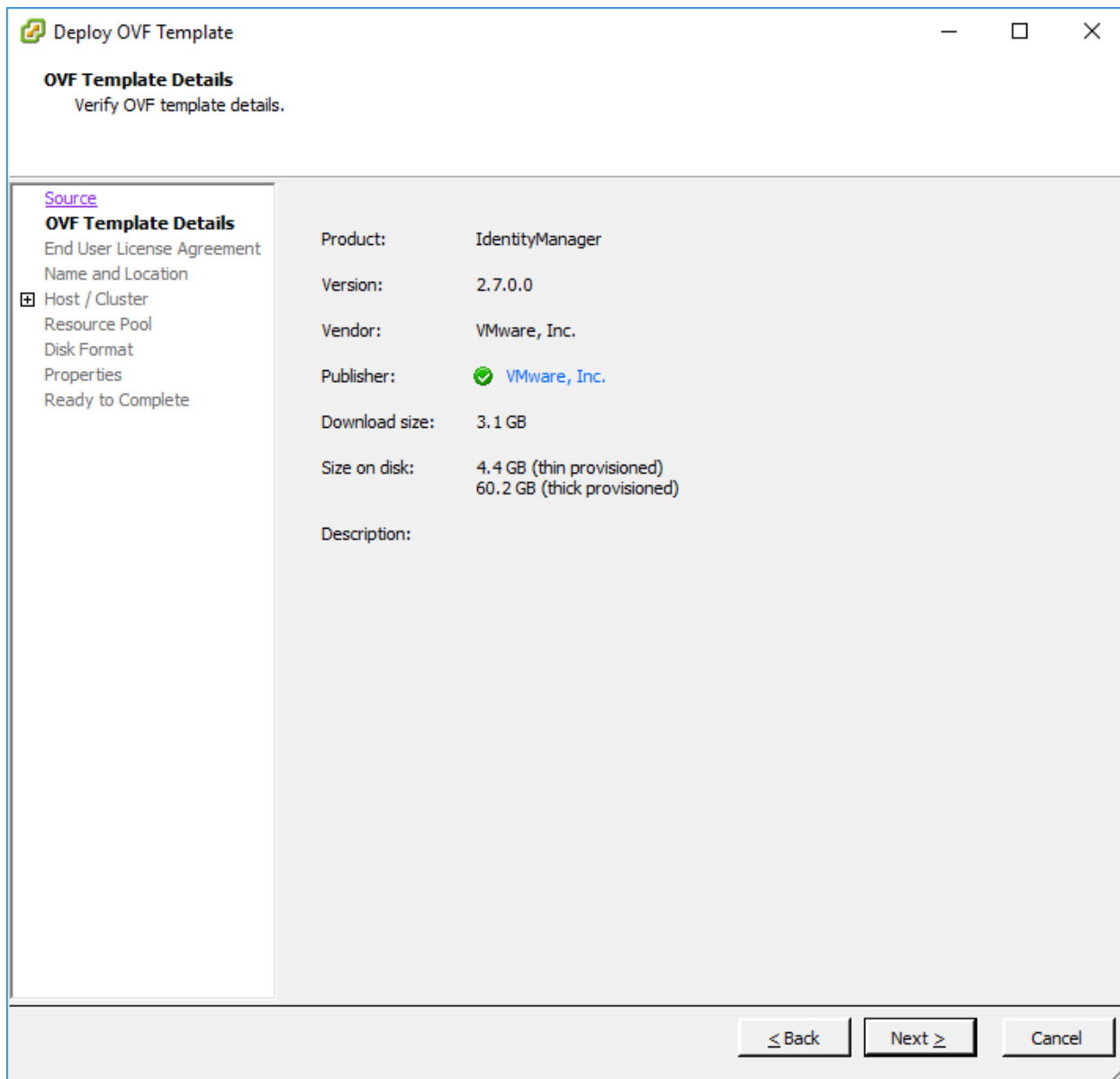
Basically UI and connectors come as OVA format appliance. you can download them from my VMware portal based on your account access.

Connect to your Vcenter server and deploy OVA files as below guide.

Deploy manager OVA



Select file from **browse** menu and select **Next**



Click **next**

Deploy OVF Template

End User License Agreement

Accept the end user license agreements.

[Source](#)
[OVF Template Details](#)
End User License Agreement

- Name and Location
- Host / Cluster
- Resource Pool
- Disk Format
- Properties
- Ready to Complete

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls that party, and here "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of that entity.

Accept and select Next

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)

Name and Location

- Host / Cluster
- Resource Pool
- Disk Format
- Properties
- Ready to Complete

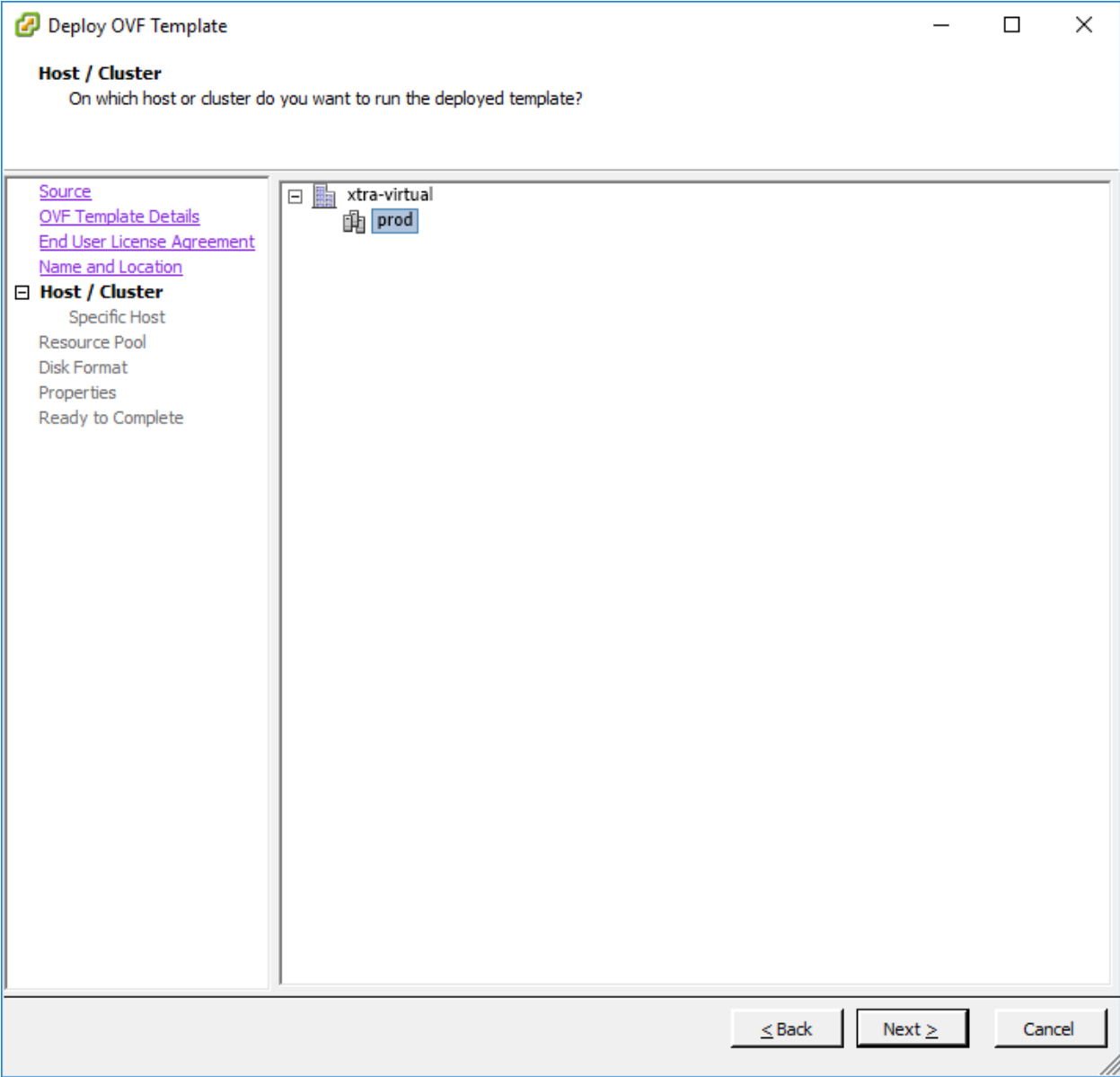
Name:
xtra-ws1-ui
The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

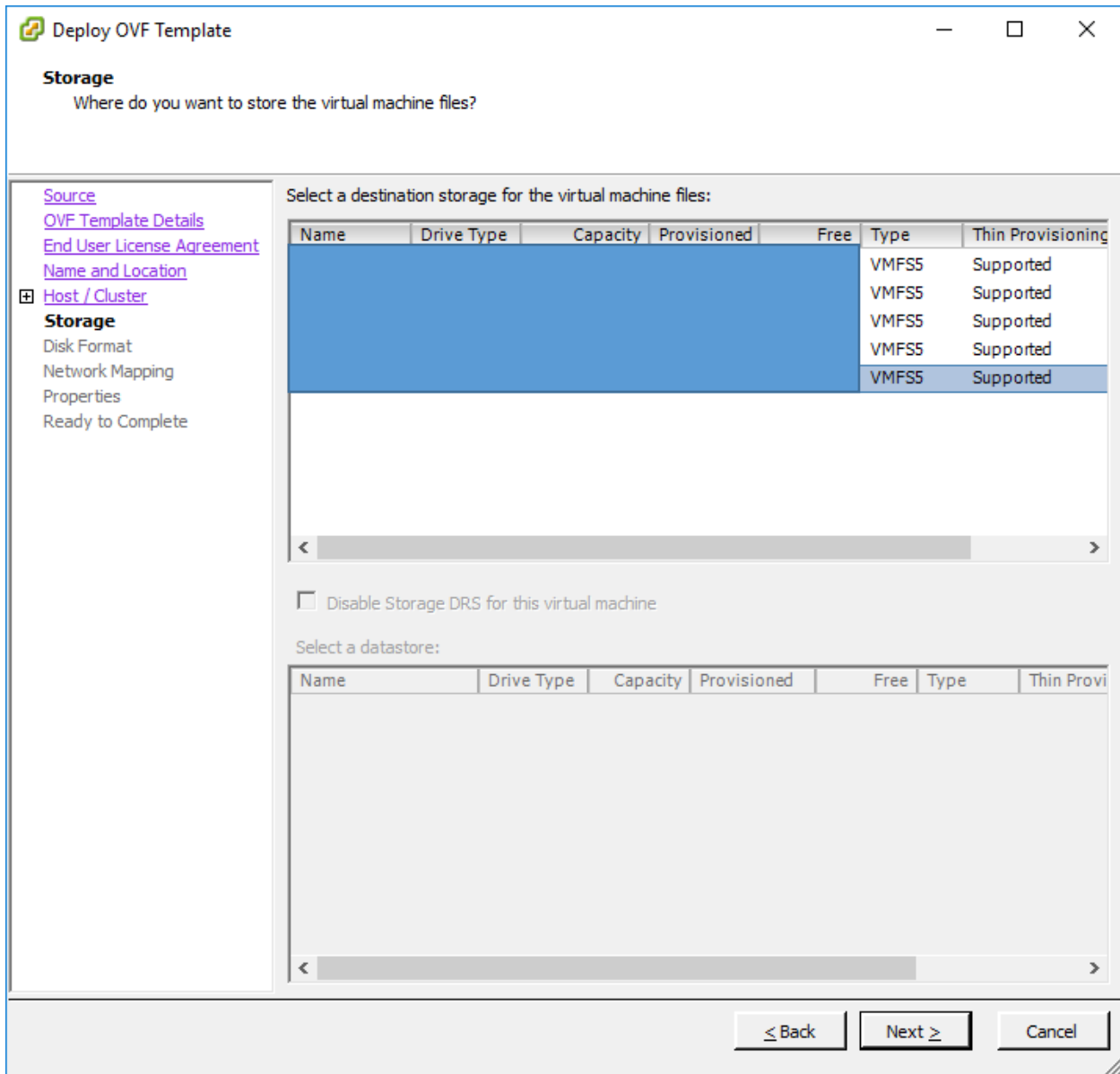
- xtra-virtual
 - Core
 - DESKTOP
 - Discovered virtual machine
 - MGMT
 - WS1

< Back Next > Cancel

Give some **name** to your appliance **select** your folder location and select **next**



Select **cluster /host** and hit **next**

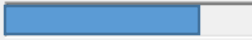


Select **Datastore** where you want to put your VM

Deploy OVF Template

Disk Format
In which format do you want to store the virtual disks?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
Host / Cluster
Storage
Disk Format
Network Mapping
Properties
Ready to Complete

