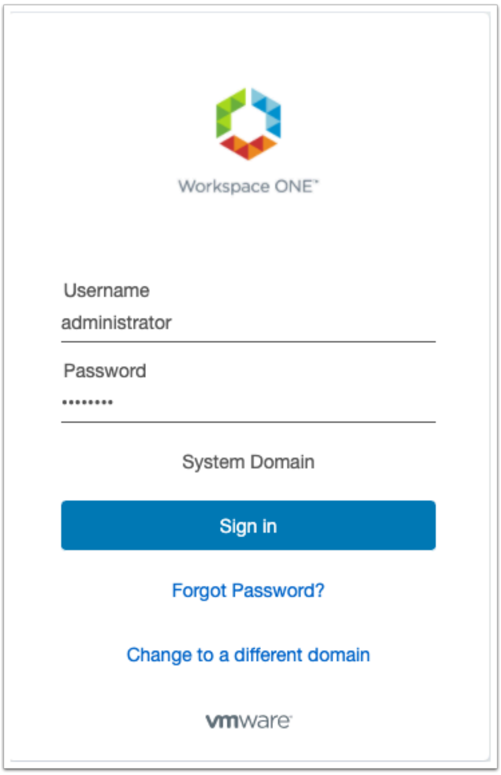
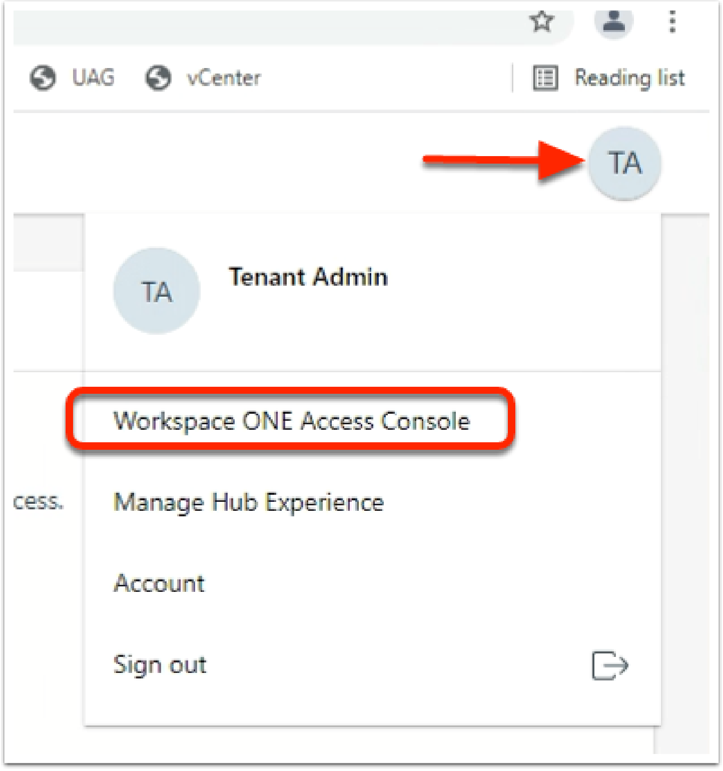
Chapter 1: Configuring the Workspace ONE Access and the AirWatch Cloud Connector

Part 1. Configuring the Workspace ONE Access Connector

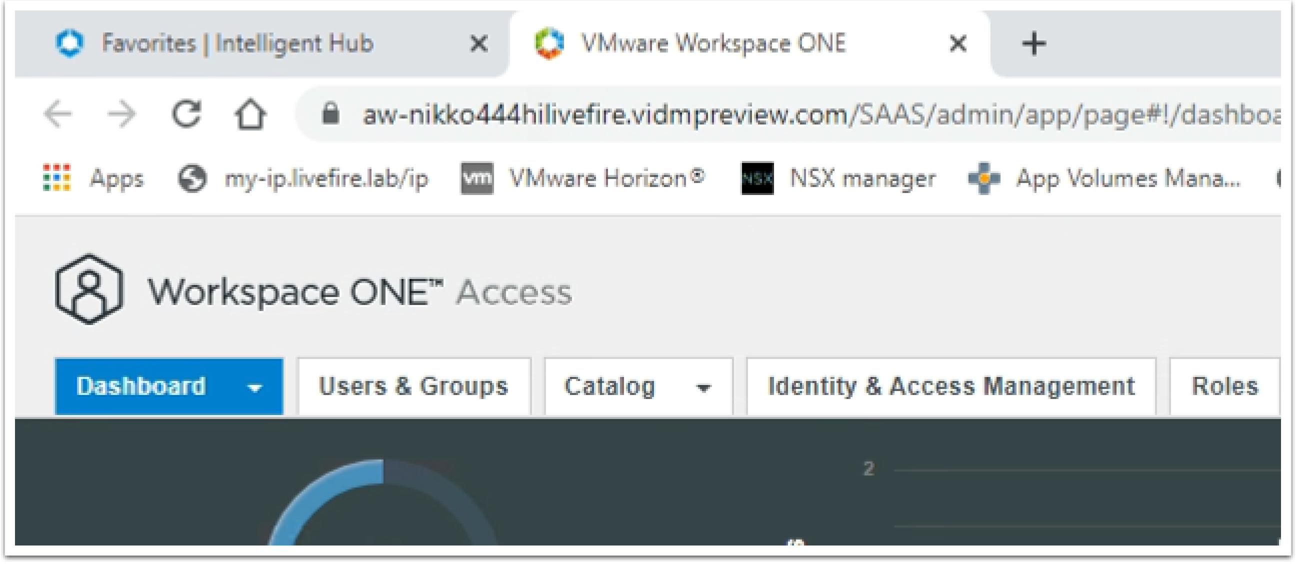
- We will be downloading a custom JSON for the Workspace ONE Access Connector



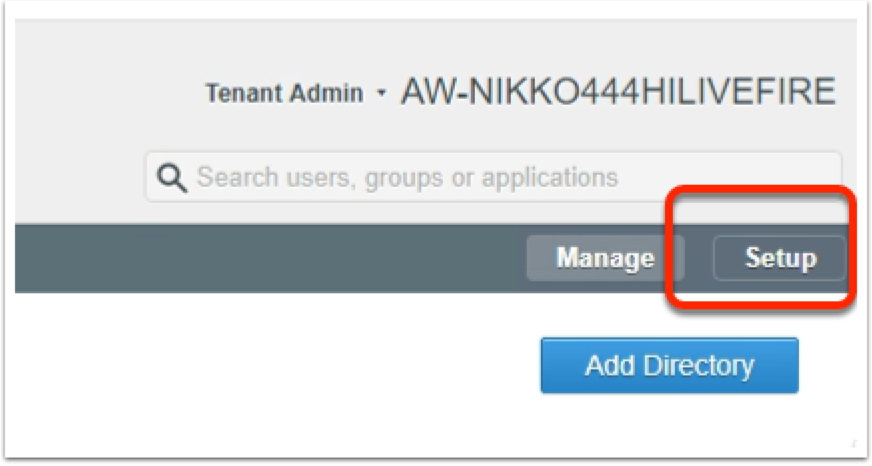
1. On your ControlCenter Server:
    - Open your **Chrome** browser
    - In the **Address bar**, enter your **custom Workspace ONE Access URL**
    - In the **Username** area, enter **system administrator name**
    - In the **Password** area, enter **your custom password**
    - Select **Sign In**



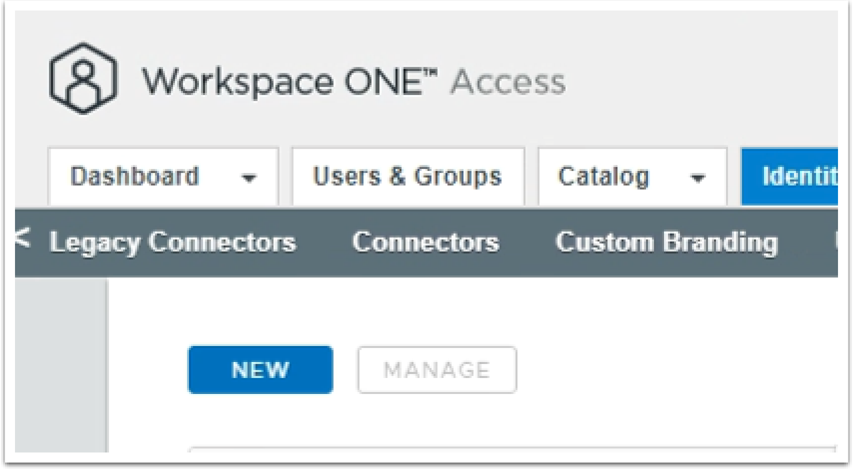
2. In the Web Intelligent Hub console
   - To the right, select and right click the **TA** icon
   - Select **Workspace ONE Access Console**



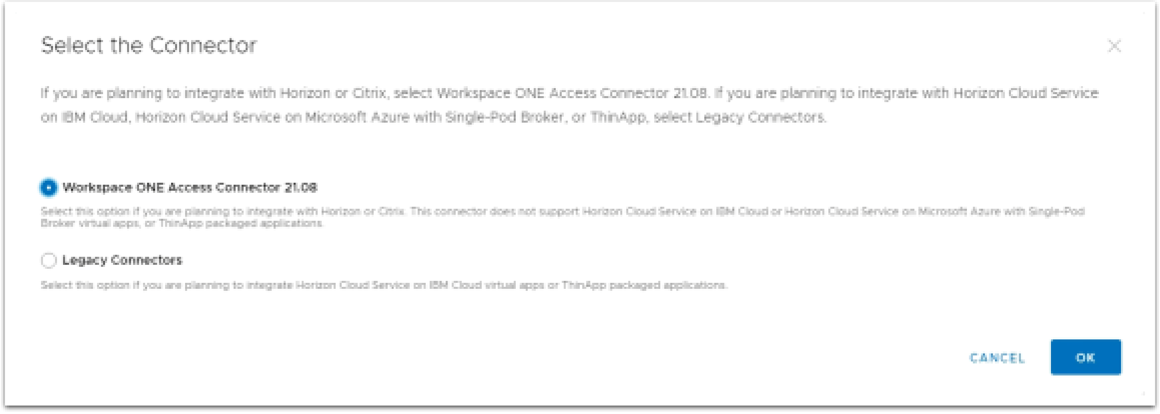
3. In the Workspace ONE Access Console
   - Select the **Identity & Access Management** tab



4. In the Workspace ONE Access Console
   - Select **Setup**



5. In the **Workspace ONE Access Console** > **Setup** area
   - Select **NEW**



Select the Connector

If you are planning to integrate with Horizon or Citrix, select Workspace ONE Access Connector 21.08. If you are planning to integrate with Horizon Cloud Service on IBM Cloud, Horizon Cloud Service on Microsoft Azure with Single-Pod Broker, or ThinApp, select Legacy Connectors.

● Workspace ONE Access Connector 21.08

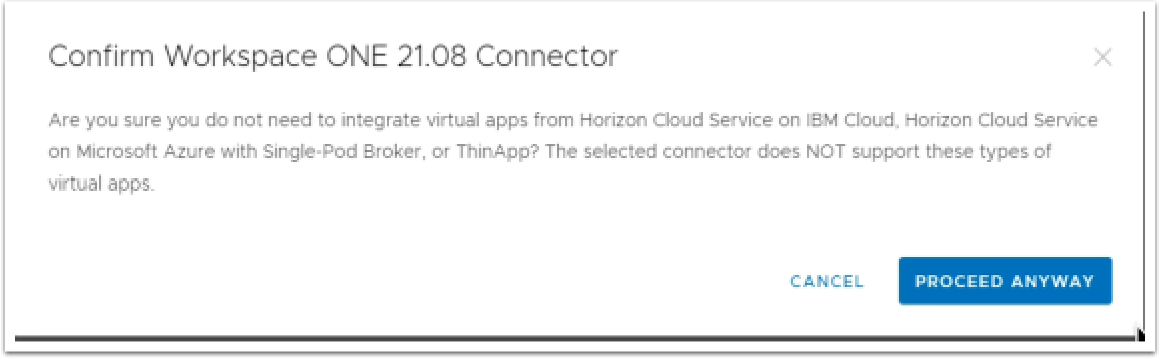
Select this option if you are planning to integrate with Horizon or Citrix. This connector does not support Horizon Cloud Service on IBM Cloud or Horizon Cloud Service on Microsoft Azure with Single-Pod Broker virtual apps, or ThinApp packaged applications.

○ Legacy Connectors

Select this option if you are planning to integrate Horizon Cloud Service on IBM Cloud virtual apps or ThinApp packaged applications.

CANCEL OK

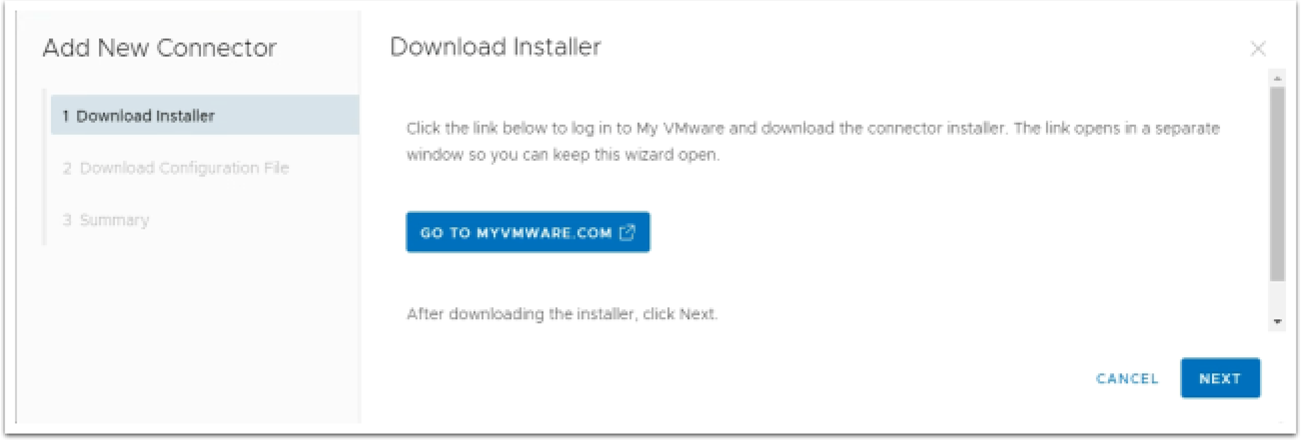
6. In the **Workspace ONE Access Console** > **Setup** area > **Select the Connector** window
   - Select the **radio button** next to **Workspace ONE Access Connector 21.08**
   - Select **OK**



Confirm Workspace ONE 21.08 Connector

Are you sure you do not need to integrate virtual apps from Horizon Cloud Service on IBM Cloud, Horizon Cloud Service on Microsoft Azure with Single-Pod Broker, or ThinApp? The selected connector does NOT support these types of virtual apps.

7. In the **Confirm Workspace ONE 21.08 Connector** window
   - Select **PROCEED ANYWAY**



Add New Connector

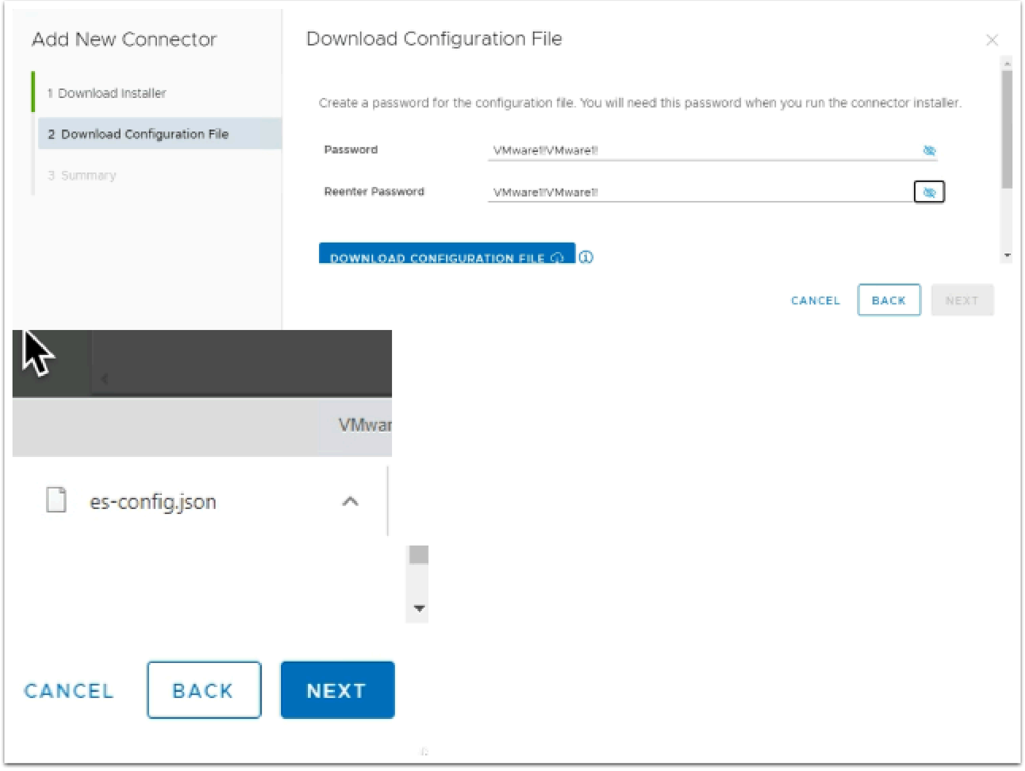
1 Download Installer
2 Download Configuration File
3 Summary

Download Installer

Click the link below to log in to My VMware and download the connector installer. The link opens in a separate window so you can keep this wizard open.

After downloading the installer, click Next.

8. In the **Add New Connector** window
   - Select **NEXT**



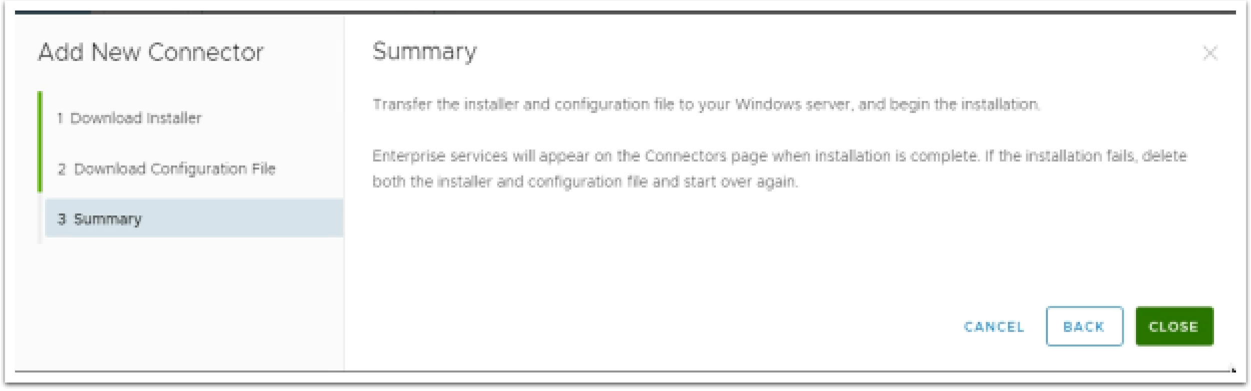
Download Configuration File

Create a password for the configuration file. You will need this password when you run the connector installer.

Password VMware1!VMware1!

Reenter Password VMware1!VMware1!

9. In the **Add New Connector** window
   - Next to **Password** , enter **VMware1!VMware1!**
   - Next to **Reenter Password**, enter **VMware1!VMware1!**
   - Select **DOWNLOAD CONFIGURATION FILE**
   - Note a **es-config.json** file should have downloaded
   - Select **NEXT**

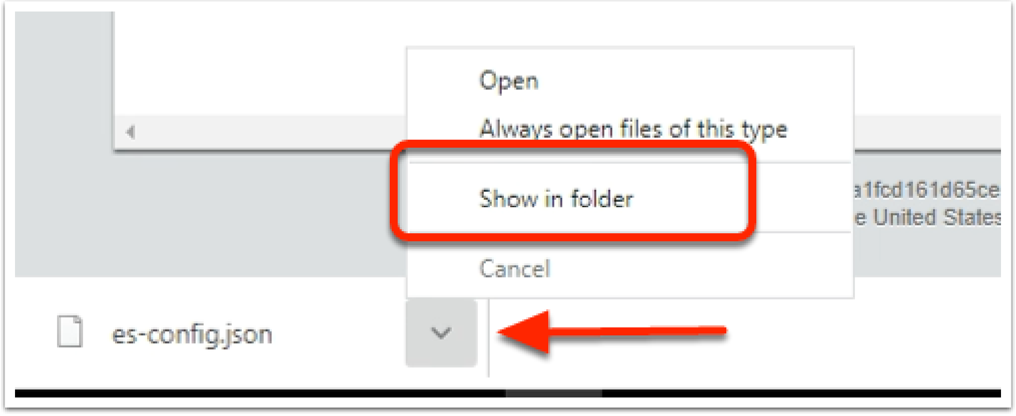


Summary

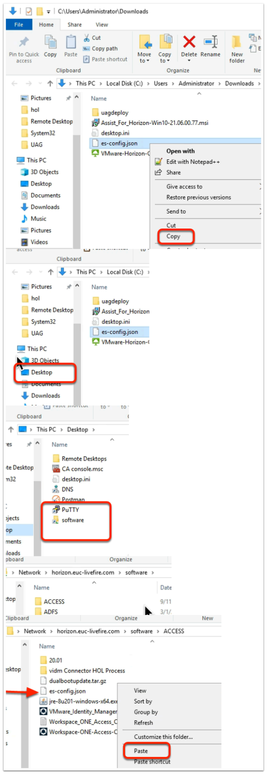
Transfer the installer and configuration file to your Windows server, and begin the installation.

Enterprise services will appear on the Connectors page when installation is complete. If the installation fails, delete both the installer and configuration file and start over again.

10. In the **Add New Connector/Summary** window
    - Select **CLOSE**



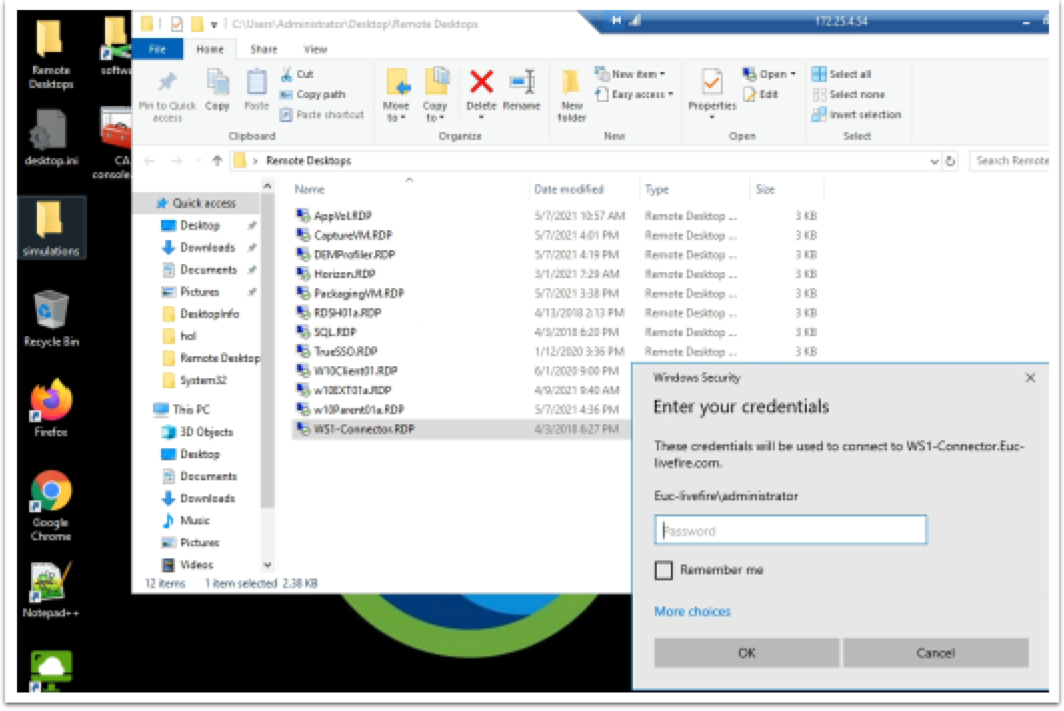
11. On your ControlCenter server
    - Select the **dropdown Icon** next to your **json** download
    - Select **Show in folder**



12. In the **Downloads** folder
    - Select and right-click the **es-config.json** file
    - Select **Copy**
    - In the **File Explorer** Inventory, select **Desktop**
    - Under **Desktop**, select the **software** shortcut
    - Under **Software**, open the **ACCESS** folder
    - In the **ACCESS** folder, Paste the **es-config.json** file

Part 2. Installing and Configuring the Workspace ONE

Access Connector



Name	Date modified	Type	Size
AppVol.RDP	5/7/2021 10:57 AM	Remote Desktop ...	3 KB
CaptureVM.RDP	5/7/2021 4:01 PM	Remote Desktop ...	3 KB
DEMProfiler.RDP	5/7/2021 4:19 PM	Remote Desktop ...	3 KB
Horizon.RDP	3/1/2021 7:29 AM	Remote Desktop ...	3 KB
PackagingVM.RDP	5/7/2021 3:38 PM	Remote Desktop ...	3 KB
RDSH01a.RDP	4/13/2018 2:13 PM	Remote Desktop ...	3 KB
SQL.RDP	4/3/2018 6:20 PM	Remote Desktop ...	3 KB
TrueSSO.RDP	1/12/2020 3:36 PM	Remote Desktop ...	3 KB
W10Client01.RDP	6/1/2020 9:00 PM		
w10EXT01a.RDP	4/9/2021 9:40 AM		
w10Parent01a.RDP	5/7/2021 4:36 PM		
WS1-Connector.RDP	4/3/2018 6:27 PM		

Windows Security

Enter your credentials

These credentials will be used to connect to WS1-Connector.Euc-livefire.com.