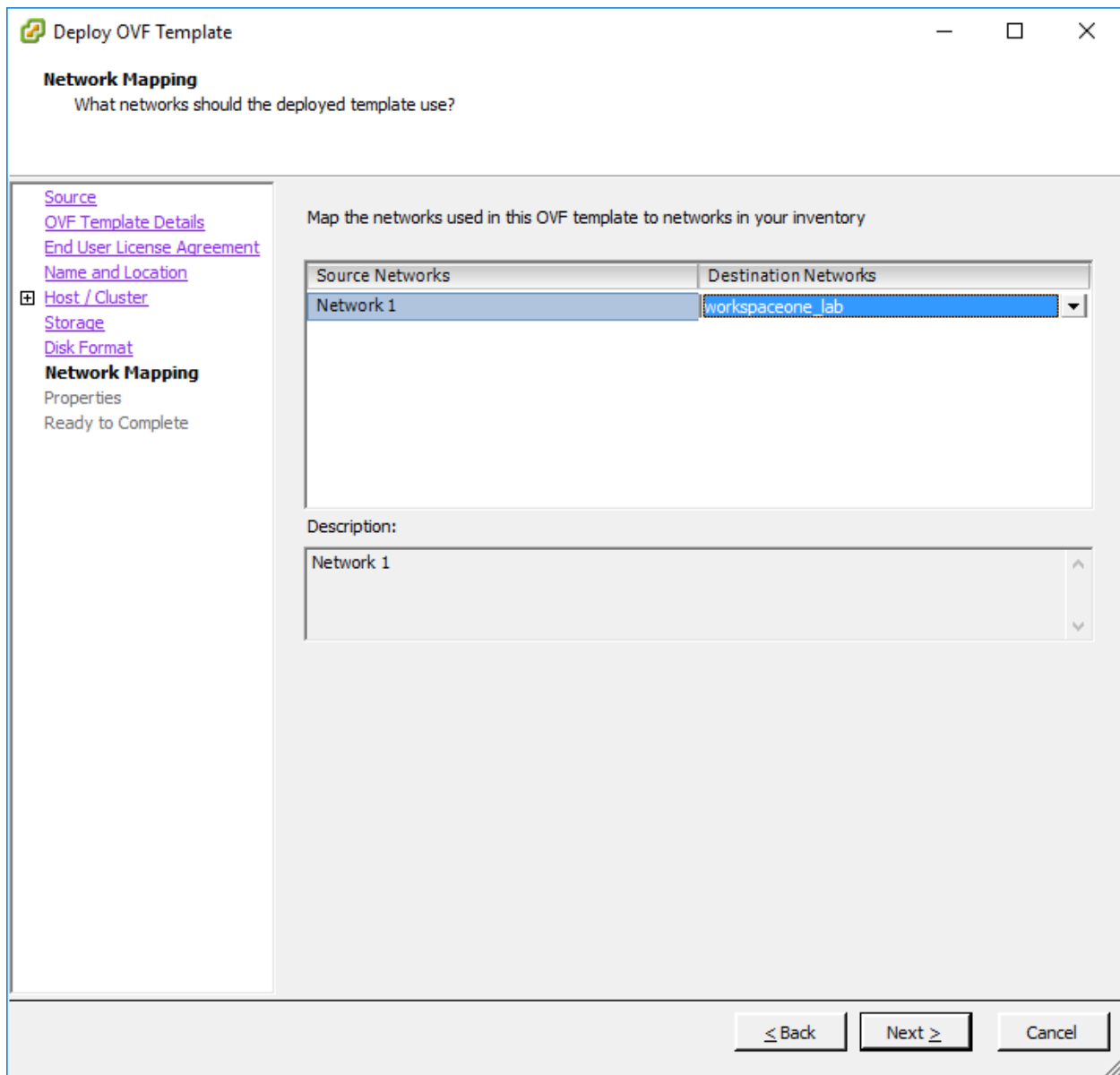
Datastore: 

Available space (GB):

Thick Provision Lazy Zeroed
 Thick Provision Eager Zeroed
 Thin Provision

≤ Back Next ≥ Cancel

Select **thin provision** as storage policy and hit **next**



Select **network port group** where you want to place your VM and hit **Next**

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
Host / Cluster
[Storage](#)
[Disk Format](#)
[Network Mapping](#)
Properties
Ready to Complete

The default gateway address for this VM. Leave blank if DHCP is desired. All fields but hostname are required for static IP.

Domain Name
The domain name of this VM. Leave blank if DHCP is desired.

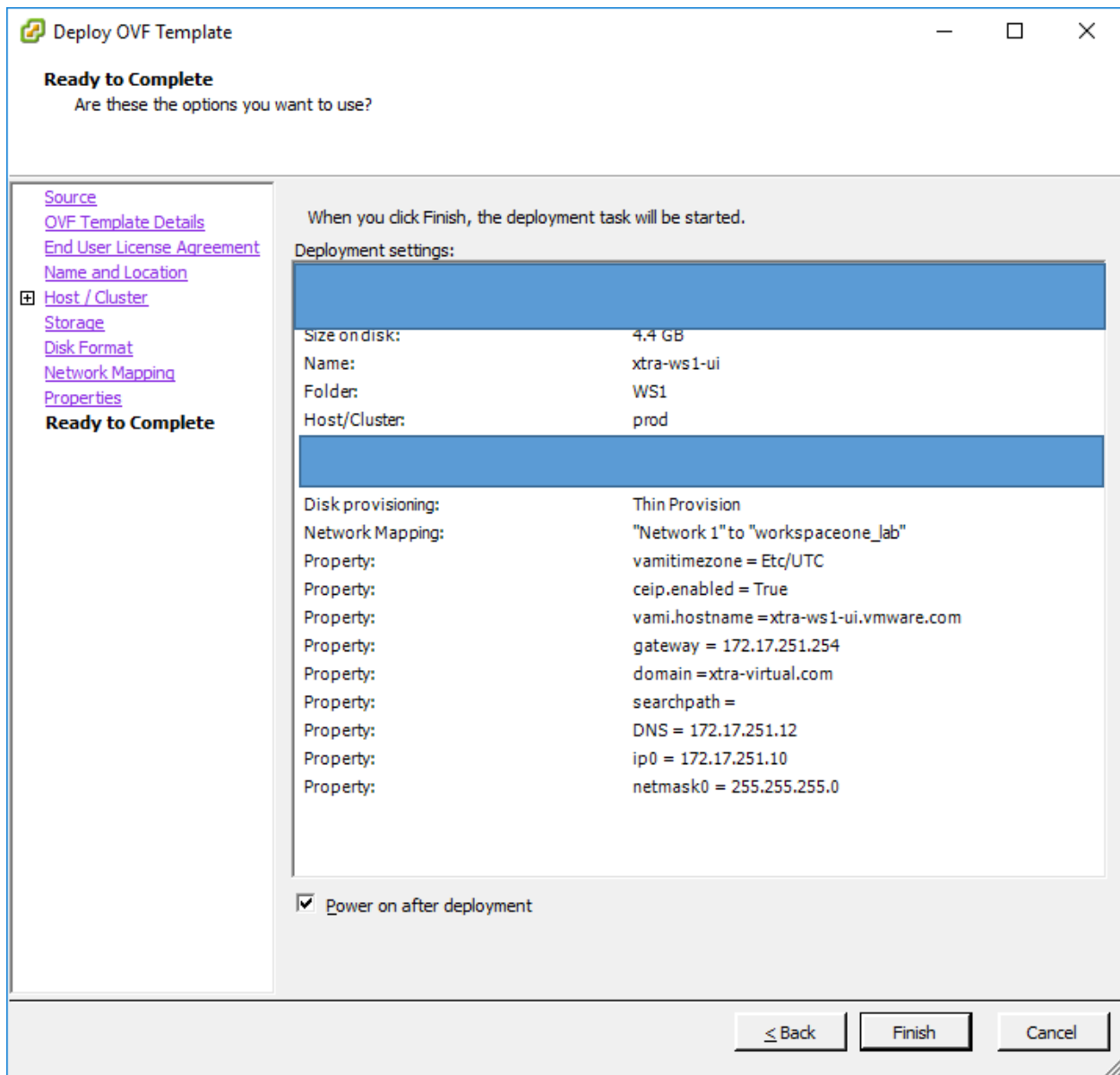
Domain Search Path
The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired.

DNS
The domain name servers for this VM (comma separated). Leave blank if DHCP is desired. All fields but hostname are required for static IP.

IP Address
The IP address for this interface. Leave blank if DHCP is desired. All fields but hostname are required for static IP.

Netmask
The netmask or prefix for this interface. Leave blank if DHCP is desired. All fields but hostname are required for static IP.

Provide **FQDN**, **IPV4** information, **DNS** and hit **next**



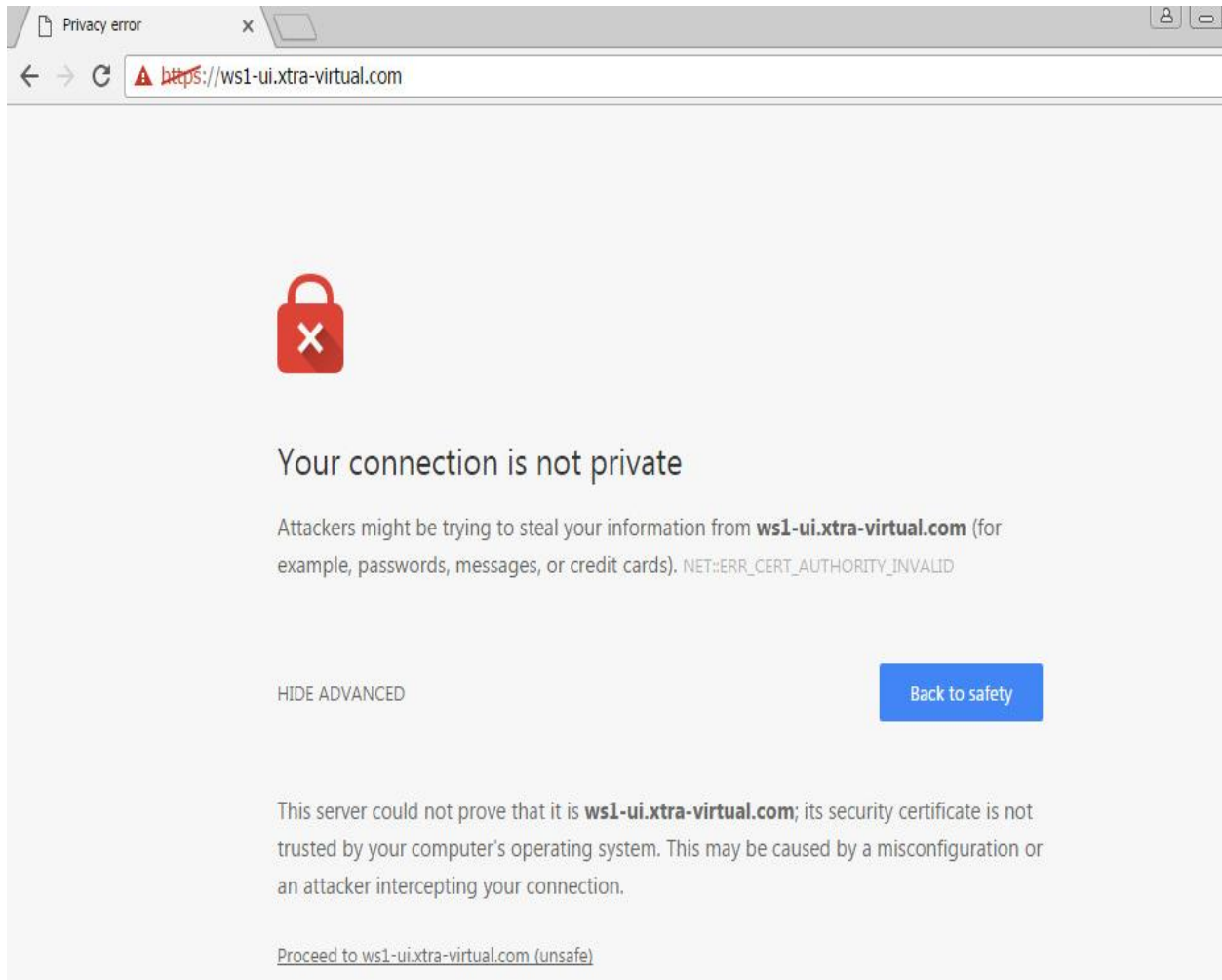
Select **Power on after deployment** and hit **finish**

Follow same steps to deploy N number of connector appliance as well. for our case we will use N=2

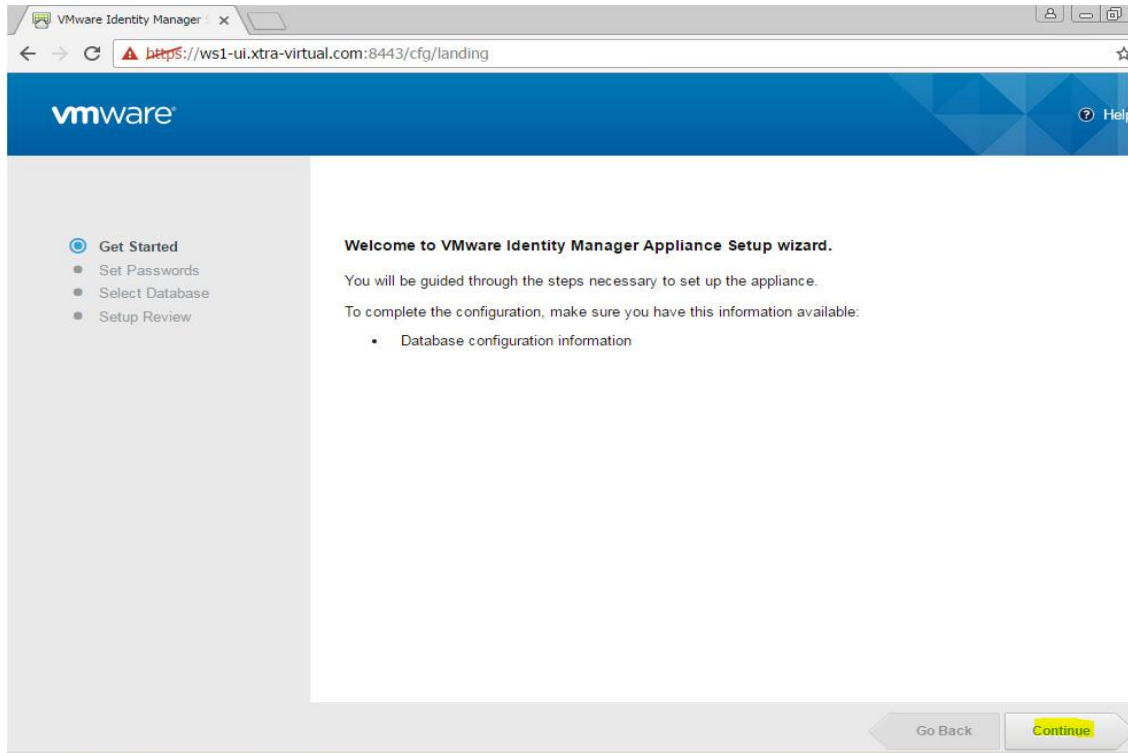
Once we have deployed all are UI and connector servers, it is time to configure them.