Euc-livefire\administrator

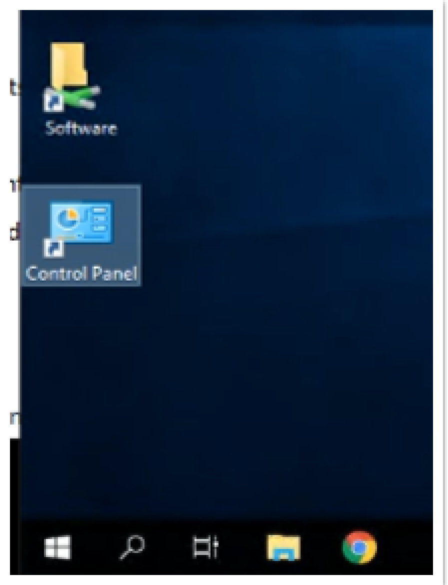
Password

□ Remember me

More choices

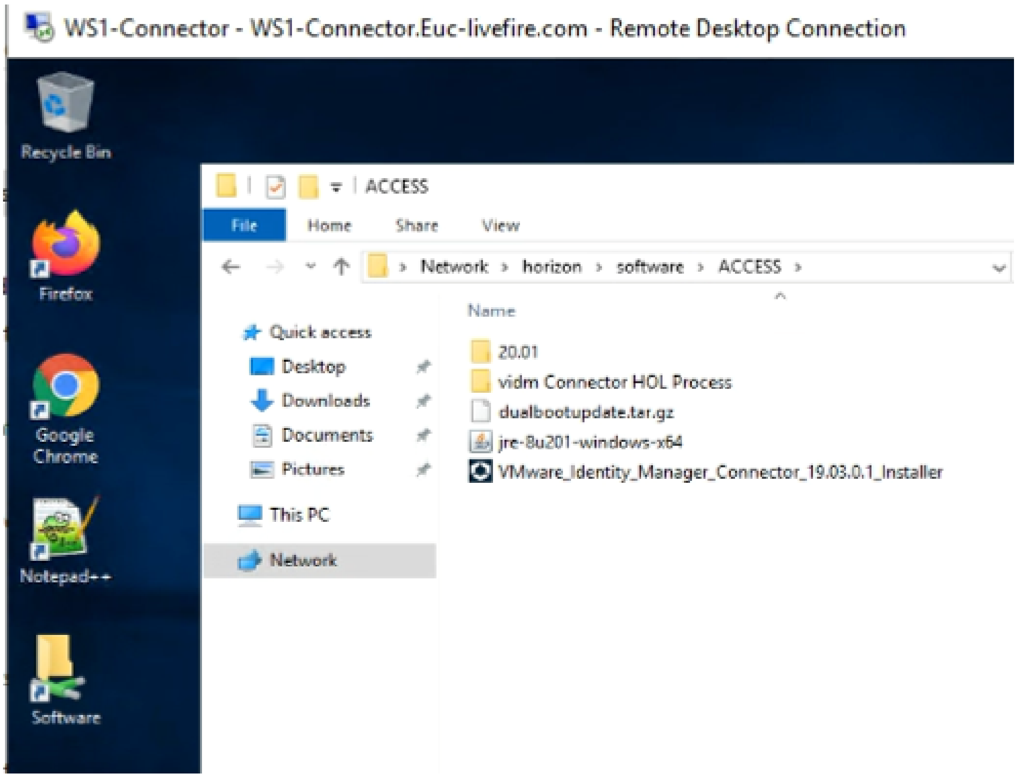
OK Cancel

1. On your **ControlCenter** server
   - On your desktop select your **Remote Desktops** folder
   - Select and launch your **WS1-Connector.RDP** shortcut.
     - **If prompted** log in as
       - username **administrator@euc-livefire.com**
       - password **VMware1!**

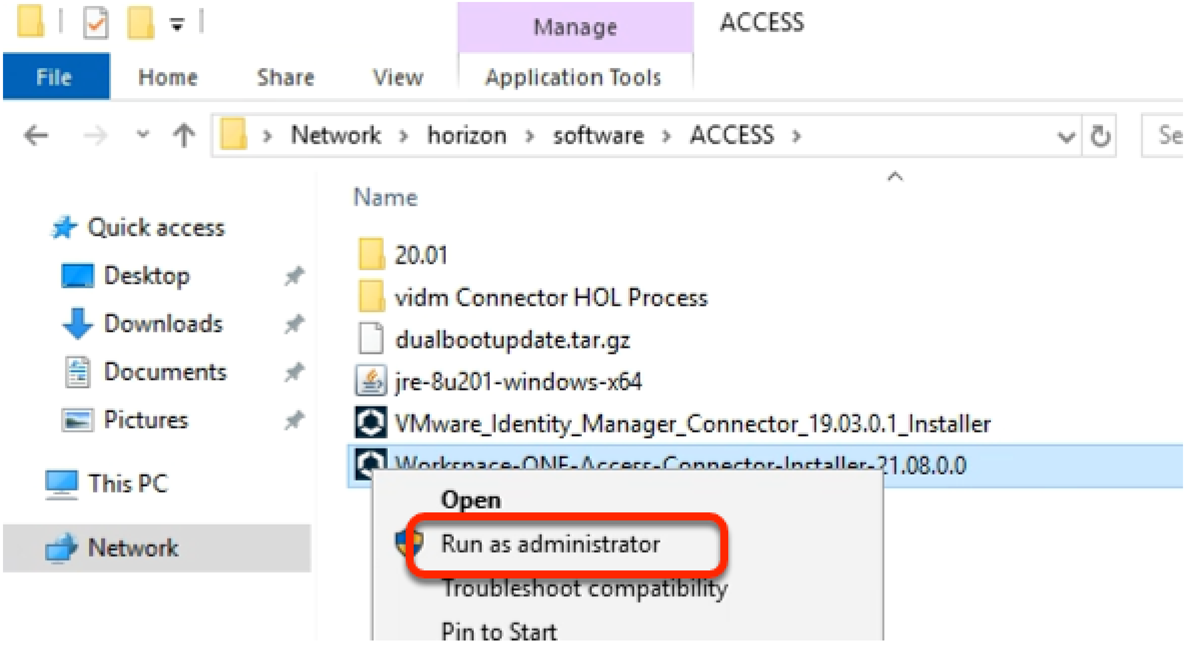


2. On the **WS1-Connector** server

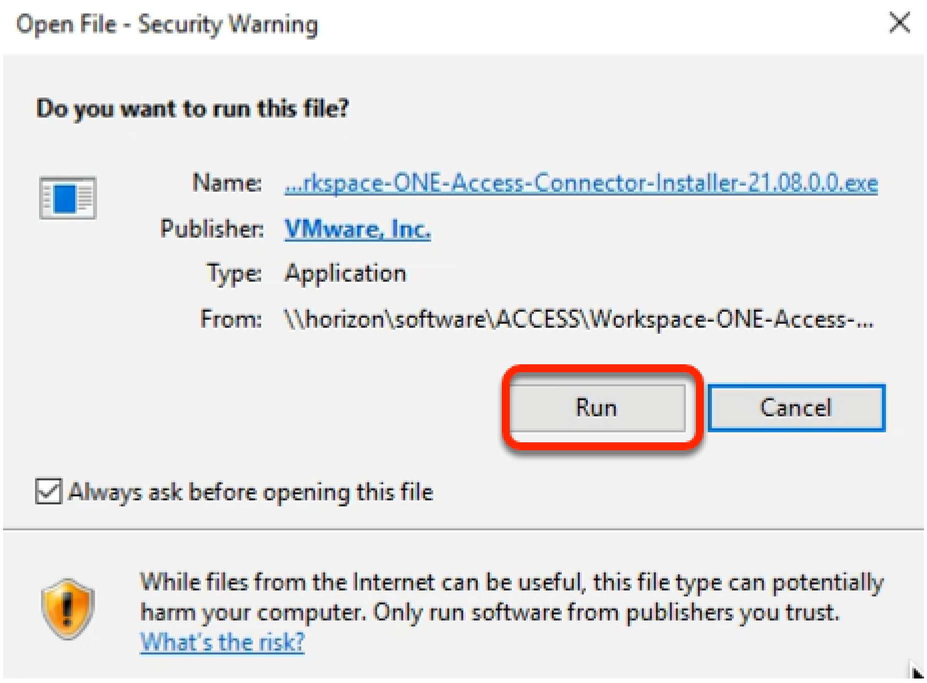
- On the Desktop, open the **Software** folder shortcut


WS1-Connector - WS1-Connector.Euc-livefire.com - Remote Desktop Connection
Recycle Bin
Firefox
Google Chrome
Notepad++
Software
ACCESS
File
Home
Share
View
Network › horizon › software › ACCESS ›
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
20.01
vidm Connector HOL Process
dualbootupdate.tar.gz
jre-8u201-windows-x64
VMware_Identity_Manager_Connector_19.03.0.1_Installer

3. On the **WS1-Connector** server
   - In the **software** network share, browse the **ACCESS** directory


Manage
ACCESS
File
Home
Share
View
Application Tools
Network › horizon › software › ACCESS ›
Se
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
20.01
vidm Connector HOL Process
dualbootupdate.tar.gz
jre-8u201-windows-x64
VMware_Identity_Manager_Connector_19.03.0.1_Installer
Workspace-ONE-Access-Connector-Installer-21.08.0.0
Open
Run as administrator
Troubleshoot compatibility
Pin to Start

4. In the **Access** folder
   - Select the **Workspace-ONE-Access-Connector-Installer-21.08.0.0.exe** installer
     - and **right-click,**
   - Select **Run as administrator**



Open File - Security Warning

Do you want to run this file?

Name: ...rkspace-ONE-Access-Connector-Installer-21.08.0.0.exe

Publisher: VMware, Inc.

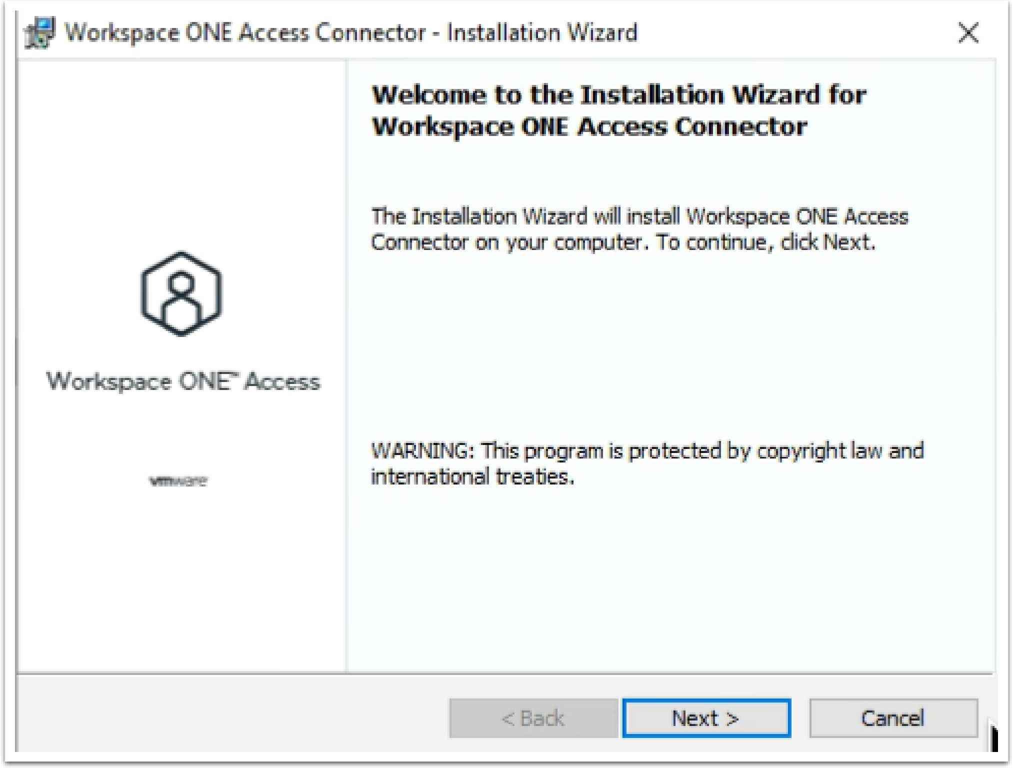
Type: Application

From: \\horizon\software\ACCESS\Workspace-ONE-Access-...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

5. In the **Open File - Security Warning** window
   - Select **Run**



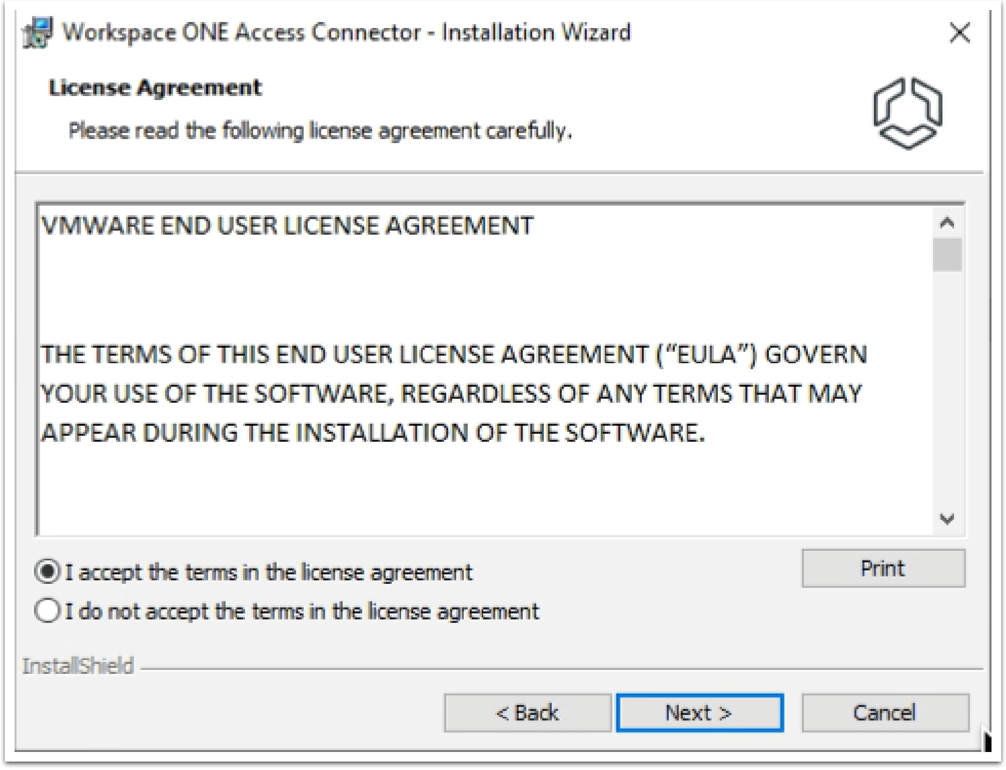
Workspace ONE Access Connector - Installation Wizard

Welcome to the Installation Wizard for Workspace ONE Access Connector

The Installation Wizard will install Workspace ONE Access Connector on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

6. On the **Workspace ONE Access Connector - Installation Wizard**
   - Select **Next**



Workspace ONE Access Connector - Installation Wizard

License Agreement

Please read the following license agreement carefully.