Configuration of UI + Database server

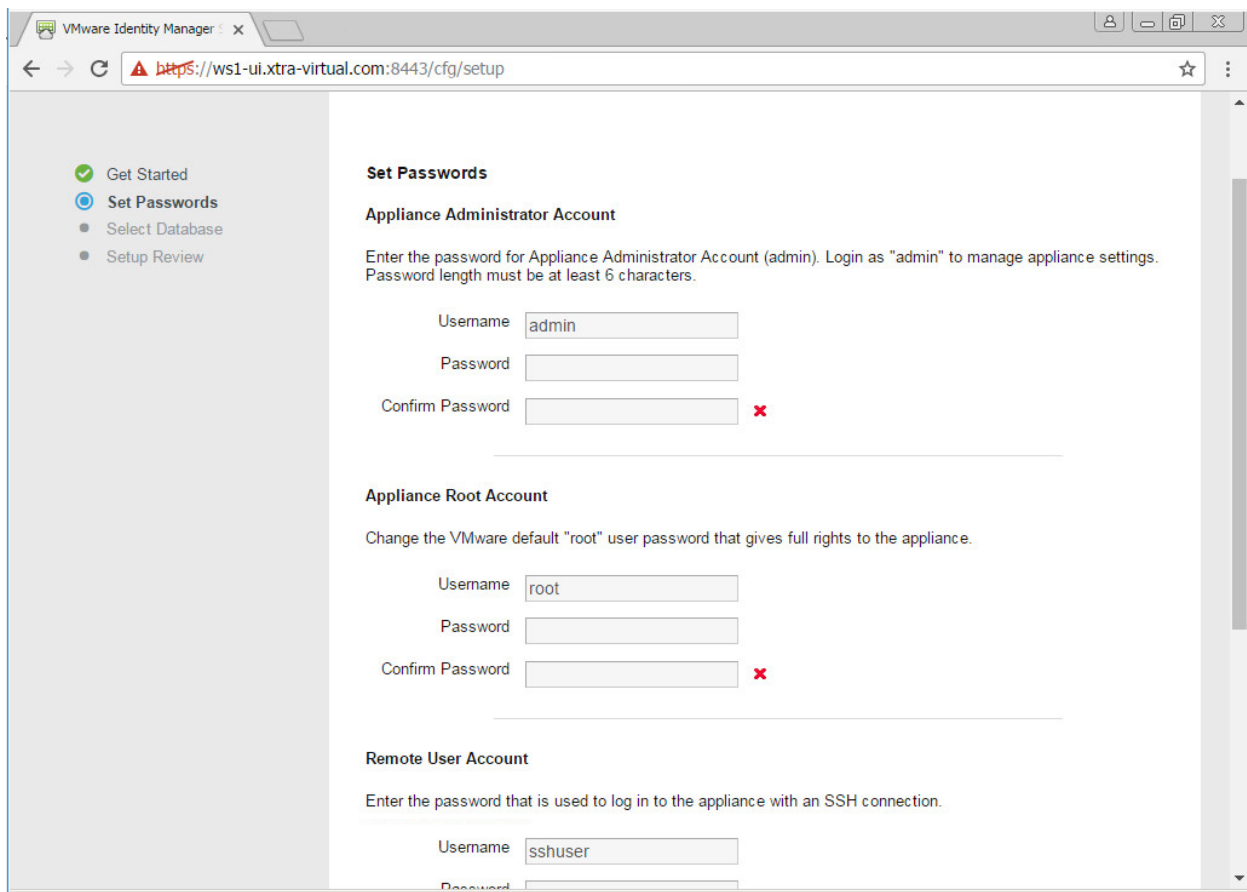
Access UI FQDN over port 443 for first configuration page. Ignore SSL error as we are using Self signed certificates only.

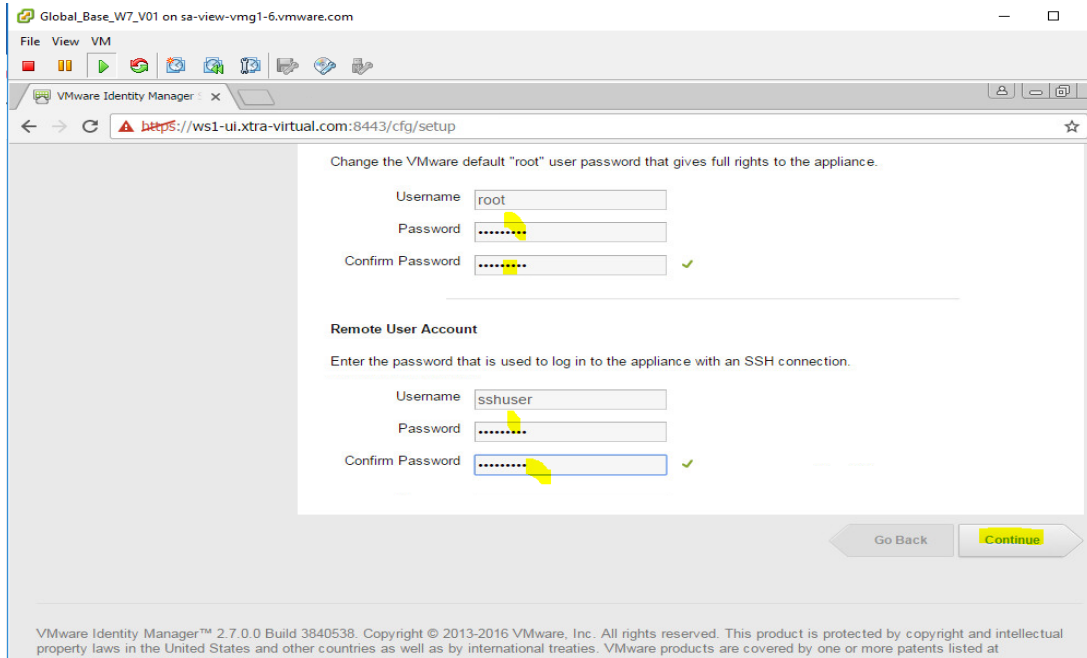


Select **Proceed** to the next page.

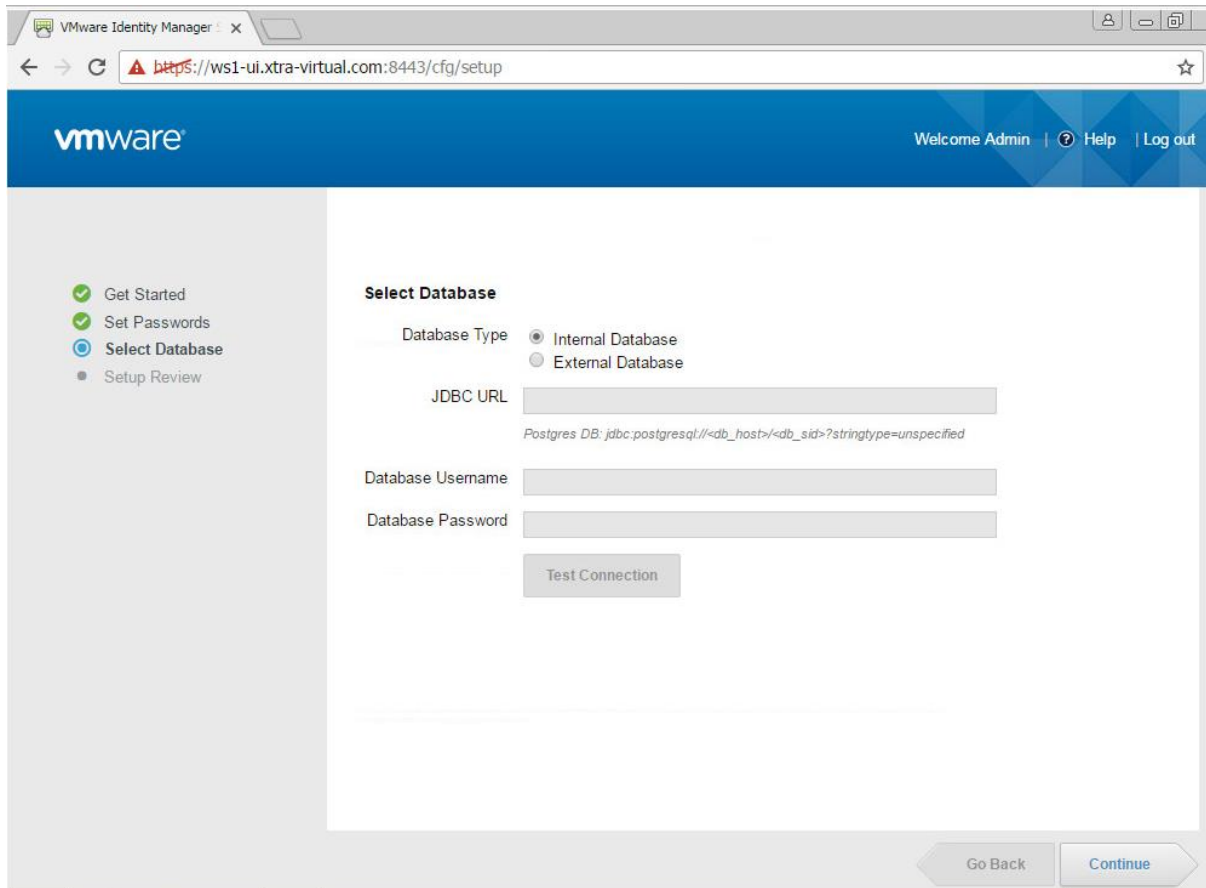


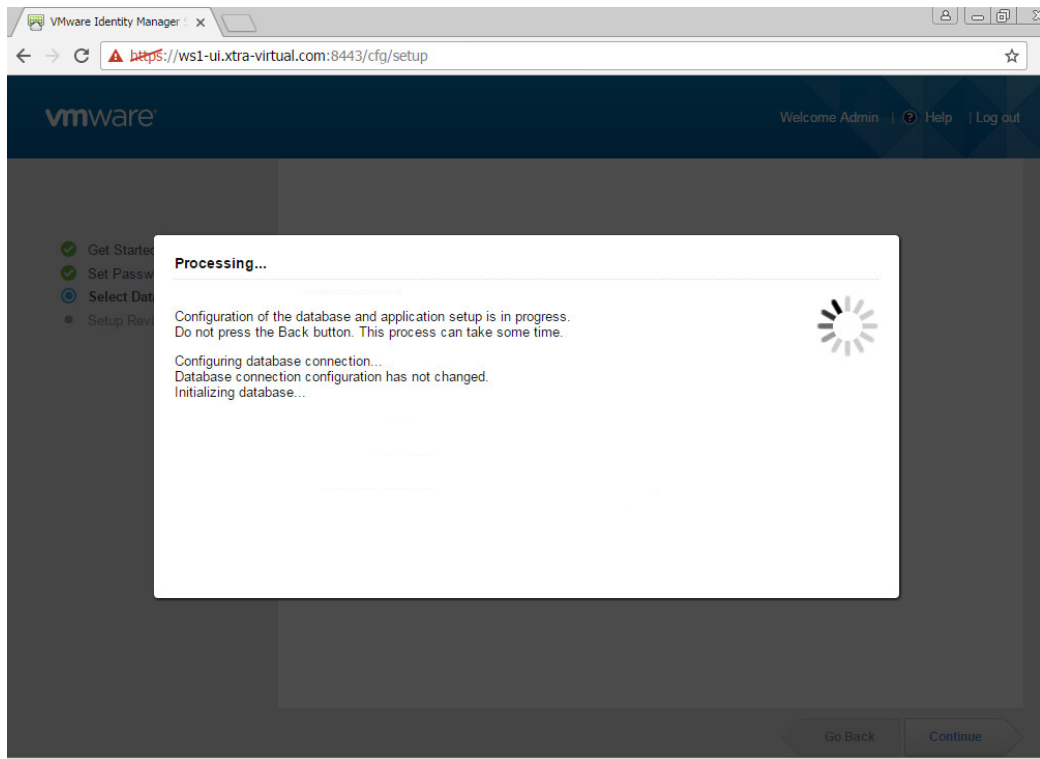
Select **continue** on the database configuration page, reset all passwords and hit **Continue**



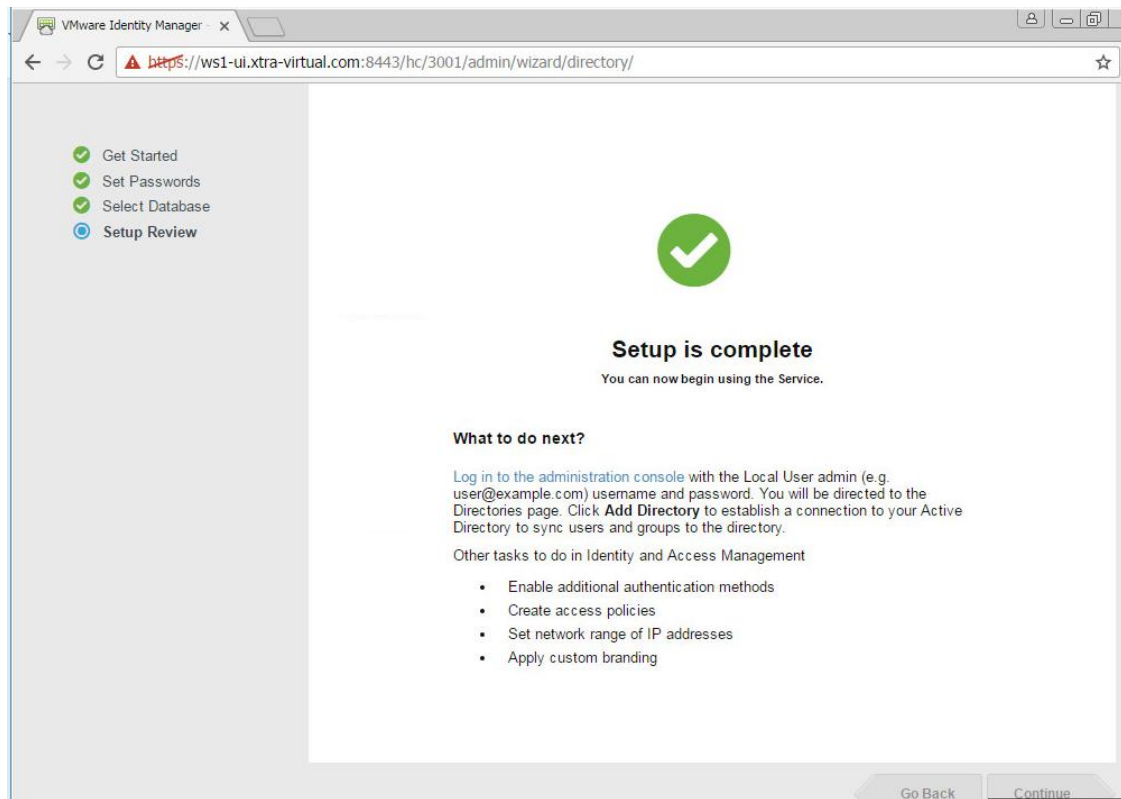


Select internal Database and hit **continue**, you can use **external Database** using external Database option, Provide **JDBS url**, database **username** and **password** to configure