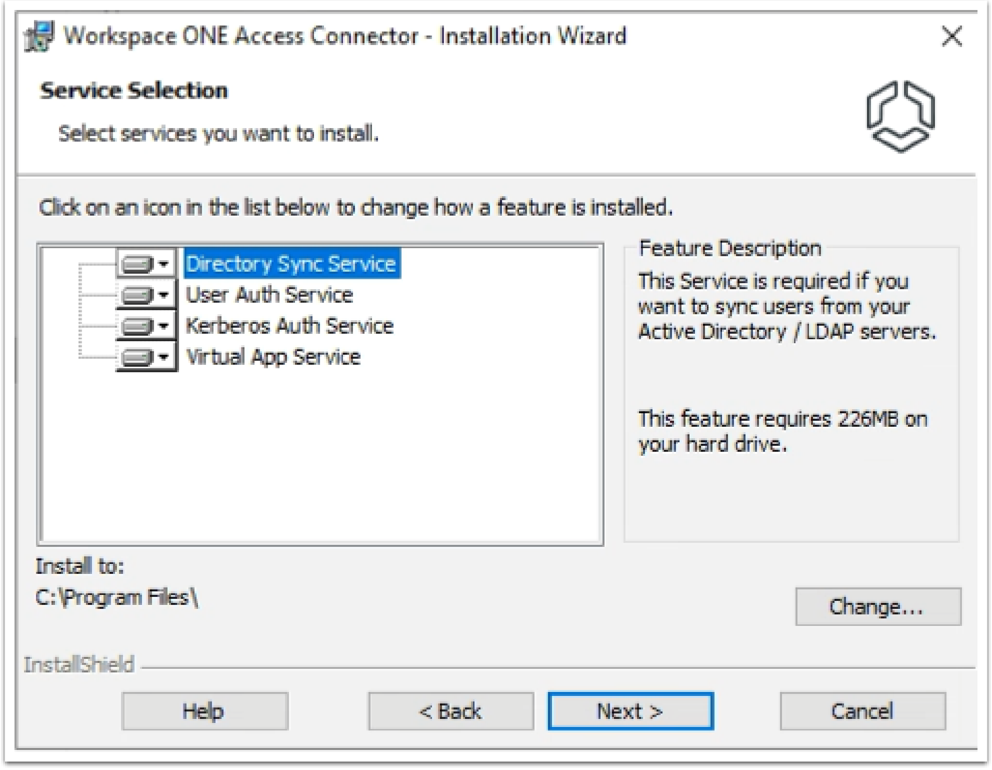
VMWARE END USER LICENSE AGREEMENT

THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA") GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

7. On the **Workspace ONE Access Connector- Installation Wizard - license agreement page**
   - Select **radio button** next to **I accept the terms in the license agreement**
   - Select **Next**



Workspace ONE Access Connector - Installation Wizard

Service Selection

Select services you want to install.

Click on an icon in the list below to change how a feature is installed.

- Directory Sync Service
- User Auth Service
- Kerberos Auth Service
- Virtual App Service

Feature Description

This Service is required if you want to sync users from your Active Directory / LDAP servers.

This feature requires 226MB on your hard drive.

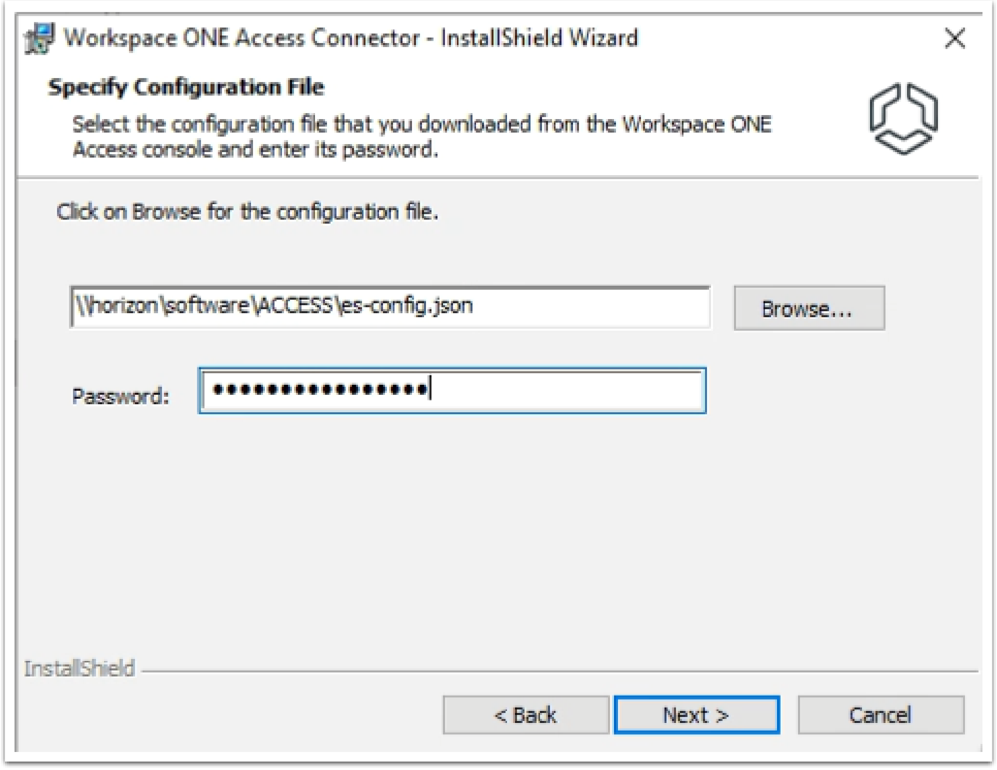
Install to:

C:\Program Files\

8. On the **Workspace ONE Access Connector- Installation Wizard**
   - Under **Service Selection**

    - Accept the Default (Note all services are installable by default)

- Select **Next**



Workspace ONE Access Connector - InstallShield Wizard

Specify Configuration File

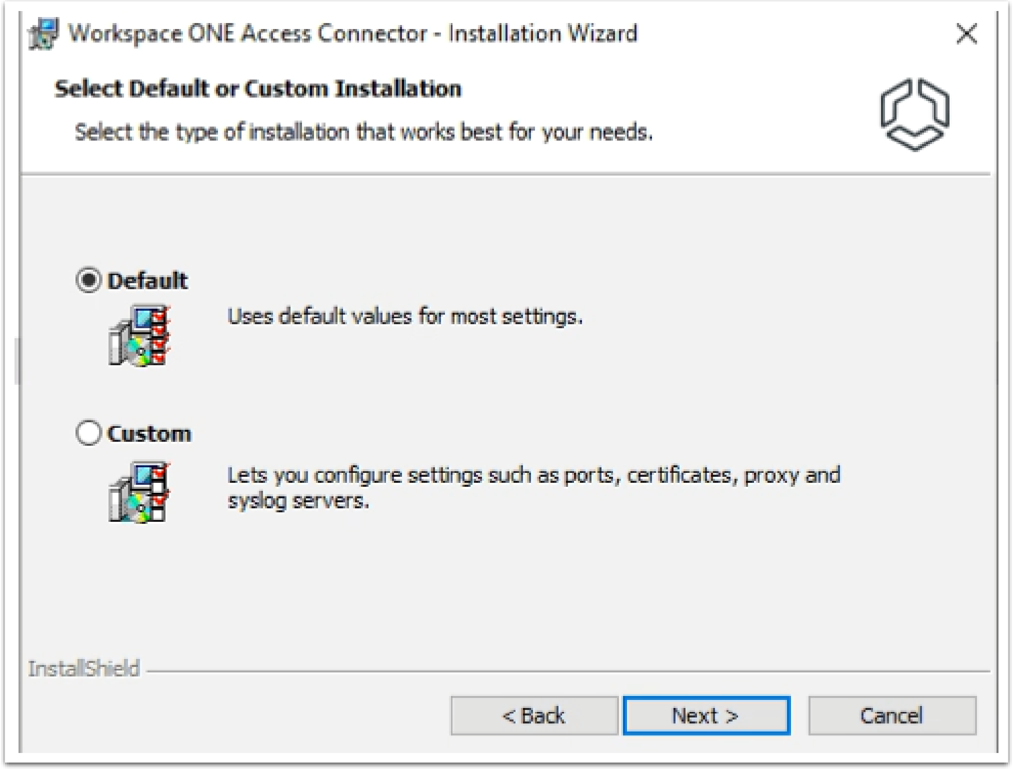
Select the configuration file that you downloaded from the Workspace ONE Access console and enter its password.

Click on Browse for the configuration file.

\\horizon\software\ACCESS\es-config.json

Password: •••••••••••••••••

9. On the **Workspace ONE Access Connector- InstallShield Wizard**
    - Under **Click on Browse for the configuration file.**
        - Enter **\\horizon\software\ACCESS\es-config.json**
    - Next to **Password:** enter **VMware1!VMware1!**
    - Select **Next**



Workspace ONE Access Connector - Installation Wizard

Select Default or Custom Installation

Select the type of installation that works best for your needs.

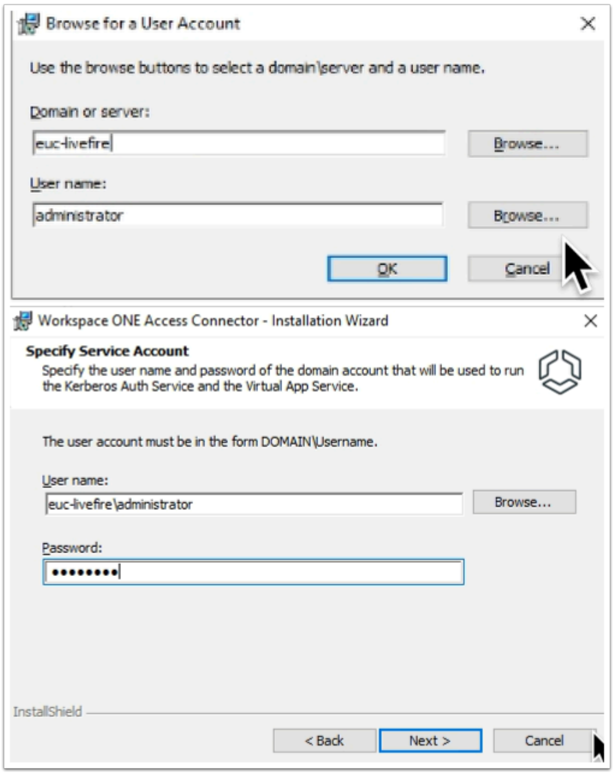
● **Default**

Uses default values for most settings.

○ **Custom**

Lets you configure settings such as ports, certificates, proxy and syslog servers.

10. **Workspace ONE Access Connector- Installation Wizard**
    - Accept the **Default**
    - Select **Next**



Browse for a User Account

Use the browse buttons to select a domain\server and a user name.

Domain or server: euc-livefire

User name: administrator

Workspace ONE Access Connector - Installation Wizard

Specify Service Account

Specify the user name and password of the domain account that will be used to run the Kerberos Auth Service and the Virtual App Service.

The user account must be in the form DOMAIN\Username.

User name: euc-livefire\administrator

Password: ••••••••

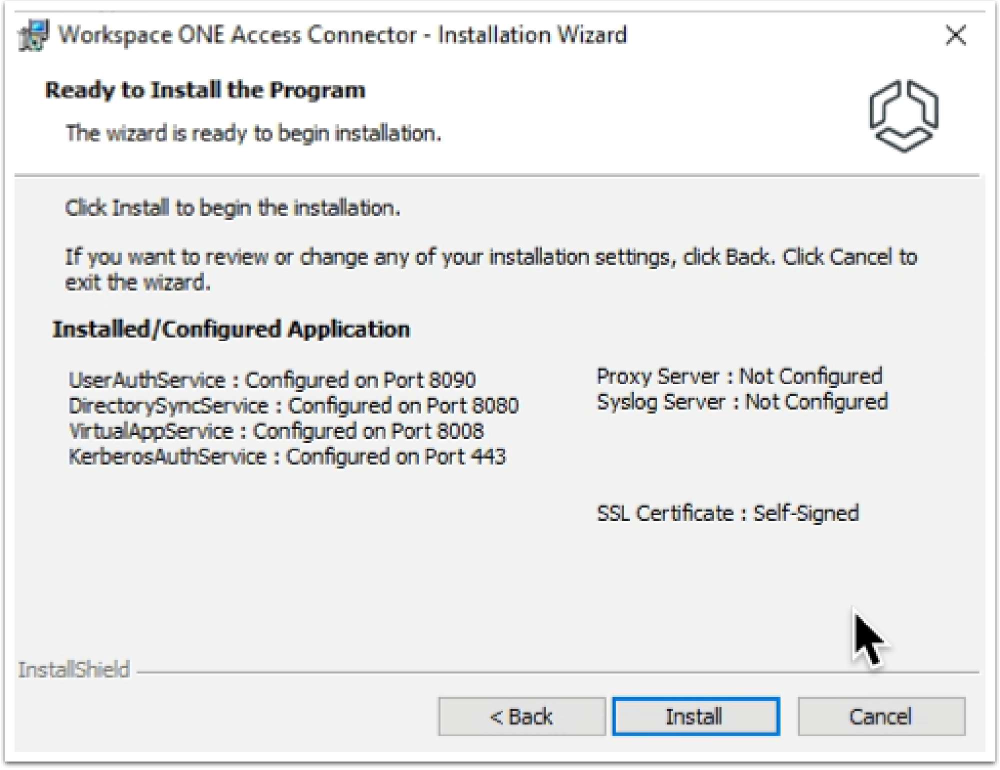
11. On the **Workspace ONE Access Connector- Installation Wizard**
    - Under **Domain or Server:** enter

    - **euc-livefire**

- Under **User name:** enter
    - **administrator**

- Select **OK**
- Under **Password:** enter
    - **VMware1!**

- Select **Next**



Workspace ONE Access Connector - Installation Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

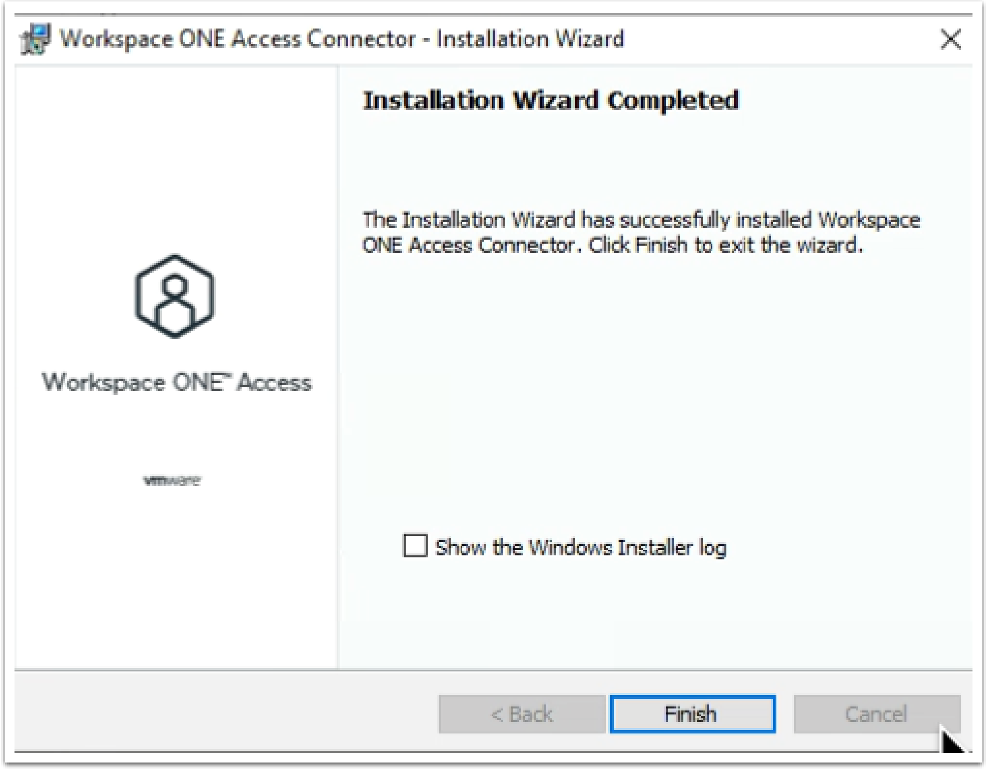
Installed/Configured Application

UserAuthService : Configured on Port 8090
DirectorySyncService : Configured on Port 8080
VirtualAppService : Configured on Port 8008
KerberosAuthService : Configured on Port 443

Proxy Server : Not Configured
Syslog Server : Not Configured

SSL Certificate : Self-Signed

12. On the **Workspace ONE Access Connector- Installation Wizard**
    - Select **Install**
        - The Installation takes about 7 min.

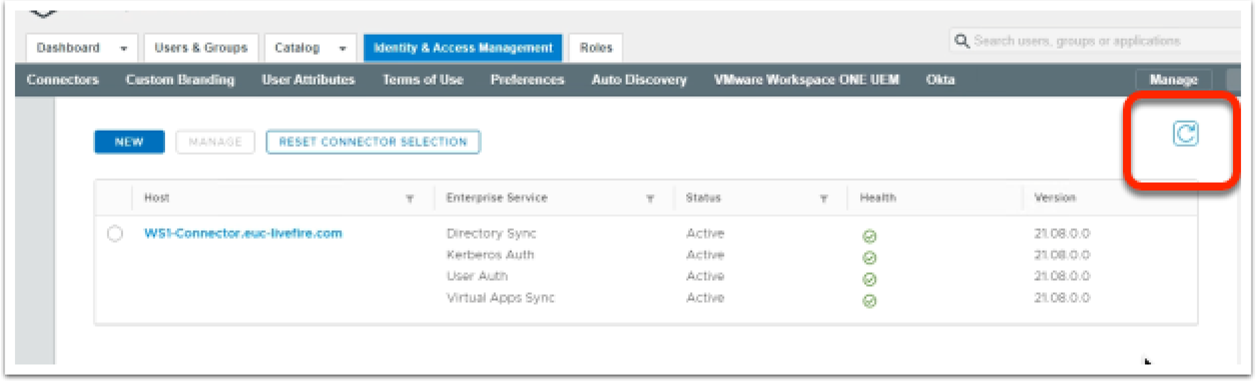


Installation Wizard Completed

The Installation Wizard has successfully installed Workspace ONE Access Connector. Click Finish to exit the wizard.

□ Show the Windows Installer log

13. On the **Workspace ONE Access Connector- Installation Wizard**
    - Select **Finish**

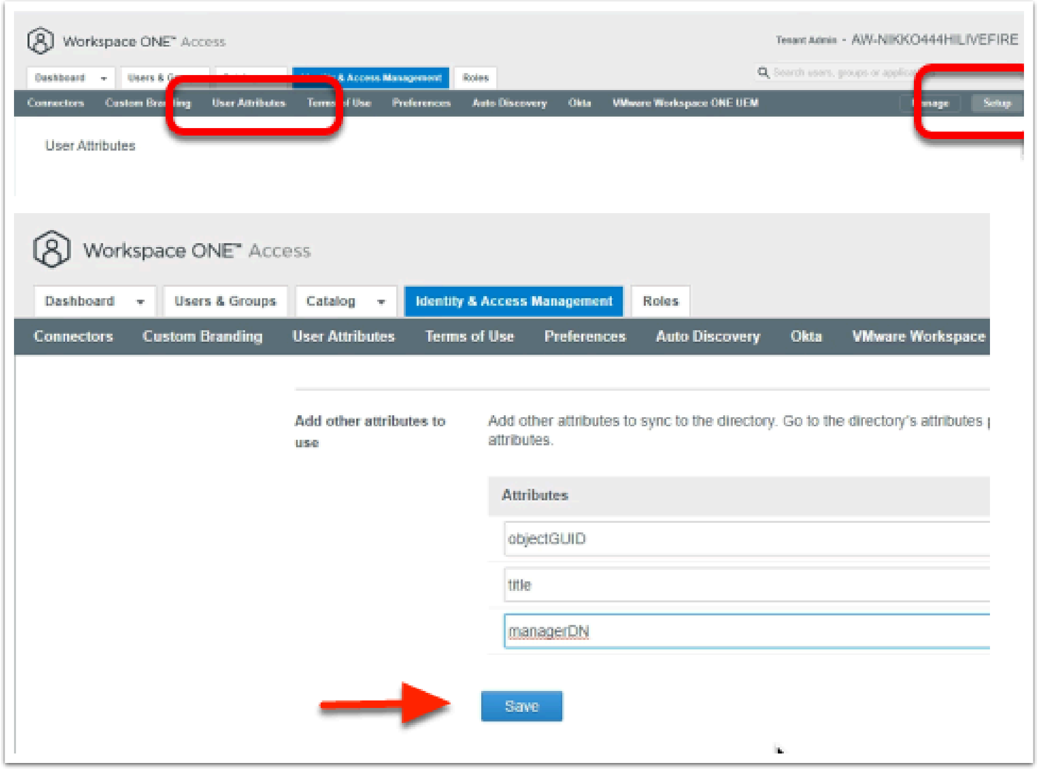


	Host	Enterprise Service	Status	Health	Version
○	WS1-Connector.euc-livefire.com	Directory Sync	Active	✓	21.08.0.0
		Kerberos Auth	Active	✓	21.08.0.0
		User Auth	Active	✓	21.08.0.0
		Virtual Apps Sync	Active	✓	21.08.0.0

14. On your ControlCenter server
    - Switch back to your **Workspace ONE Access Admin** console
    - Selet the **refresh** button to the right of your **Connectors** window
        - Note the Added connector with its associated Enterprise Services

Part 3 . Configuring Active Directory Sync

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



Add other attributes to use

Add other attributes to sync to the directory. Go to the directory's attributes
attributes.

Attributes

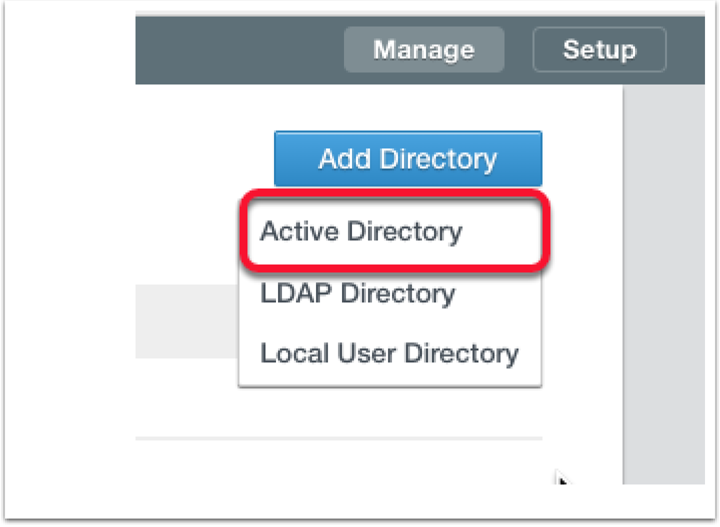
objectGUID

title

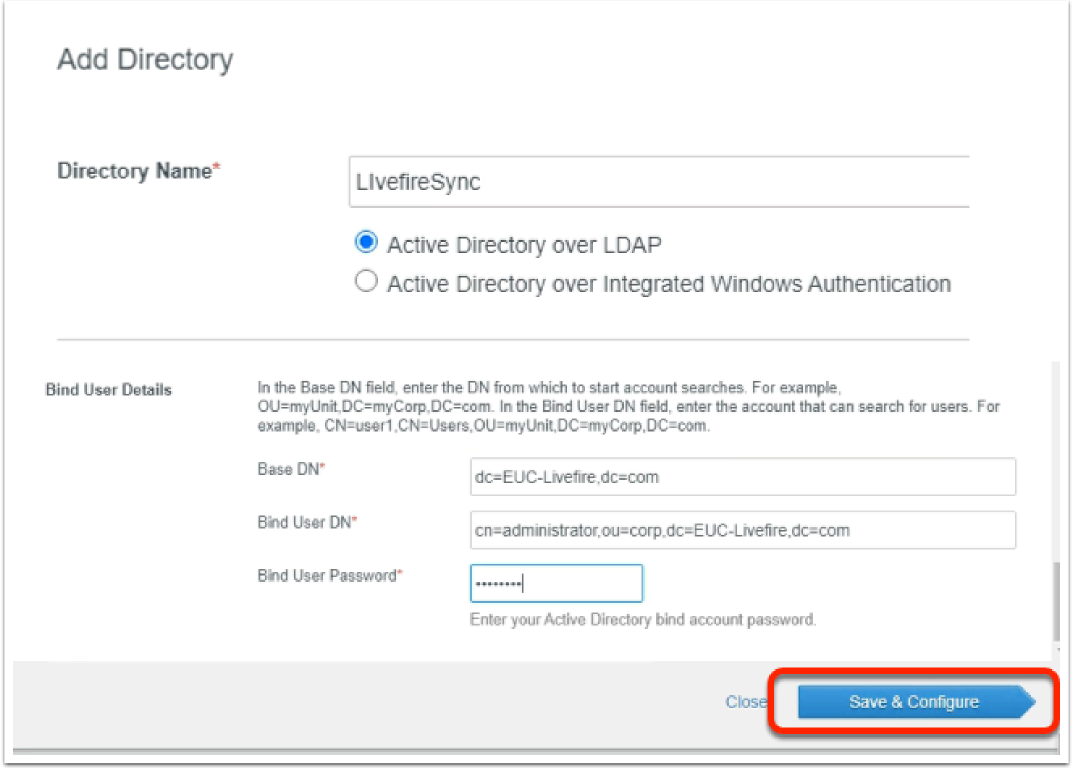
managerDN

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.
   - Set the attribute **distinguishedName** and **userPrincipalName** to **Required**
   - Under Attributes to the right select the **Green Plus** (+) Add the following additional attributes (case sensitive) :
     - **objectGUID**
     - **title**
     - **managerDN**
   - Select **Save**