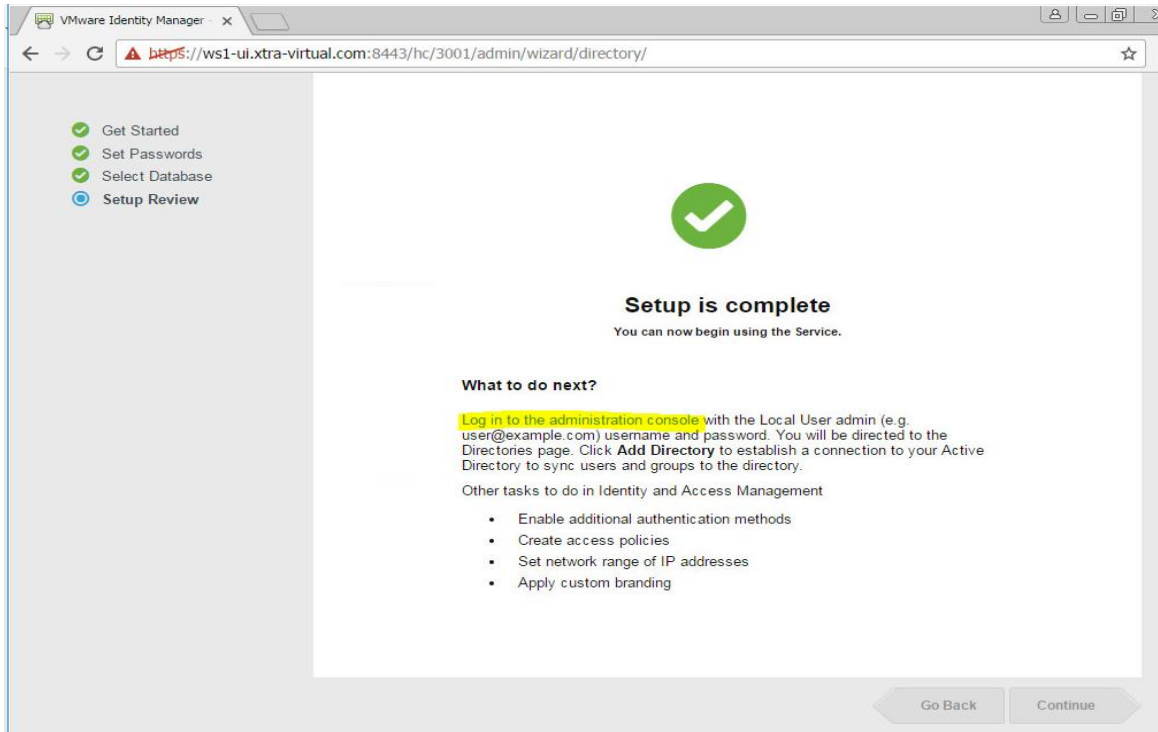




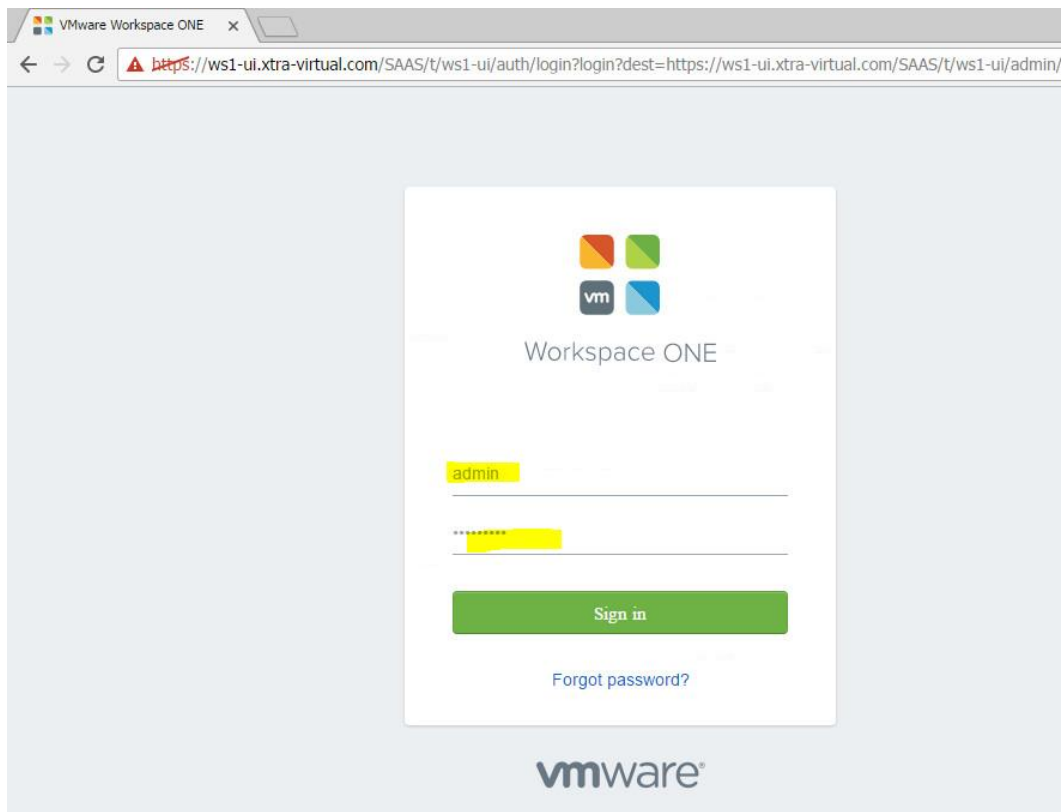
Wait for some time, till you get **below page** which means **UI + DB are configured**



Now it is time to **configure connectors to UI server** and adding the **directory** information to be used click **login to the administration console**



Use **Admin** as **username** and **password** you set in initial configuration



Click **Setup** and you will land to the below page select **add connector**

VMware Workspace ONE x Privacy error x

← → ↻ <https://ws1-ui.xtra-virtual.com/SAAS/t/ws1-ui/admin/identity> ☆

Workspace ONE Local Admin · WS1-UI

Dashboard Users & Groups Catalog Identity & Access Management Appliance Settings Search users, groups or applications

Connectors Custom Branding User Attributes Network Ranges Auto Discovery AirWatch Preferences Manage **Setup**

Connectors (1) [Add Connector](#)

Host Name	Worker	Identity Provider	Authentication M...	Associated Direc...	Available Actions
Host Name: ws1-ui.xtra-virtual.com Port: 8443 Version: 2.7.0.0 Build 3840538 Domain:	ws1-ui.xtra-virtual.com				Join Domain

Add connector FQDN in **connector ID Name** and generate activation code

VMware Workspace ONE x Privacy error x

← → ↻ <https://ws1-ui.xtra-virtual.com/SAAS/t/ws1-ui/admin/identity> ☆

Workspace ONE Local Admin · WS1-UI

Dashboard Users & Groups Catalog Identity & Access Management Appliance Settings Search users, groups or applications

Connectors Custom Branding User Attributes Network Ranges Auto Discovery AirWatch Preferences Manage **Setup**

Add a Connector

Add the connector name and click Generate Activation Code. The connector activation code is used to establish communication between your service and the connector. Copy the activation code and apply it to your connector setup.

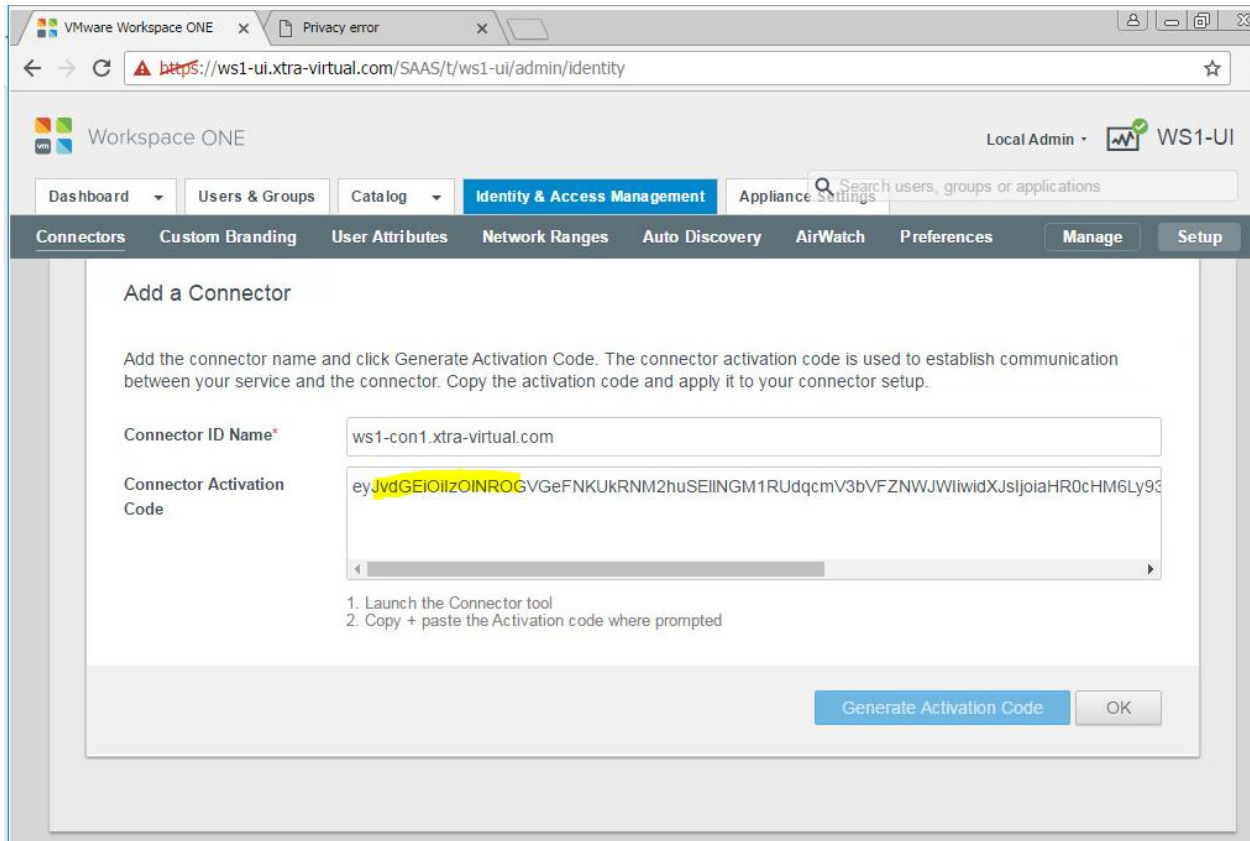
Connector ID Name*

Connector Activation Code

1. Launch the Connector tool
2. Copy + paste the Activation code where prompted

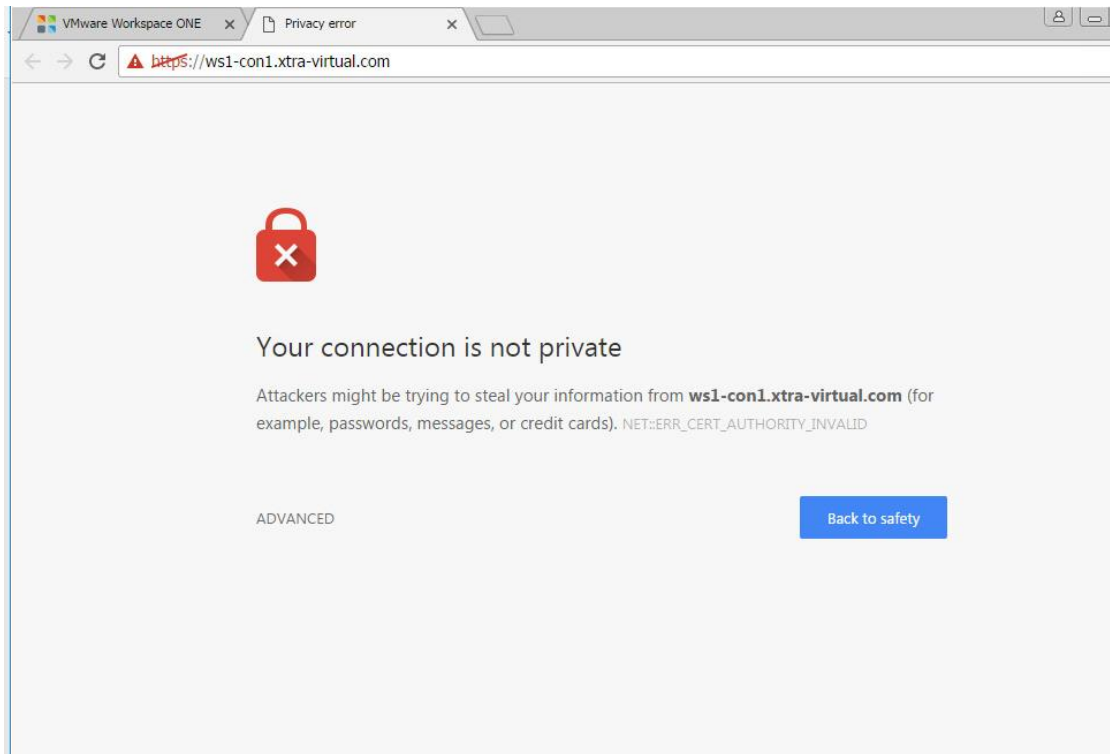
[Generate Activation Code](#) [Cancel](#)

You will need this activation code when you will configure the connectors for the first time

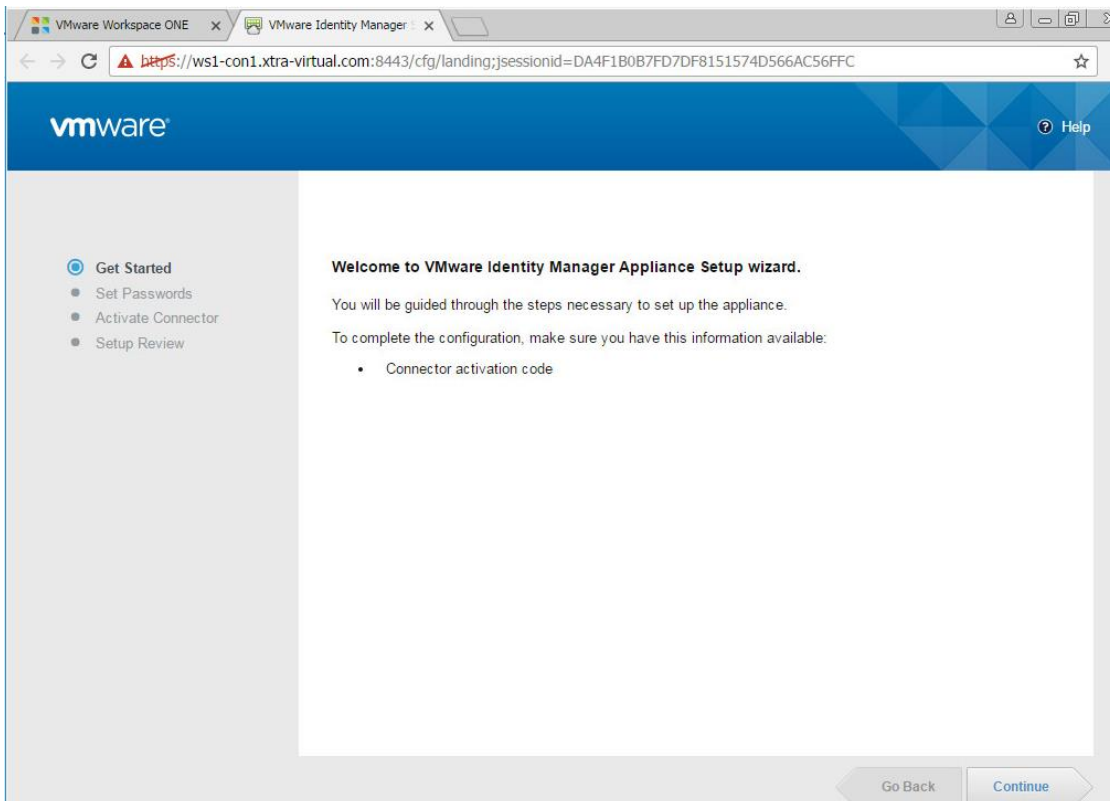


Make note of the **activation code** and **hit ok** and you should get activation code for all connector services.

Connector configuration: now it is time to configure for the first time



Open <https://fqdn> of connector servers that will open **configuration page** as below



The screenshot shows the VMware Identity Manager setup interface. The browser address bar displays `https://ws1-con1.xtra-virtual.com:8443/cfg/setup`. The page is titled "Appliance Administrator Account" and contains three sections for password configuration:

- Appliance Administrator Account:** Instructions to enter the password for the "admin" user. The "Confirm Password" field shows a red "X" error icon, indicating a mismatch.
- Appliance Root Account:** Instructions to change the default "root" user password. The "Confirm Password" field shows a green checkmark, indicating a successful match.
- Remote User Account:** Instructions to enter the password for an SSH connection. The "Confirm Password" field shows a green checkmark, indicating a successful match.

Set passwords as we did for UI server, and next page you need to put your **activation code**

The screenshot shows the "Activate Connector" page in the VMware Identity Manager administration console. The browser address bar displays `https://ws1-con1.xtra-virtual.com:8443/hc/admin/mol/`. The VMware logo is visible in the top left, and "Help" and "Log out" links are in the top right. A progress sidebar on the left shows the following steps:

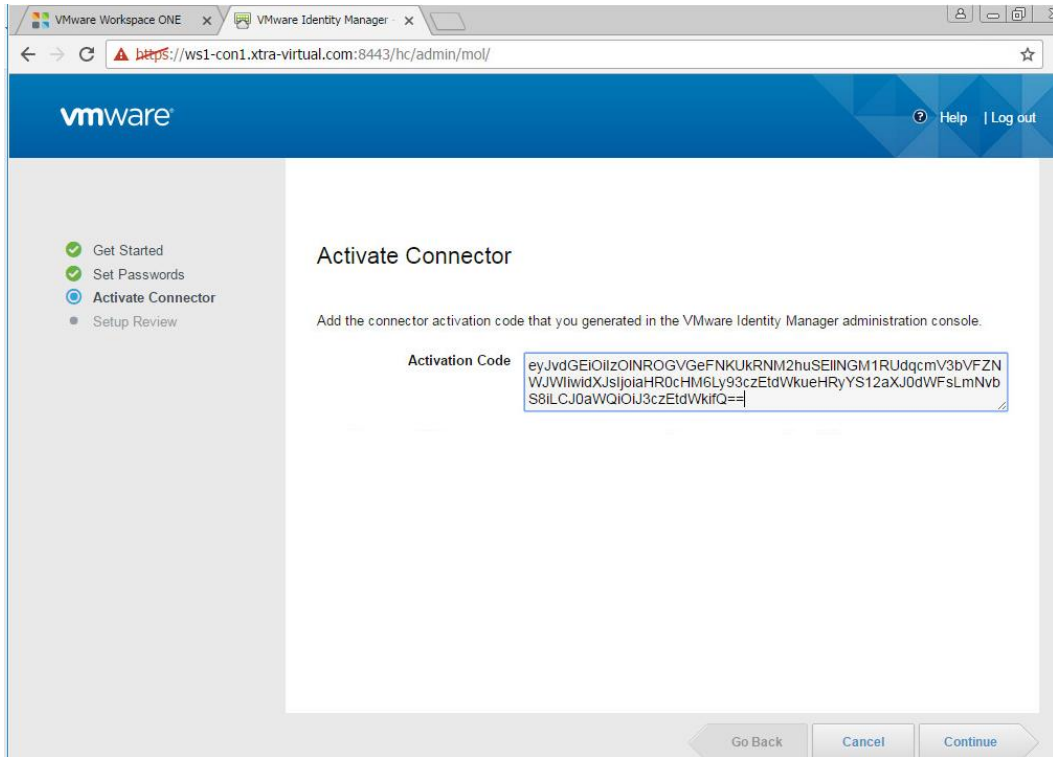
- Get Started (checked)
- Set Passwords (checked)
- Activate Connector (selected)
- Setup Review (not started)

The main content area is titled "Activate Connector" and includes the instruction: "Add the connector activation code that you generated in the VMware Identity Manager administration console." Below this, an "Activation Code" is displayed in a text box:

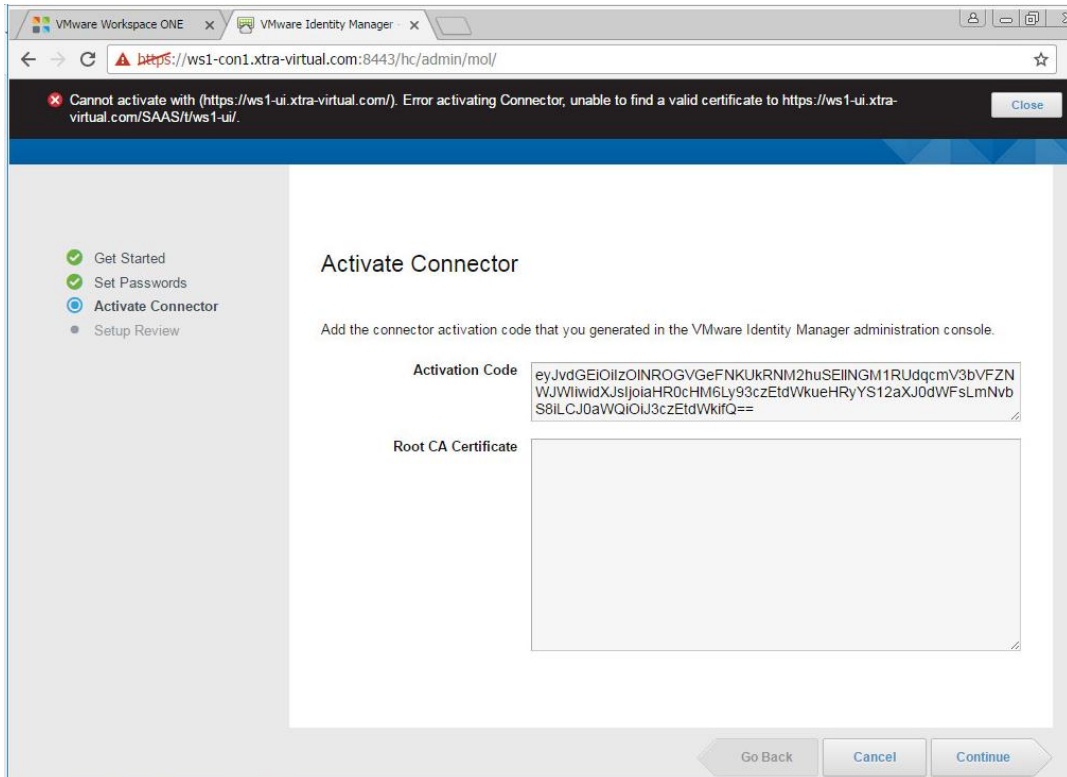
```
eyJvdGEiOIlzOINROGVGeFNkUkRNM2huSEllNGM1RUdqcmV3bVFZNVWJWlwiidXJsljoiaHR0cHM6Ly93czEtdWkueHRyYS12aXJ0dWFSLmNvbS8iLCJ0aWQiOiJ3czEtdWkifQ==
```

At the bottom of the page, there are three navigation buttons: "Go Back", "Cancel", and "Continue".

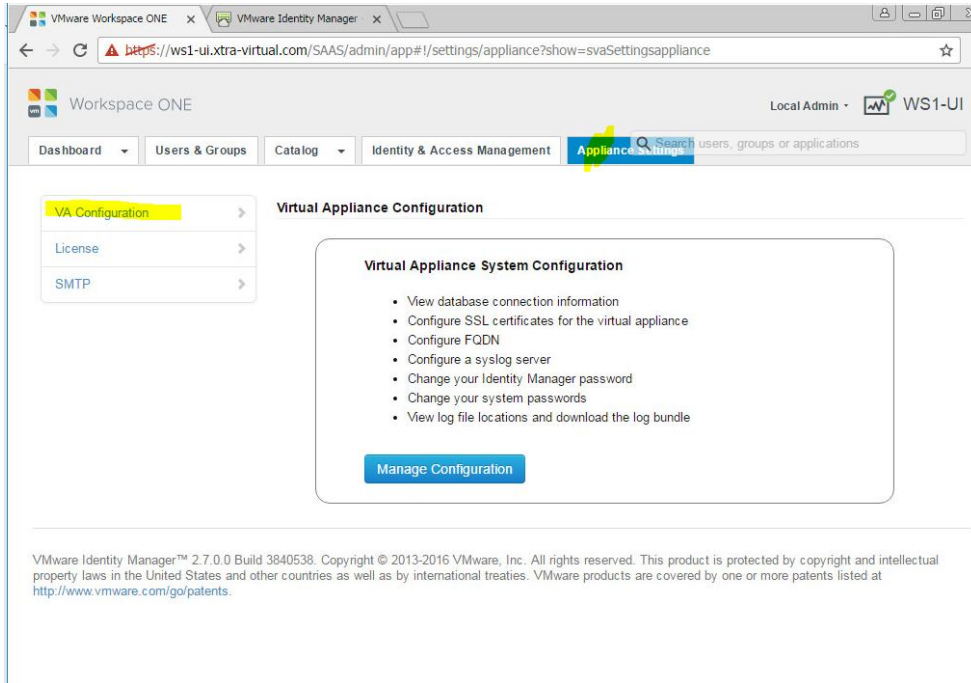
You need to use respective **activation code** that you have noted during addition of connectors to the UI server



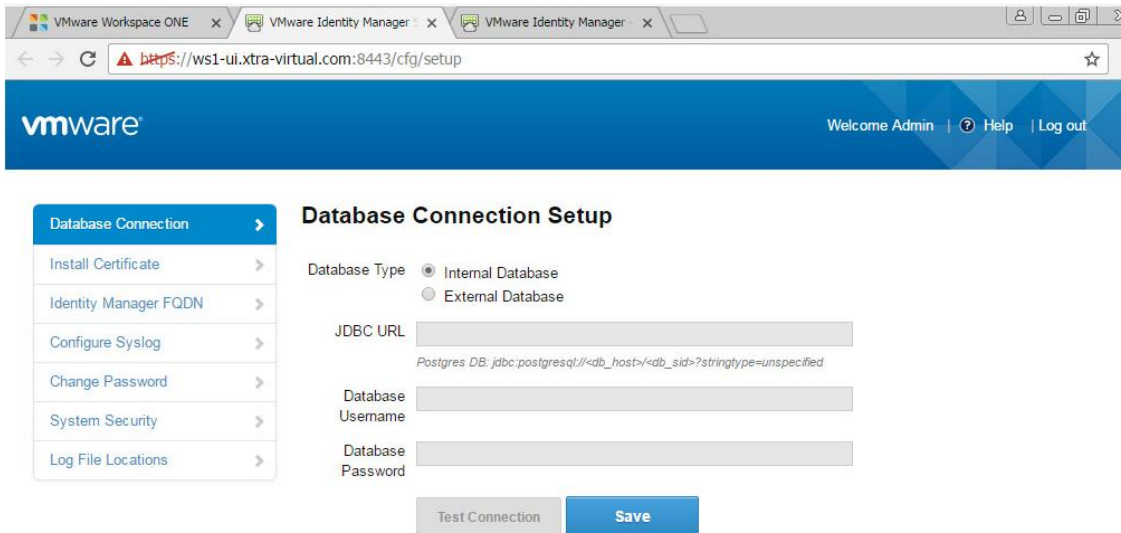
After hitting **continue** you will land to below page with and error