2. Configuring AD-sync configuration with Workspace ONE Access.
   - To the right of the screen select **Manage**, select **Directories**
   - Select **Add Directory** > **Active Directory**



Add Directory

Directory Name* LIvefireSync

● Active Directory over LDAP
○ Active Directory over Integrated Windows Authentication

Bind User Details

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

Base DN* dc=EUC-Livefire,dc=com

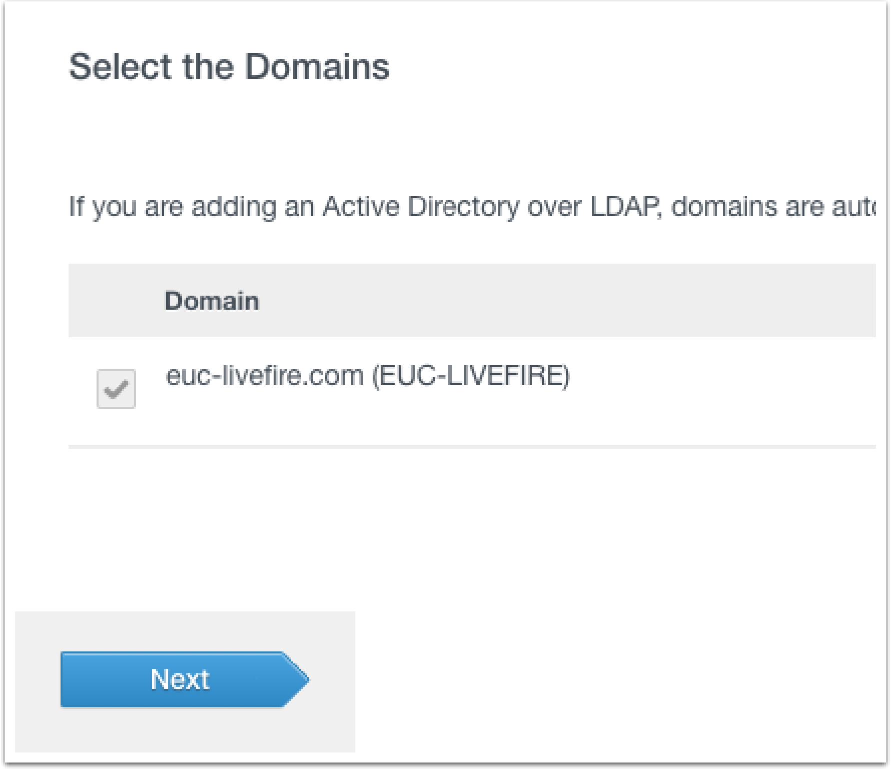
Bind User DN* cn=administrator,ou=corp,dc=EUC-Livefire,dc=com

Bind User Password* ••••••••

Enter your Active Directory bind account password.

3. In the **Add Directory** Page, configure the following (please note) The Bind syntax appears to be case sensitive
   - **Directory Name:** **LivefireSync**
   - Ensure the **Active Directory over LDAP radio button** is selected
   - **Scroll down** to **Bind User Details**
   - **Next to** :
     - **Base DN:** **dc=EUC-Livefire,dc=com**
     - **Bind DN:** **cn=administrator,ou=corp,dc=EUC-Livefire,dc=com**

    - **Bind DN Password: VMware1!**
- Select **Save & Configure**

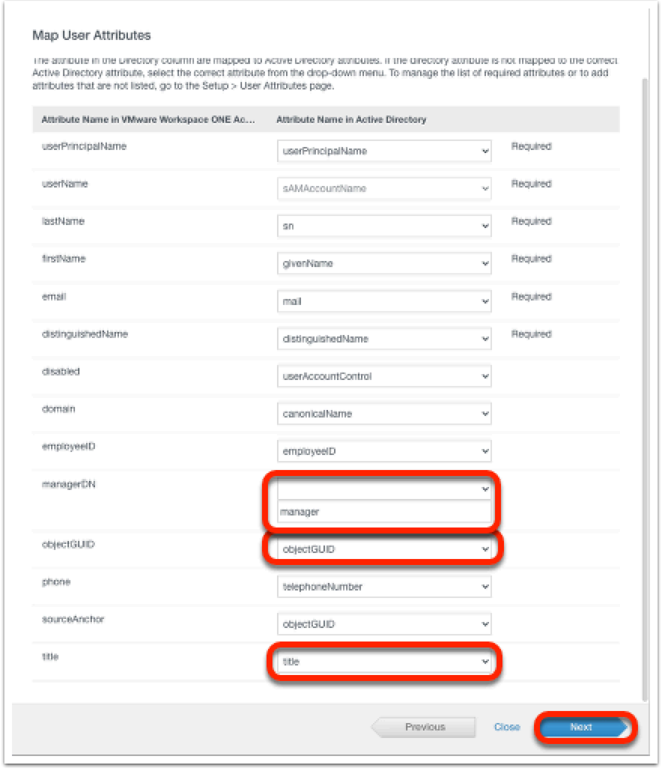


Select the Domains

If you are adding an Active Directory over LDAP, domains are aut

	Domain
☑	euc-livefire.com (EUC-LIVEFIRE)

4. On the **Select the Domains** page,
    - **euc-livefire.com** should be discovered.
        - Select **Next**.

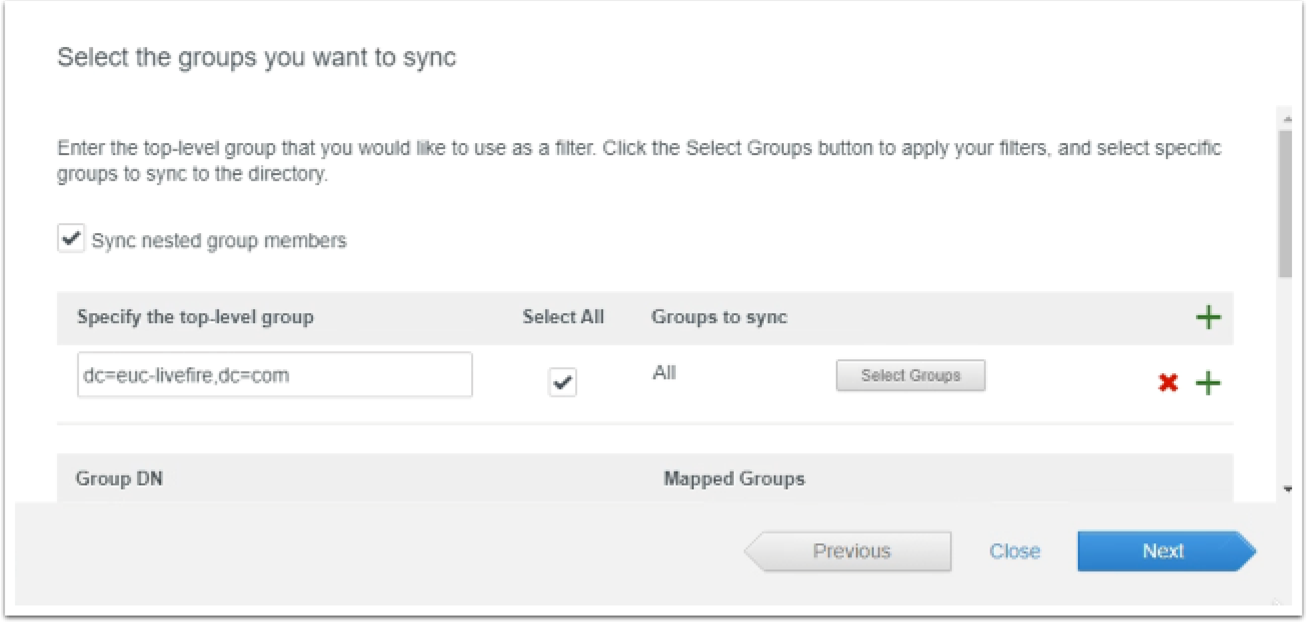


Map User Attributes

The attribute in the Directory column are mapped to Active Directory attributes. If the directory attribute is not mapped to the correct Active Directory attribute, select the correct attribute from the drop-down menu. To manage the list of required attributes or to add attributes that are not listed, go to the Setup > User Attributes page.

Attribute Name in VMware Workspace ONE Ac...	Attribute Name in Active Directory	
userPrincipalName	userPrincipalName	Required
userName	sAMAccountName	Required
lastName	sn	Required
firstName	givenName	Required
email	mail	Required
distinguishedName	distinguishedName	Required
disabled	userAccountControl	
domain	canonicalName	
employeeID	employeeID	
managerDN	manager	
objectGUID	objectGUID	
phone	telephoneNumber	
sourceAnchor	objectGUID	
title	title	

5. On the **Map User Attribute** page configure the following :
   - 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.
   - Next to **managerDN** select ***custom input*** and type **manager** in the dropdown
   - Next to **title** select **title** in the dropdown
   - Select **Next**



Select the groups you want to sync

Enter the top-level group that you would like to use as a filter. Click the Select Groups button to apply your filters, and select specific groups to sync to the directory.

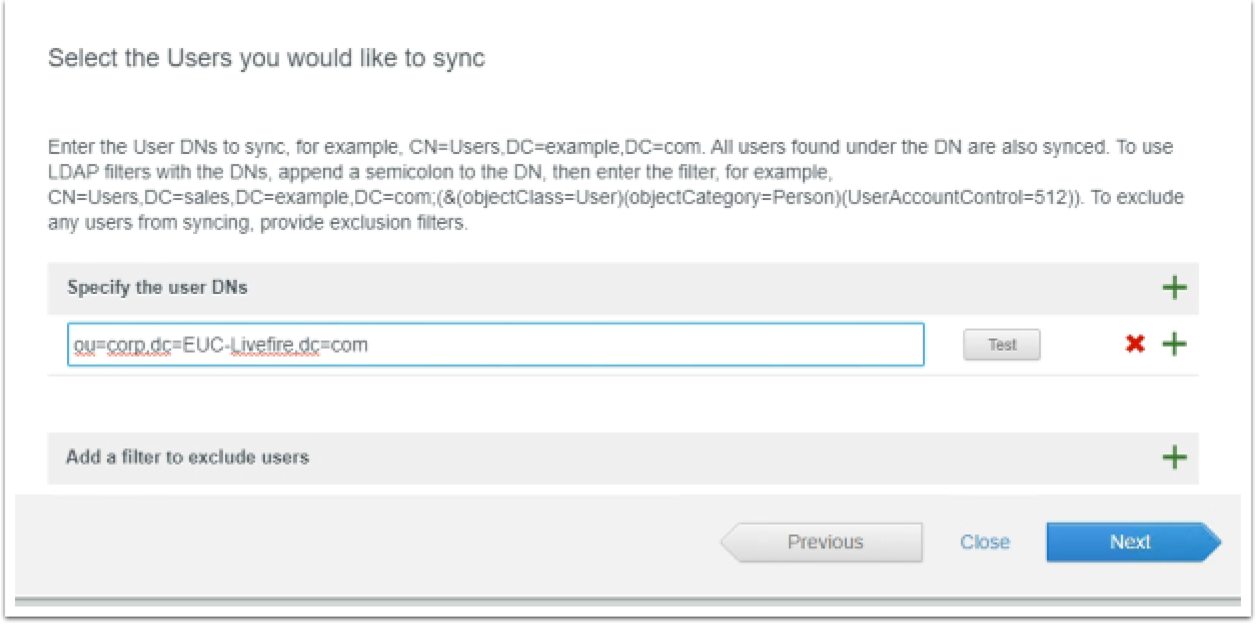
☑ Sync nested group members

Specify the top-level group	Select All	Groups to sync	
dc=euc-livefire,dc=com	☑	All	Select Groups

Group DN	Mapped Groups

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

- On the **Select the Groups you want to sync** page, select the green plus (+) to the right of the page,
- Under **Specify the group DNs** enter **dc=euc-livefire,dc=com**
- Select **Select All** check box
- Select **Next**.