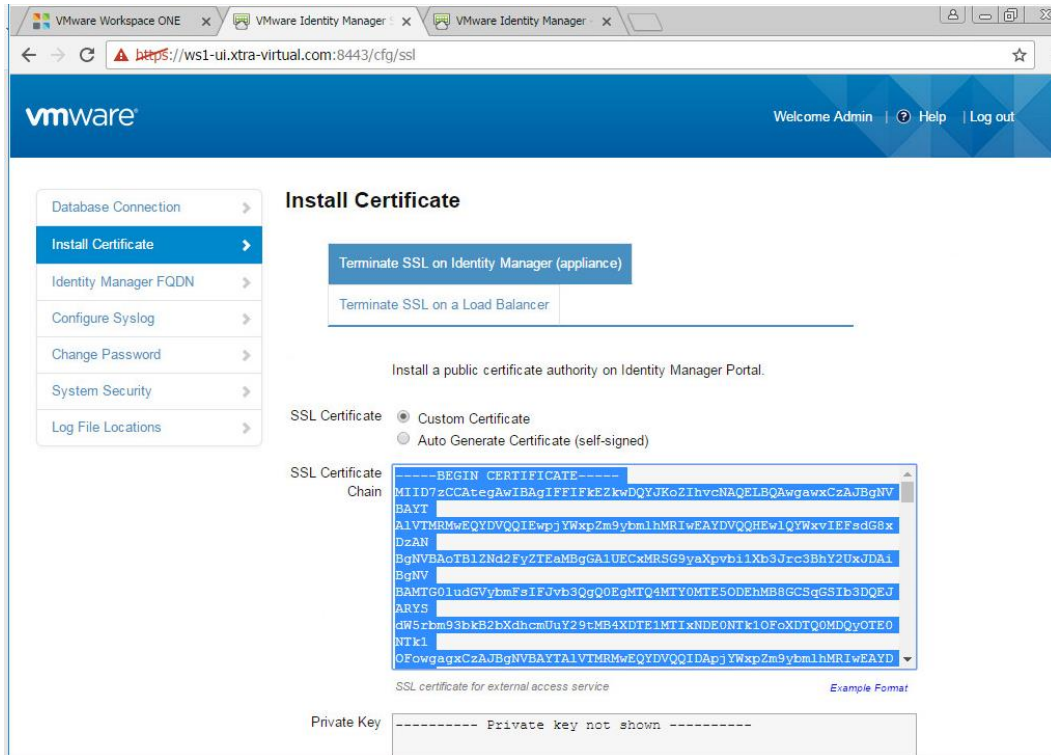
This error is due to **certificate error**; you need to update **Root CA** that is from **UI server** for that you need to go back to **UI appliance** configuration. Click **appliance settings**



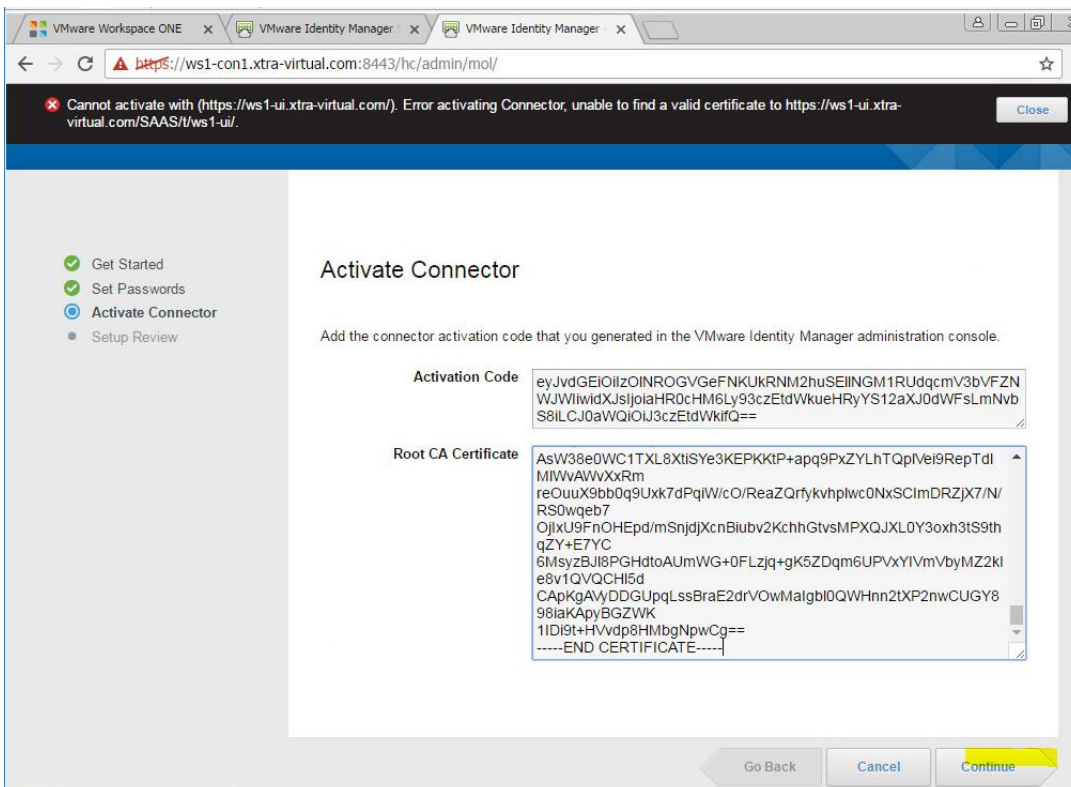
Manage Configuration > that will open another page with appliance configuration as below



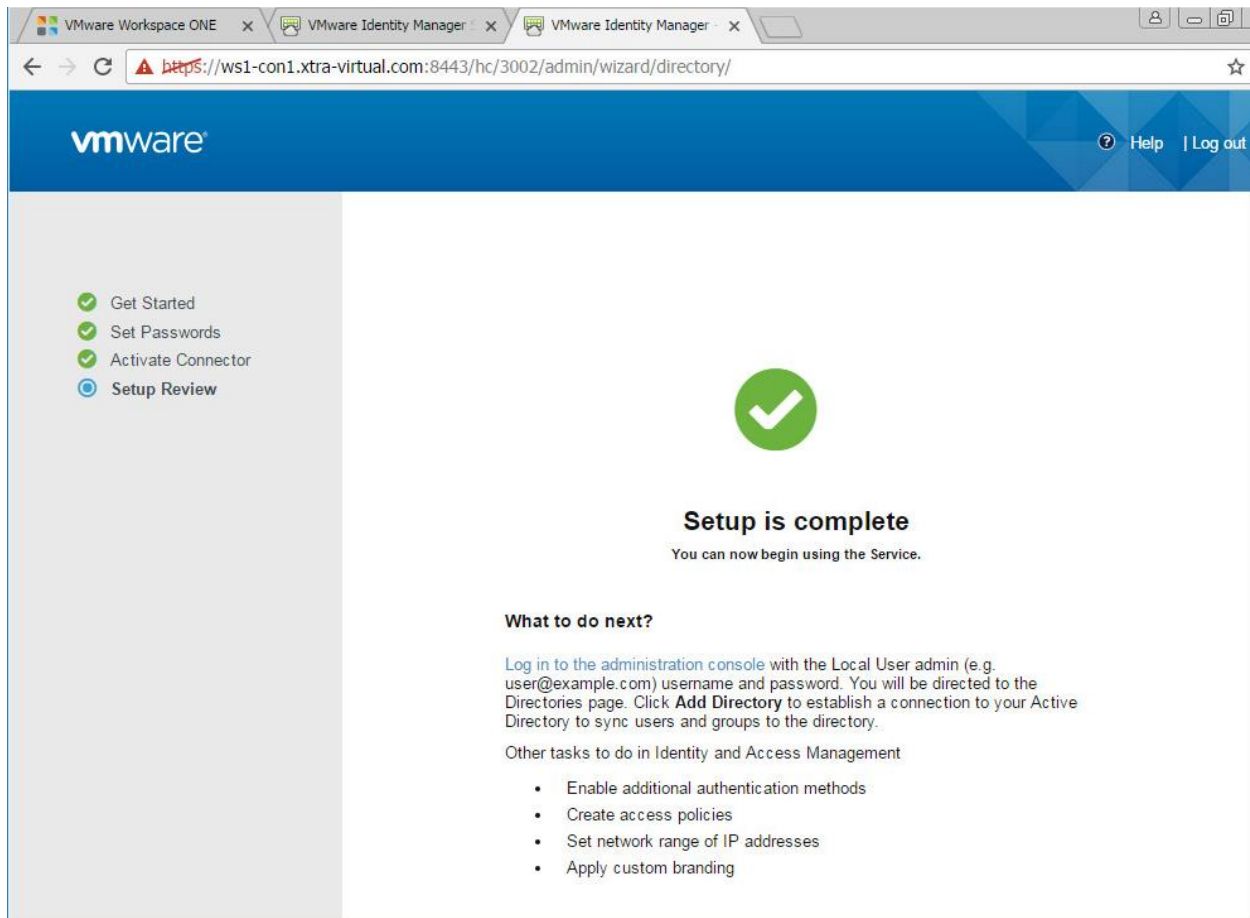
Click on **Install Certificate** and copy the **SSL certificate chain** this is the Root SSL we need to put on the connector Page .



Paste the SSL from about page to the connector page as below, **continue**



Configuration for connector is finished as you get below page. Configuration all connectors **one by one** using the same **Root certificate** and **activation codes** you already have



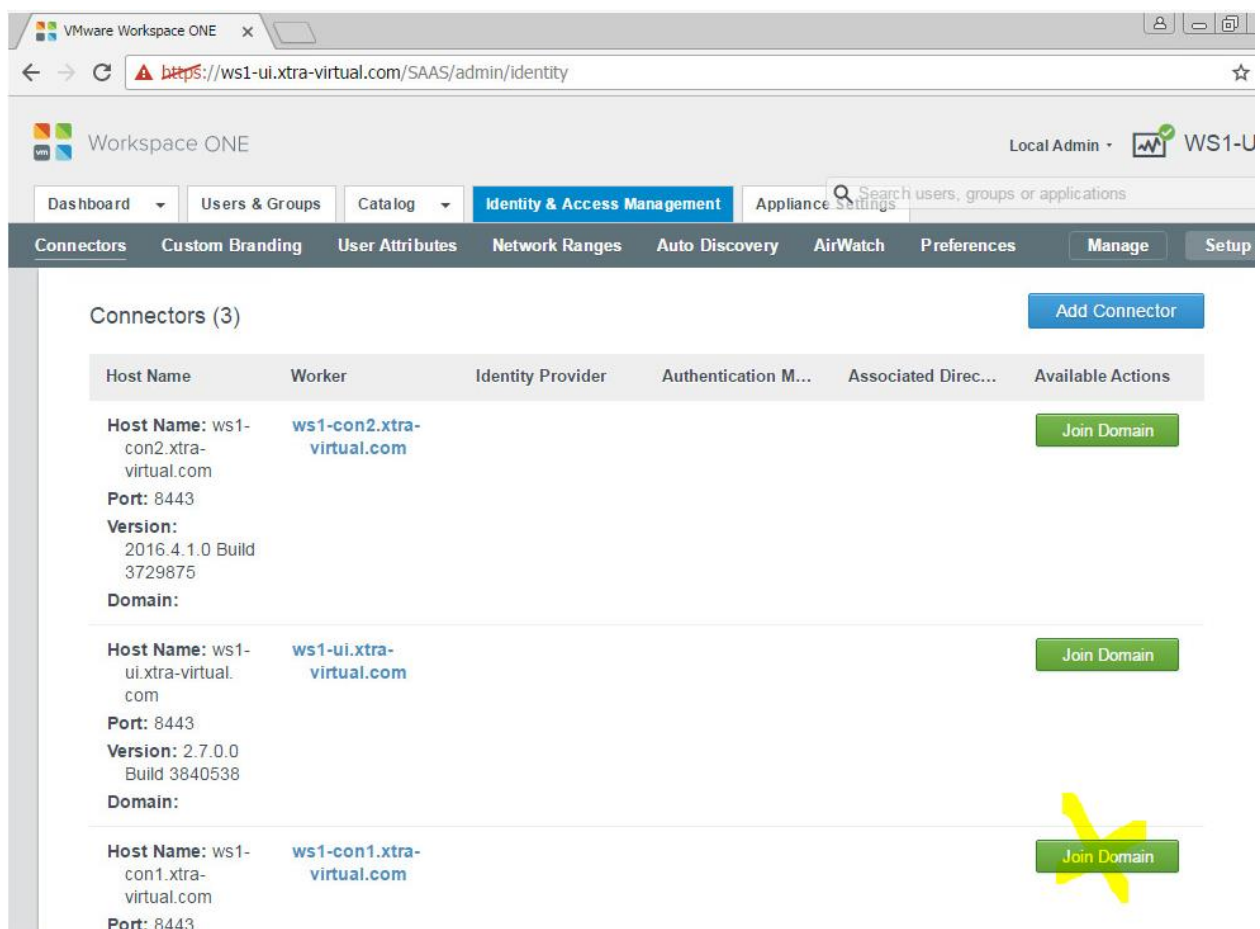
The screenshot shows a web browser window with three tabs: 'VMware Workspace ONE', 'VMware Identity Manager', and 'VMware Identity Manager'. The address bar shows the URL: <https://ws1-con1.xtra-virtual.com:8443/hc/3002/admin/wizard/directory/>. The page features the VMware logo in the top left and 'Help | Log out' in the top right. A left-hand navigation menu lists four steps: 'Get Started', 'Set Passwords', 'Activate Connector', and 'Setup Review', with 'Setup Review' selected. The main content area displays a large green checkmark icon, the heading 'Setup is complete', and the message 'You can now begin using the Service.' Below this, a section titled 'What to do next?' provides instructions: 'Log in to the administration console with the Local User admin (e.g. user@example.com) username and password. You will be directed to the Directories page. Click **Add Directory** to establish a connection to your Active Directory to sync users and groups to the directory.' It also lists 'Other tasks to do in Identity and Access Management' with four bullet points: 'Enable additional authentication methods', 'Create access policies', 'Set network range of IP addresses', and 'Apply custom branding'.

Once User interface server and connections are configured we need to configure which **Active directory** our instance should talk to so it can help users to authenticate for providing **single sign** services. follow steps below to configure directory services for **Workspace one** as below.

Adding Directory services to Workspace1 (Adding Active directory)

Click **setup** that will show you all connectors, we need to add one connector to domain as this will be our sync connector, this will sync users, groups and attributes from Active directory

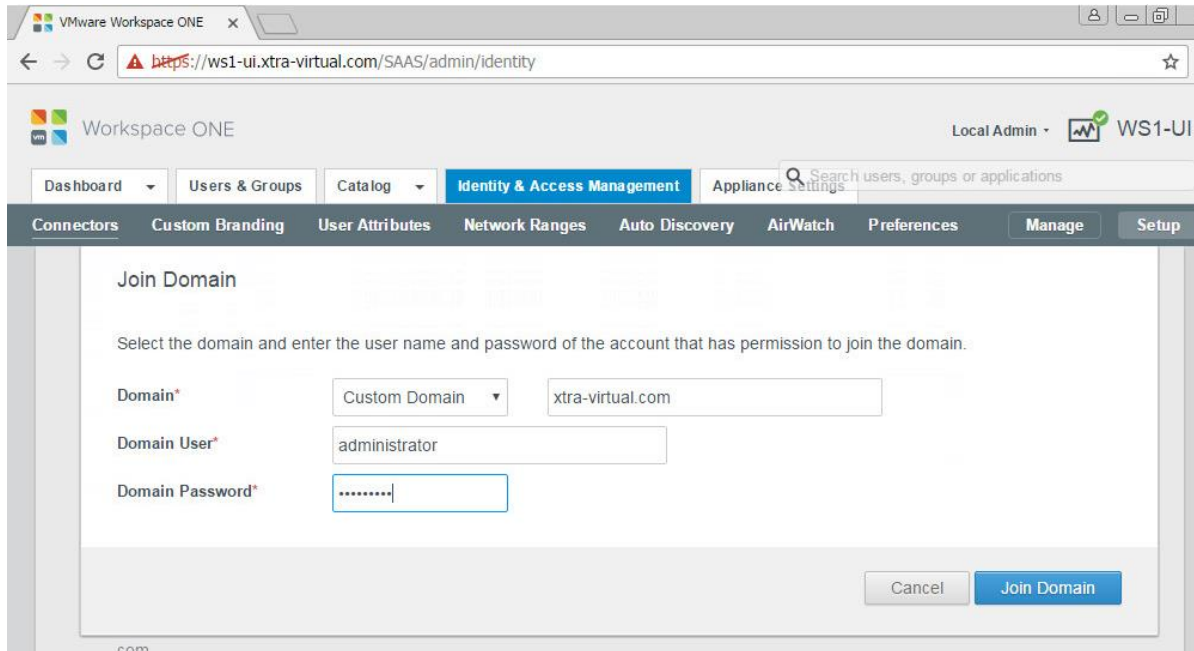
Once all connectors **registered / configured** it will show as below.



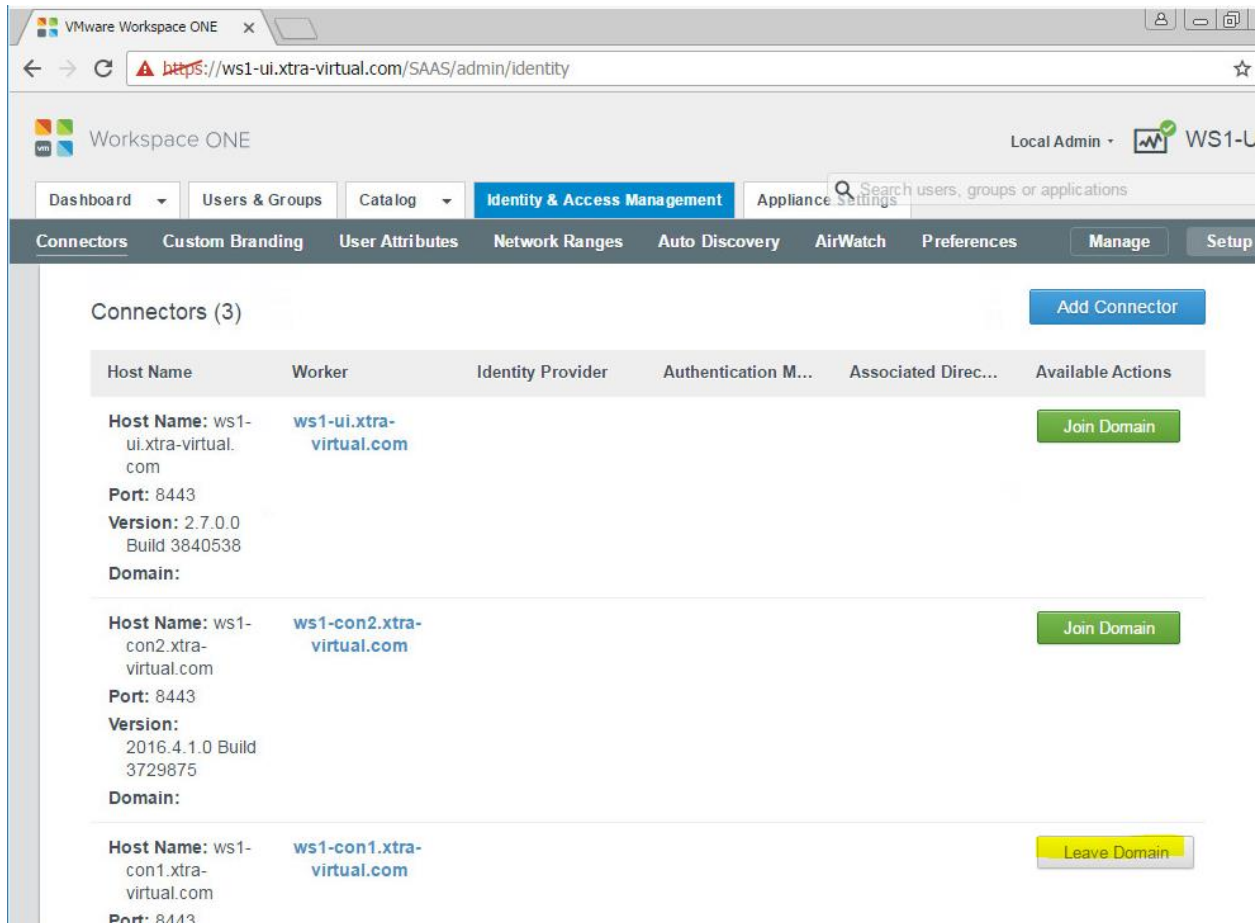
The screenshot shows the VMware Workspace ONE Identity & Access Management console. The browser address bar displays `https://ws1-ui.xtra-virtual.com/SAAS/admin/identity`. The navigation menu includes **Connectors**, **Custom Branding**, **User Attributes**, **Network Ranges**, **Auto Discovery**, **AirWatch**, **Preferences**, **Manage**, and **Setup**. The **Connectors** section is active, showing a list of three connectors. Each connector entry includes its Host Name, Worker, Identity Provider, Authentication Method, Associated Directory, and Available Actions. The **Join Domain** button for the third connector is highlighted with a yellow 'X'.

Host Name	Worker	Identity Provider	Authentication M...	Associated Direc...	Available Actions
Host Name: ws1-con2.xtra-virtual.com Port: 8443 Version: 2016.4.1.0 Build 3729875 Domain:	ws1-con2.xtra-virtual.com				Join Domain
Host Name: ws1-ui.xtra-virtual.com Port: 8443 Version: 2.7.0.0 Build 3840538 Domain:	ws1-ui.xtra-virtual.com				Join Domain
Host Name: ws1-con1.xtra-virtual.com Port: 8443	ws1-con1.xtra-virtual.com				Join Domain

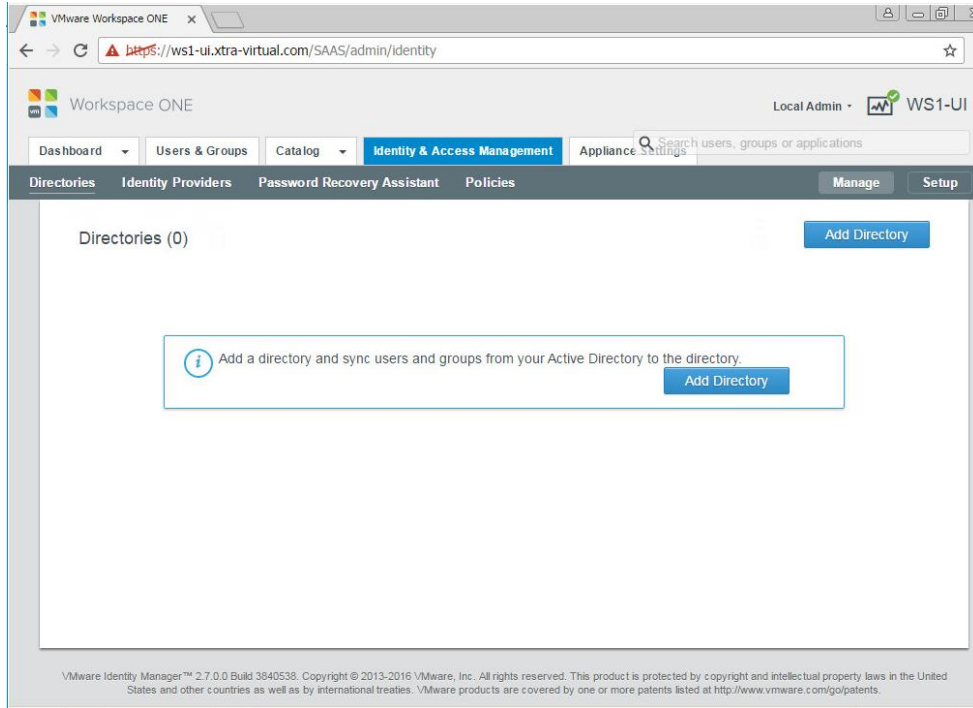
Hit **Join Domain** for any connector and provide **domain information** along with **username** and **password** to add that connector to the Domain.



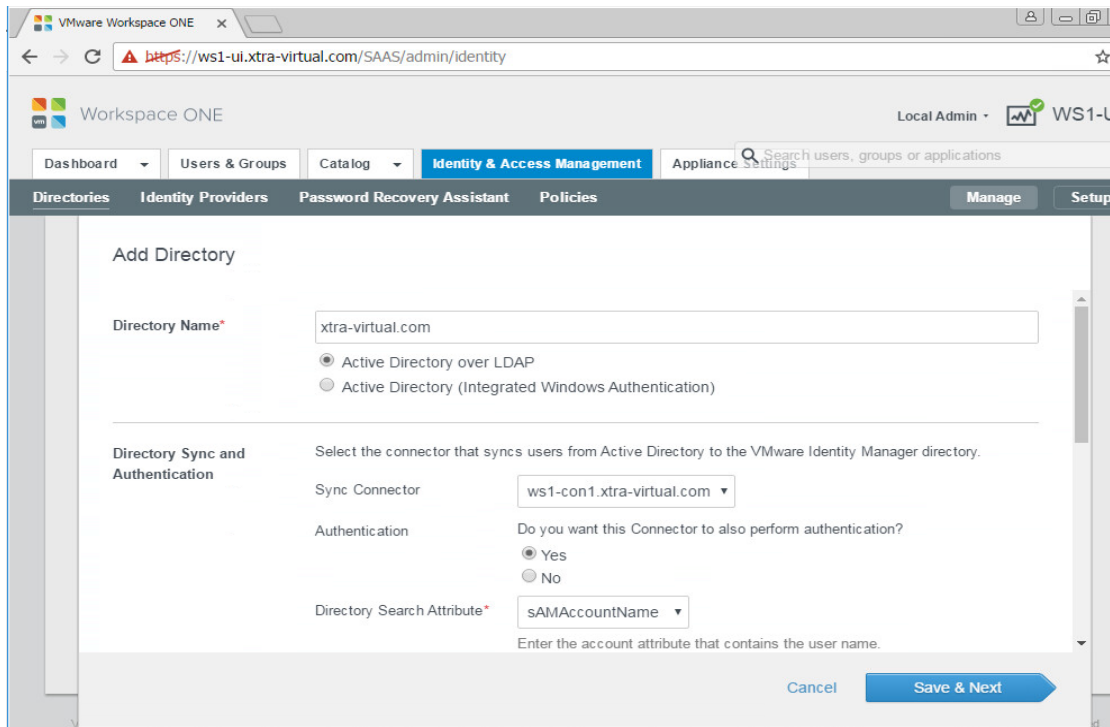
Connector once added looks as below



Now its time to **add directory services** and sync **users and groups**



Provide **Directory name**, select connector which is added to domain as **sync connector**



Select **Authentication** to be performed by **Connector**

VMware Workspace ONE

Local Admin - WS1-UI

Dashboard Users & Groups Catalog **Identity & Access Management** Appliance Search users, groups or applications

Directories Identity Providers Password Recovery Assistant Policies Manage Setup

Add Directory

Certificates

If your Active Directory requires STARTTLS encryption, select the check box below and provide the Root CA certificate. If there is more than one Root CA certificate, add all the certificates one after another. Make sure each certificate is in the PEM format with the delimiter lines 'BEGIN CERTIFICATE' and 'END CERTIFICATE'.

This Directory requires all connections to use STARTTLS

Bind User Details

In the Base DN field, enter DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. In the Bind DN field, enter the account that can search for users. For example, CN=user1,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Base DN*

Bind DN*

Bind DN Password* **Test Connection**

Enter your Active Directory bind account password.

Cancel **Save & Next**

States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

Click **Test Connection** to confirm password and once verified click **Save & Next**

VMware Workspace ONE

Local Admin - WS1-UI

Dashboard Users & Groups Catalog **Identity & Access Management** Appliance Search users, groups or applications

Directories Identity Providers Password Recovery Assistant Policies Manage Setup

Add Directory

Connection is successful.

Certificates

If your Active Directory requires STARTTLS encryption, select the check box below and provide the Root CA certificate. If there is more than one Root CA certificate, add all the certificates one after another. Make sure each certificate is in the PEM format with the delimiter lines 'BEGIN CERTIFICATE' and 'END CERTIFICATE'.