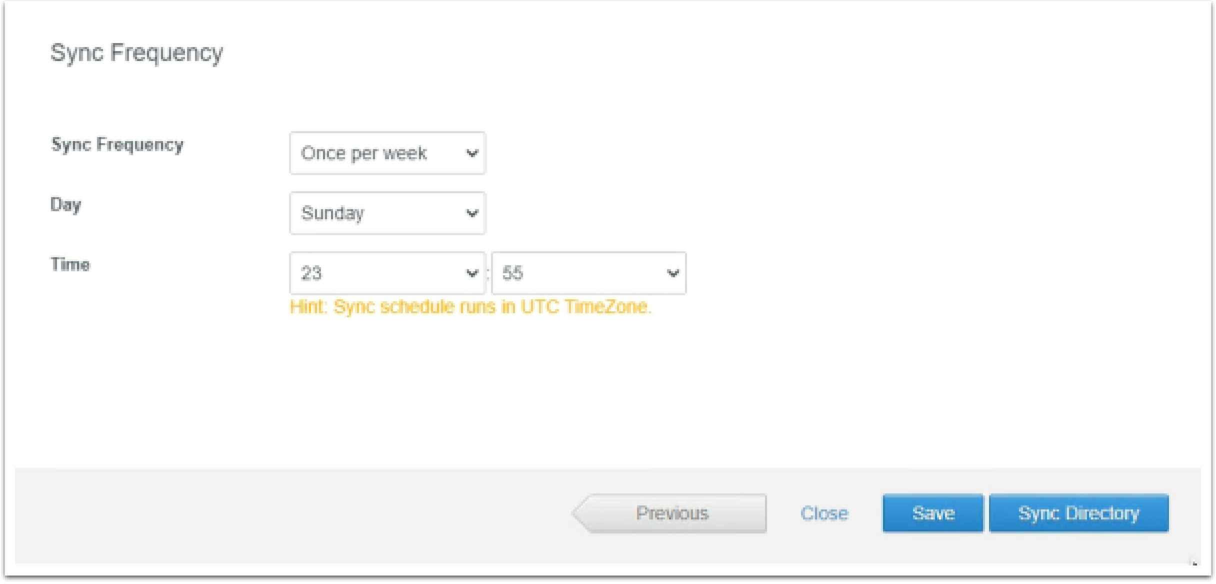


Select the Users you would like to sync

Enter the User DNs to sync, for example, CN=Users,DC=example,DC=com. All users found under the DN are also synced. To use LDAP filters with the DNs, append a semicolon to the DN, then enter the filter, for example, CN=Users,DC=sales,DC=example,DC=com;(&(objectClass=User)(objectCategory=Person)(UserAccountControl=512)). To exclude any users from syncing, provide exclusion filters.

Specify the user DNs: ou=corp,dc=EUC-Livefire,dc=com

7. In the **Select Users you would like to sync** window
   - Under **Specify the user DNs**
     - edit the existing syntax so that it reads
       - **ou=corp,dc=EUC-Livefire,dc=com**
     - Select **Next**



Sync Frequency

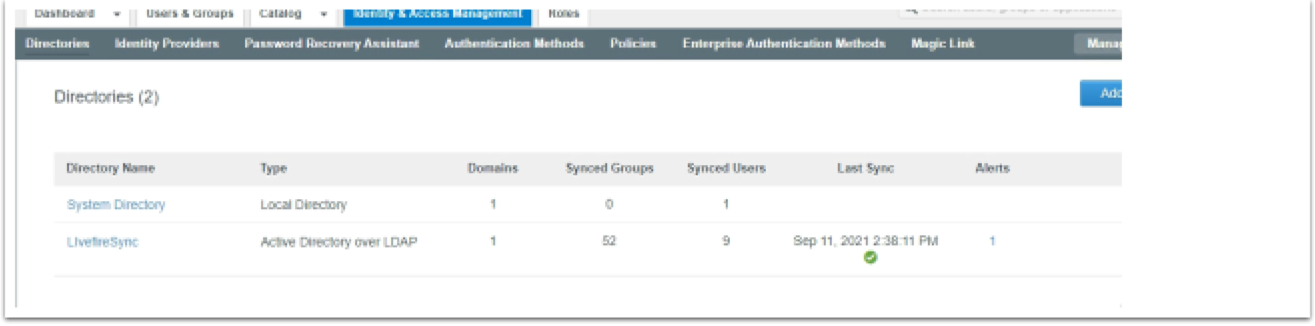
Sync Frequency: Once per week

Day: Sunday

Time: 23 : 55

Hint: Sync schedule runs in UTC TimeZone.

8. On the **Sync Frequency** window
   - Select **Sync Directory**

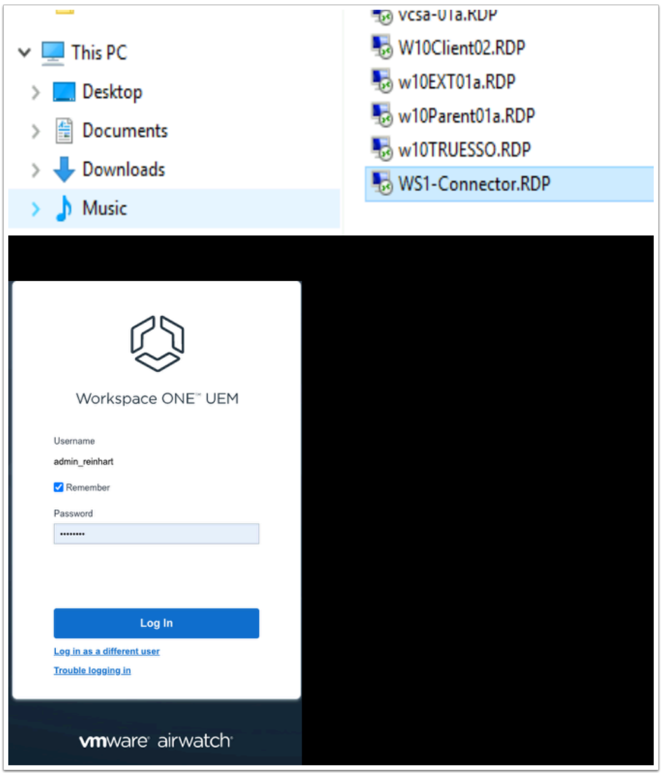


Directories (2)

Directory Name	Type	Domains	Synced Groups	Synced Users	Last Sync	Alerts
System Directory	Local Directory	1	0	1		
LivefireSync	Active Directory over LDAP	1	52	9	Sep 11, 2021 2:38:11 PM ✓	1

9. On the Directories window
   - Refresh your window
   - Note the Synced Groups and Users

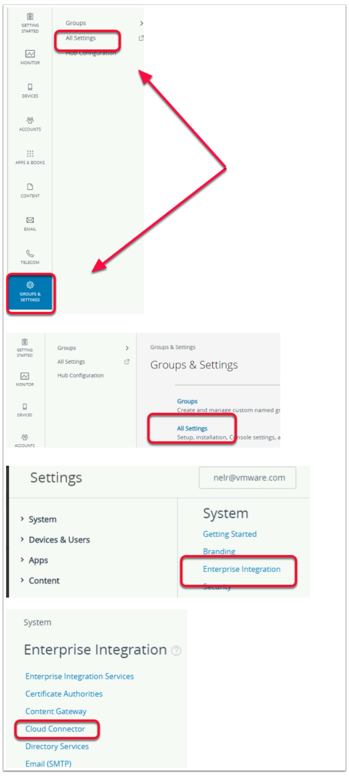
Part 4: AirWatch Cloud Connector - Installation



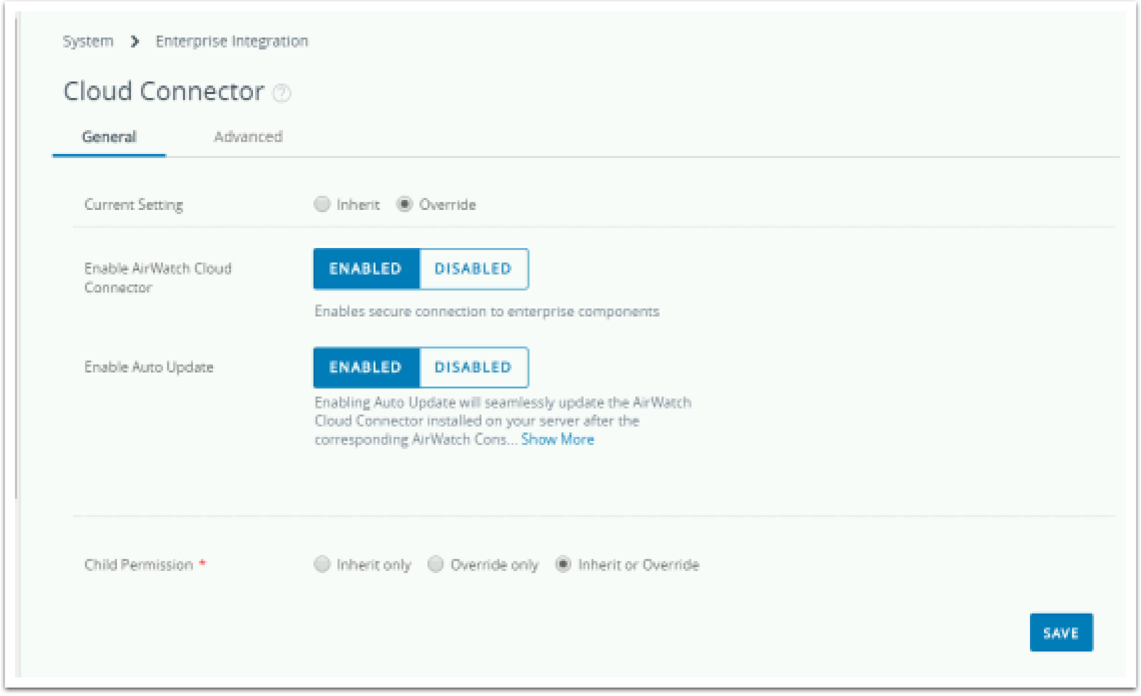
Username
admin_reinhart
☑ Remember
Password
••••••••

1. On the **ControlCenter** desktop
   - Open the **Remote Desktop** Folder**.**
   - Launch **WS1-Connector RDP shortcut.**
   - Open your **chrome browser**
   - In the address bar, enter **DW-livefire.awmdm.com**,
   - In the username area, enter your **custom email username**
     - Select **Next**

   - In the **Password** area **enter VMware1!**
   - If you get prompted with **Workspace ONE UEM highlights**, **Close** the window.



2. Navigate to Groups & **Settings** > **All Settings** > **System** > **Enterprise Integration** > **Cloud Connector**



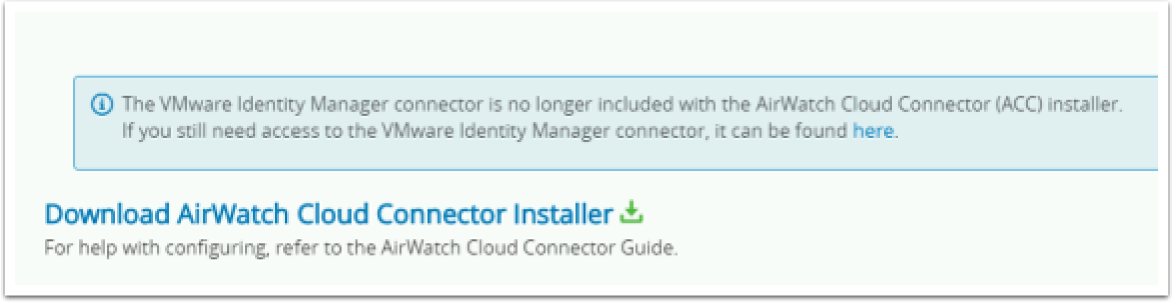
Current Setting ○ Inherit ● Override

Enable AirWatch Cloud Connector **ENABLED** DISABLED
Enables secure connection to enterprise components

Enable Auto Update **ENABLED** DISABLED
Enabling Auto Update will seamlessly update the AirWatch Cloud Connector installed on your server after the corresponding AirWatch Cons... Show More

Child Permission * ○ Inherit only ○ Override only ● Inherit or Override

3. In the Cloud Connector area
   - Select the **Overide** radio button
     - Scroll down, select **Save** at the bottom of the page

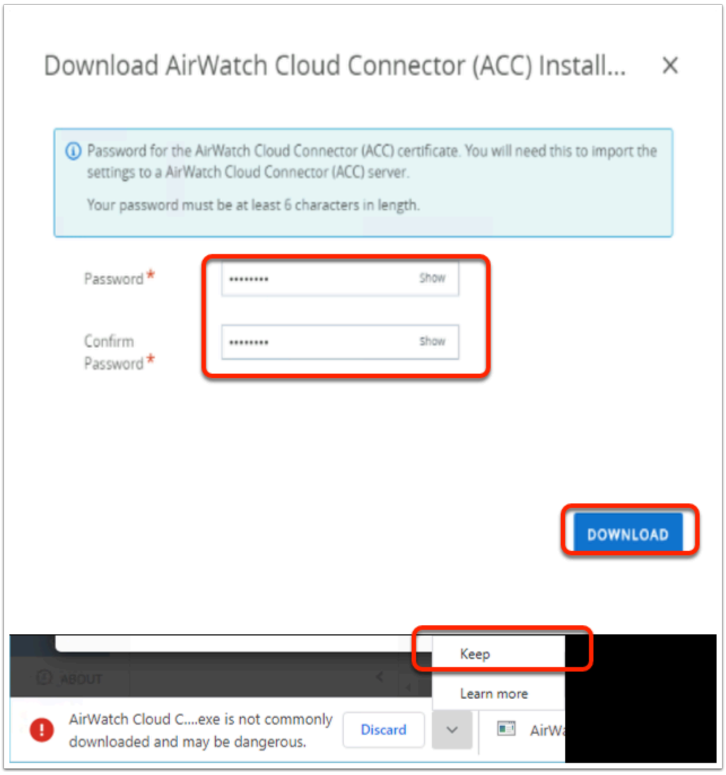


The VMware Identity Manager connector is no longer included with the AirWatch Cloud Connector (ACC) installer. If you still need access to the VMware Identity Manager connector, it can be found here.