This Directory requires all connections to use STARTTLS

Bind User Details

In the Base DN field, enter DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. In the Bind DN field, enter the account that can search for users. For example, CN=user1,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Base DN*

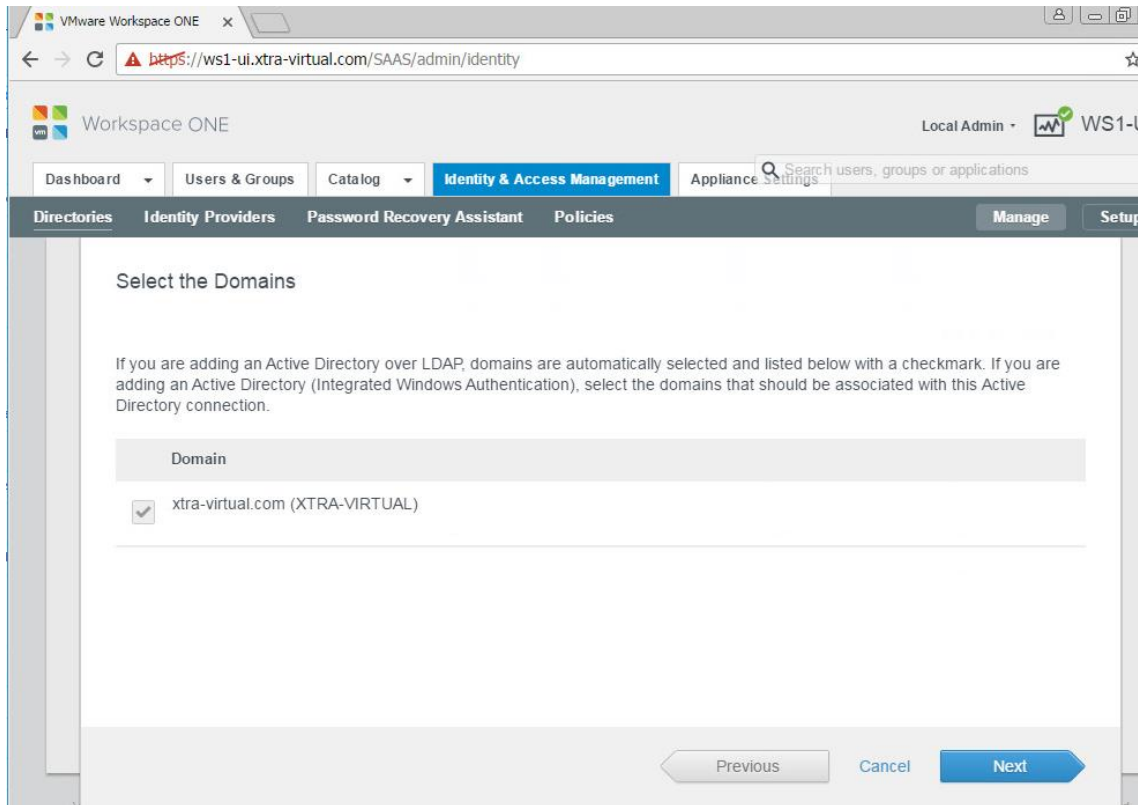
Bind DN*

Bind DN Password* **Test Connection**

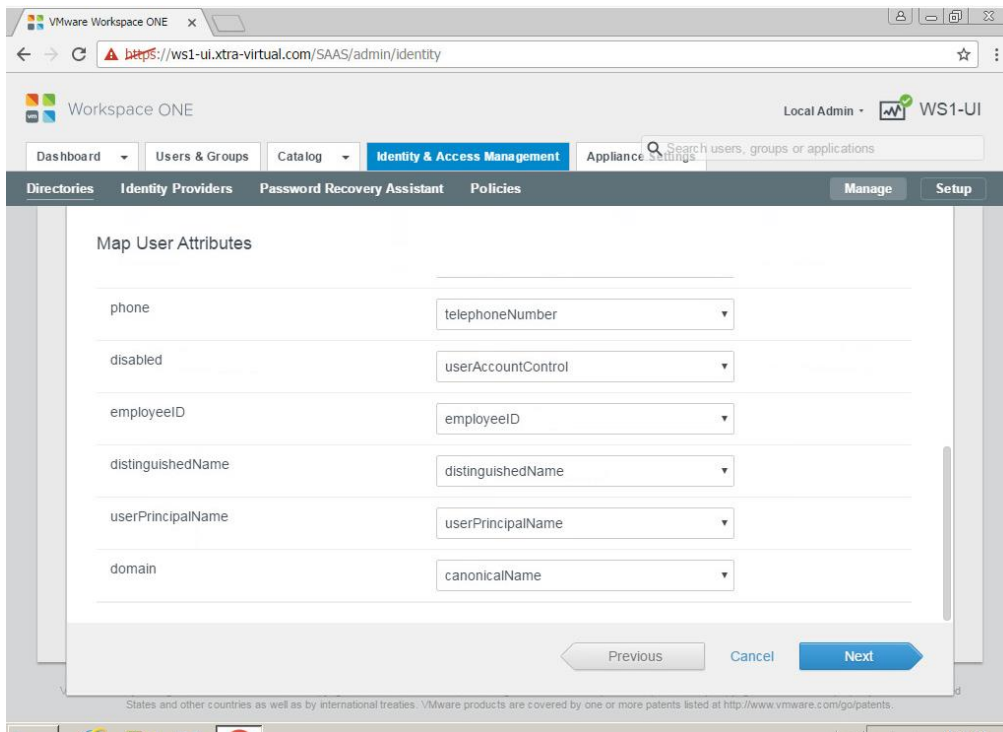
Enter your Active Directory bind account password.

Cancel **Save & Next**

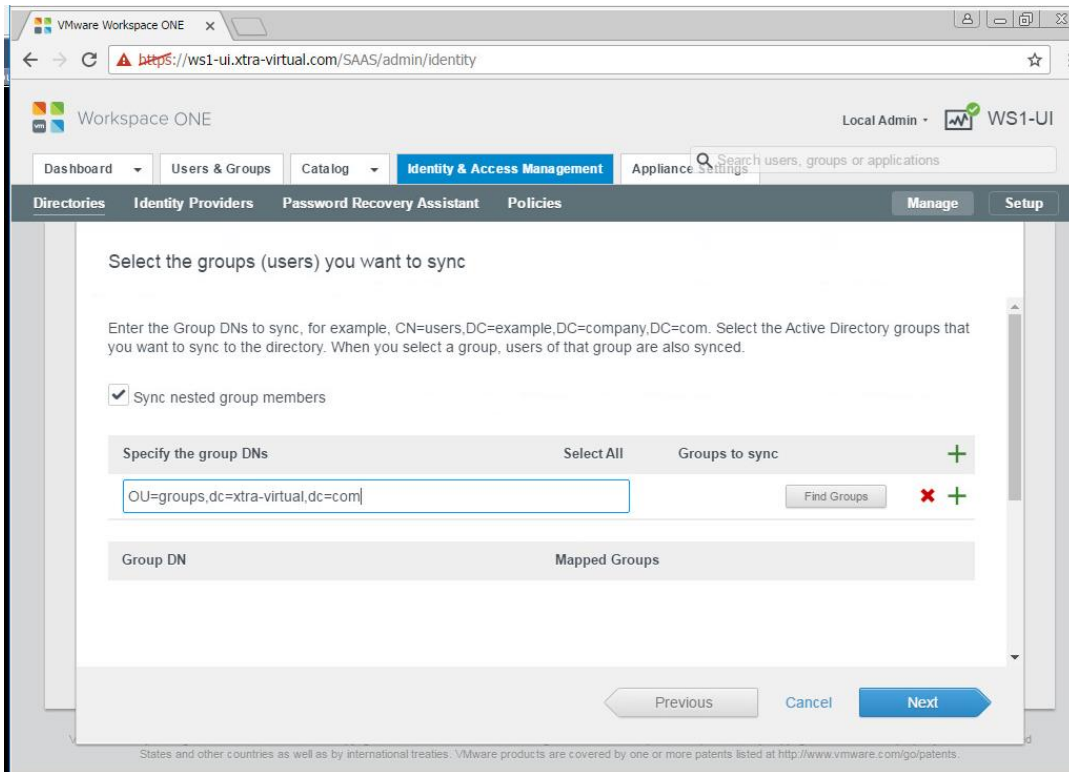
States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.



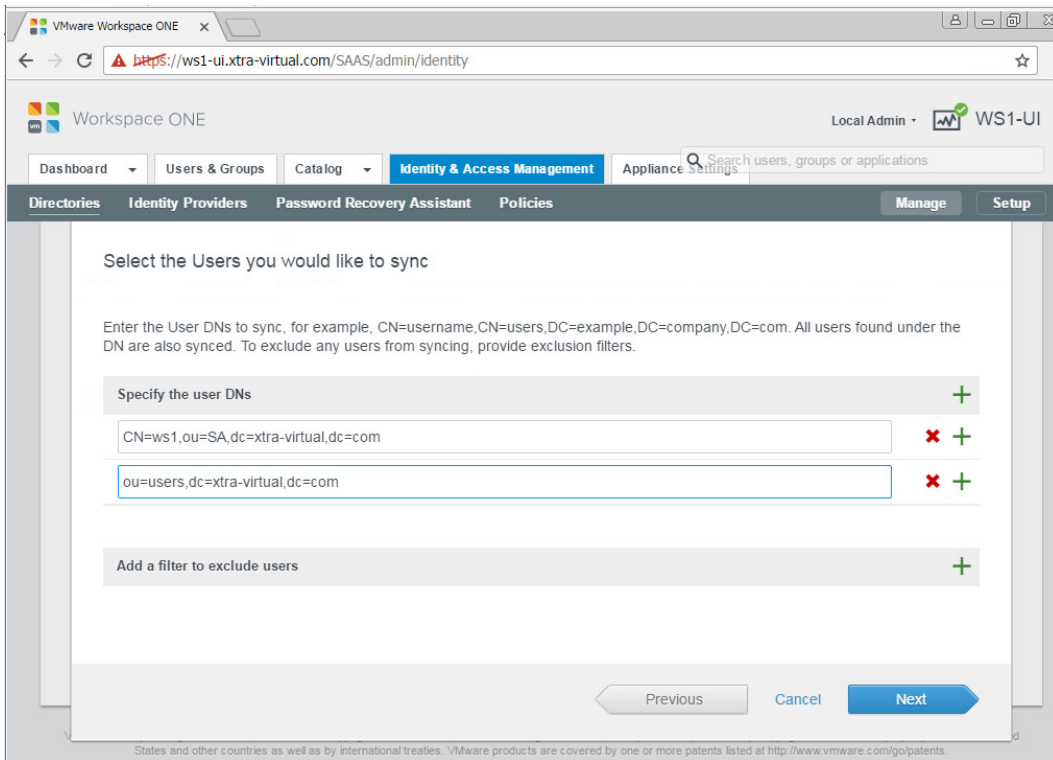
Make sure that right domain is checked there Click **Next**



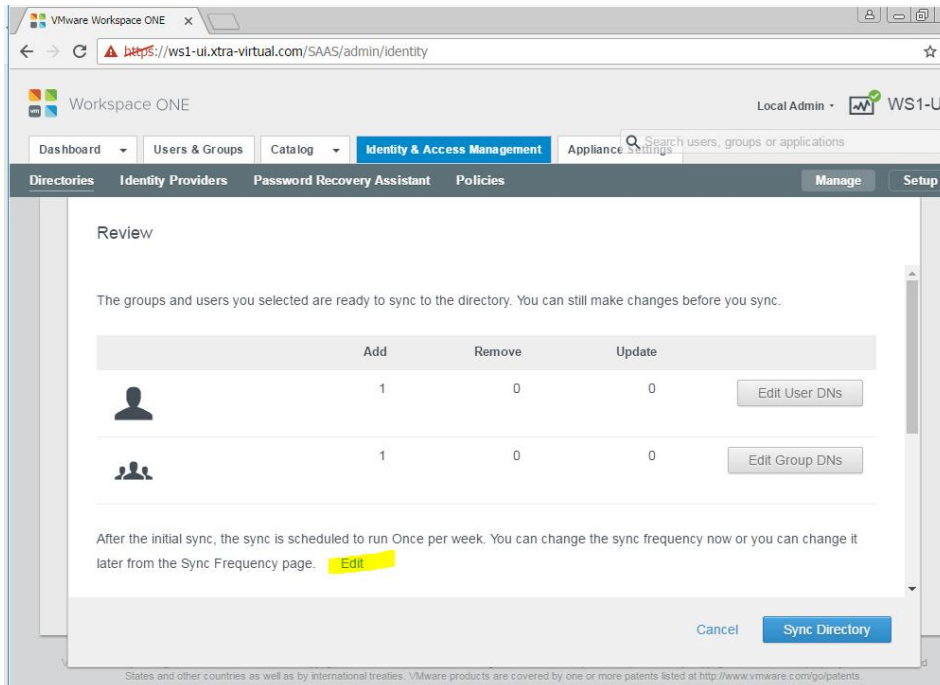
You may keep attributes selected as default and click **Next**



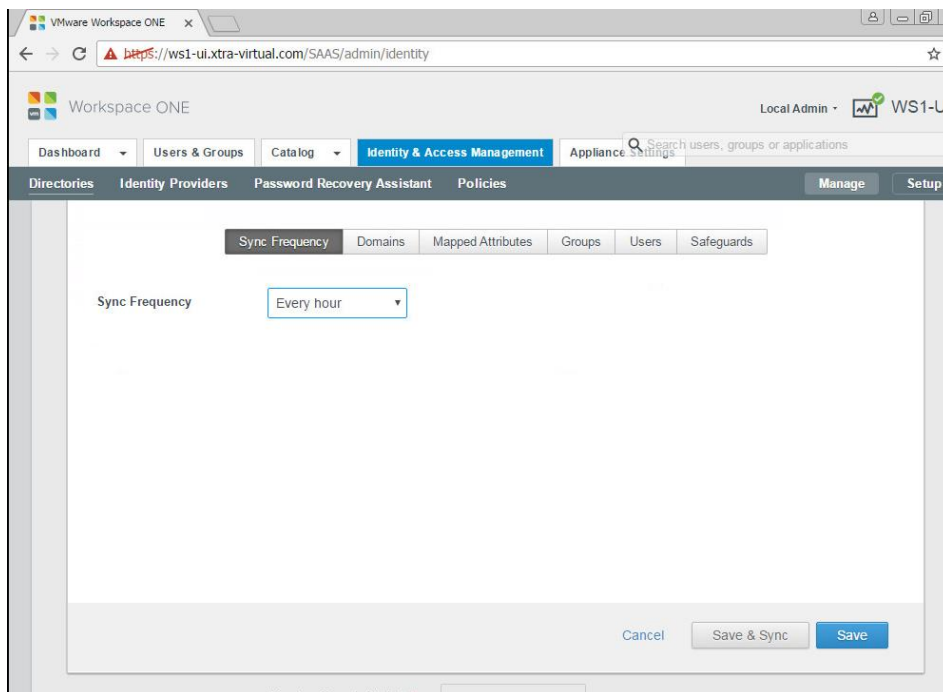
Select User and Group DNs from Active Directory that you want to sync



Click Next



Click Edit to select sync frequency for our case its **Every Hour**



Finally save and select **Save & Sync**. And Workspace one is ready after its syncs all users and groups, now you are ready to configure your applications!!!