Download AirWatch Cloud Connector Installer

For help with configuring, refer to the AirWatch Cloud Connector Guide.

4. In the Cloud Connector area
   - Scroll down and select the **Download AirWatch Cloud Connector Installer**



Download AirWatch Cloud Connector (ACC) Install...

Password for the AirWatch Cloud Connector (ACC) certificate. You will need this to import the settings to a AirWatch Cloud Connector (ACC) server.

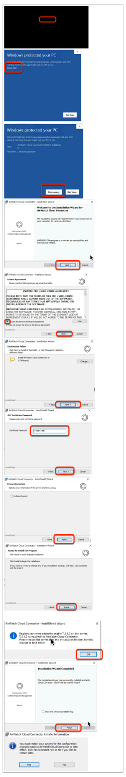
Your password must be at least 6 characters in length.

Password* •••••••• Show

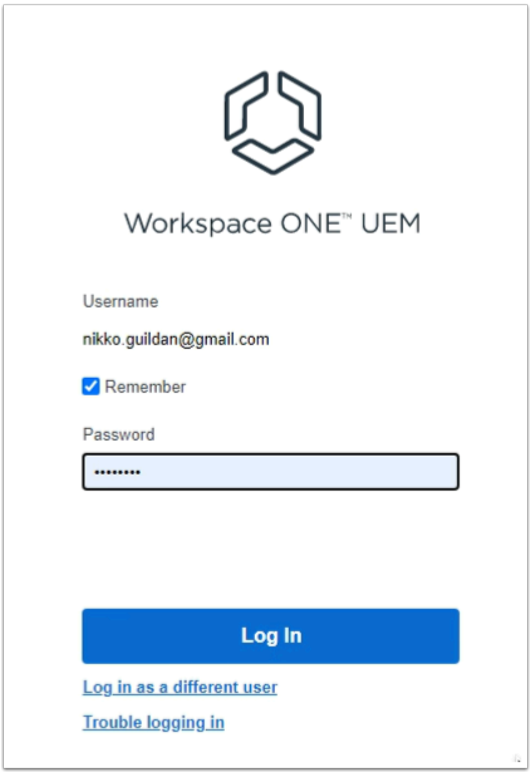
Confirm Password* •••••••• Show

AirWatch Cloud C....exe is not commonly downloaded and may be dangerous.

5. On the **Download AirWatch Cloud Connector (ACC-installer.exe)**
   - Type **VMware1!** in the **Password** and **Confirm Pasword** boxes.
   - Select **DOWNLOAD**
   - If you get a security prompt from your browser select **keep**



6. On the **Ws1-Connector** machine,
   - Select the Select **Airwatch Cloud Connector.exe**
   - Select **open**
   - Select **More Info**
   - Select **Run Anyway**
   - Select **Next**
   - Select the ***licensing to accept terms...*** **radio button** , select **Next**
   - Select **Next**
   - In the **ACC Certificate Password** window type the password **VMware1!** and select **Next**
   - Select **Next**
   - Select **Install**
   - Select **OK**
   - Select **Finish**
   - Select **Yes**



Workspace ONE™ UEM

Username

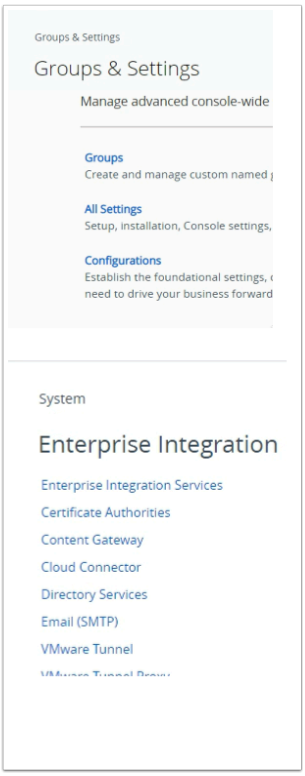
nikko.guildan@gmail.com

☑ Remember

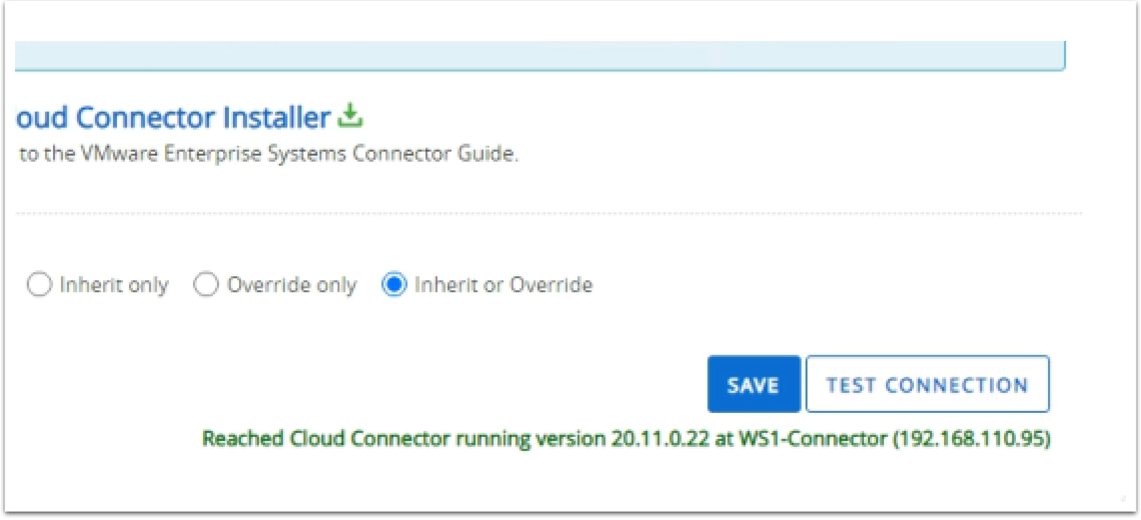
Password

••••••••

7. On your ControlCenter server
    - Open a **new tab** on your Chrome browser
    - Enter **dw-livefire.awmdm.com** in your address bar
    - Login with your **custom email username**
    - Enter your **custom Password**
    - Select **Log In**



8. In the UEM Admin Console
   - Go to **Groups & Settings** > **All Settings**
   - Under **System**, select **Enterprise Integration**
   - Under **Enterprise Integration,** select **Cloud Connector**

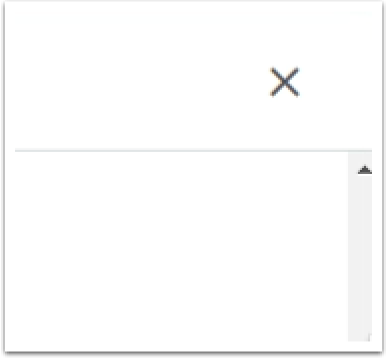

oud Connector Installer
to the VMware Enterprise Systems Connector Guide.
○ Inherit only ○ Override only ● Inherit or Override
SAVE
TEST CONNECTION

Reached Cloud Connector running version 20.11.0.22 at WS1-Connector (192.168.110.95)

9. In the Cloud Connector window
   - Scroll down
   - Select **TEST CONNECTION**

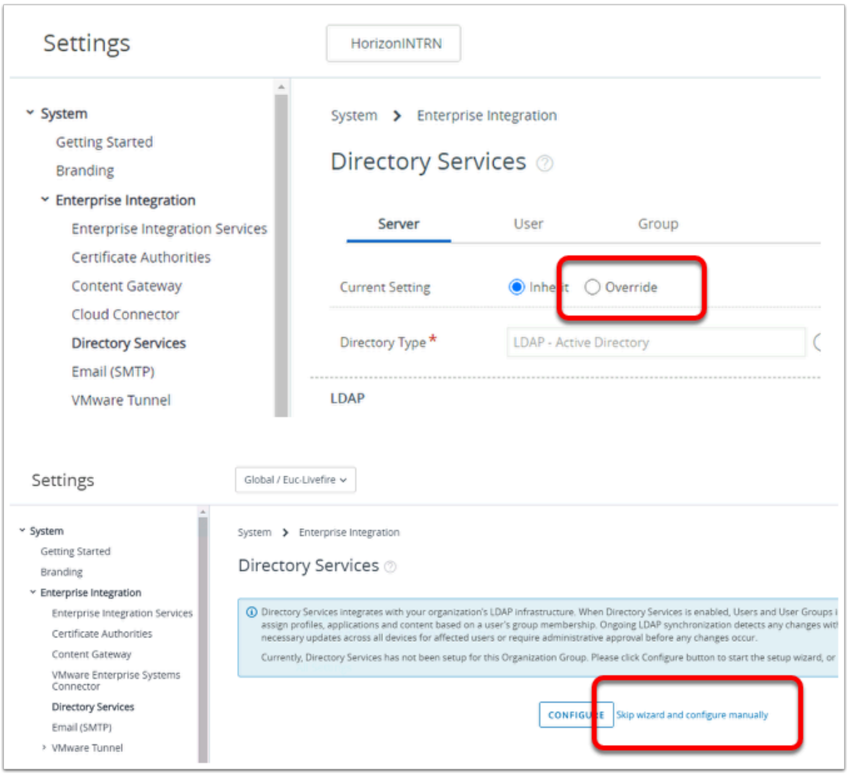
Note the screenshot

Your environment should also reflect that the Cloud Connector has been reached



10. In the Cloud Connector window
    - Select the **X** to right to close the window

Part 5 Workspace ONE UEM & Active Directory Integration



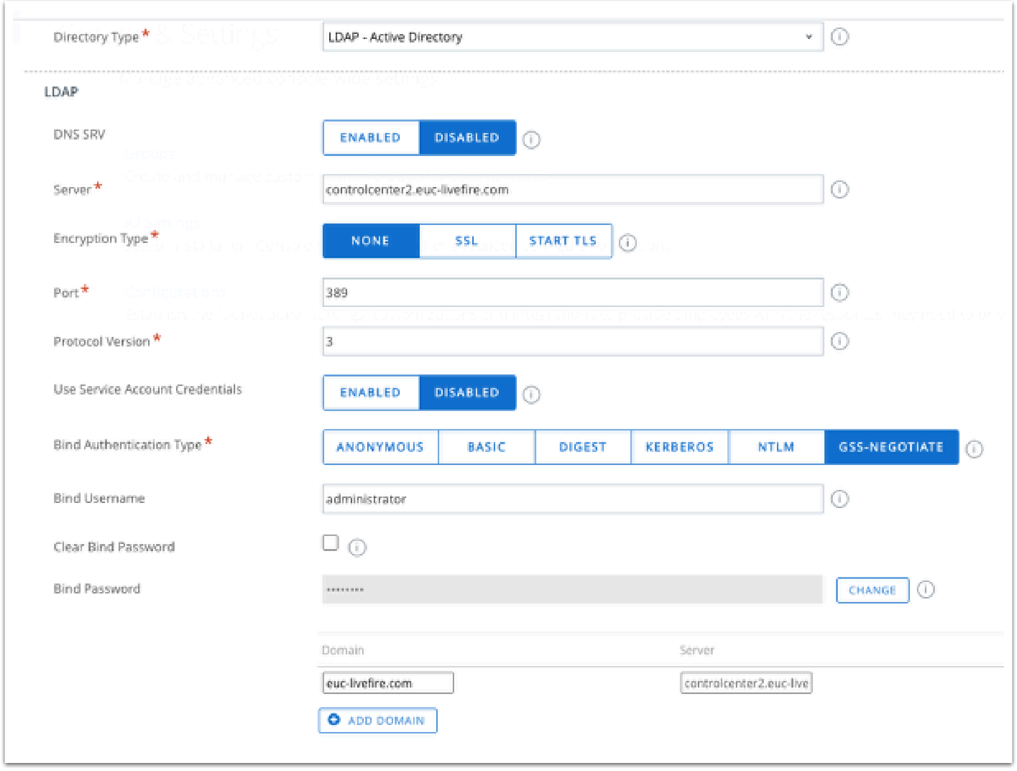
Current Setting ● Inherit ○ Override

Directory Type * LDAP - Active Directory

Directory Services integrates with your organization's LDAP infrastructure. When Directory Services is enabled, Users and User Groups i
assign profiles, applications and content based on a user's group membership. Ongoing LDAP synchronization detects any changes wit
necessary updates across all devices for affected users or require administrative approval before any changes occur.

Currently, Directory Services has not been setup for this Organization Group. Please click Configure button to start the setup wizard, or

1. In the Workspace ONE UEM admin console
    - Select **Groups & Settings** > **All Settings** > **System** > **Enterprise Integration**
    - Under **Enterprise Integration**
        - Select **Directory Services**
    - In the **Directory Services** window
        - Select the **Overide radio button**
    - Select **Skip wizard and configure manually**

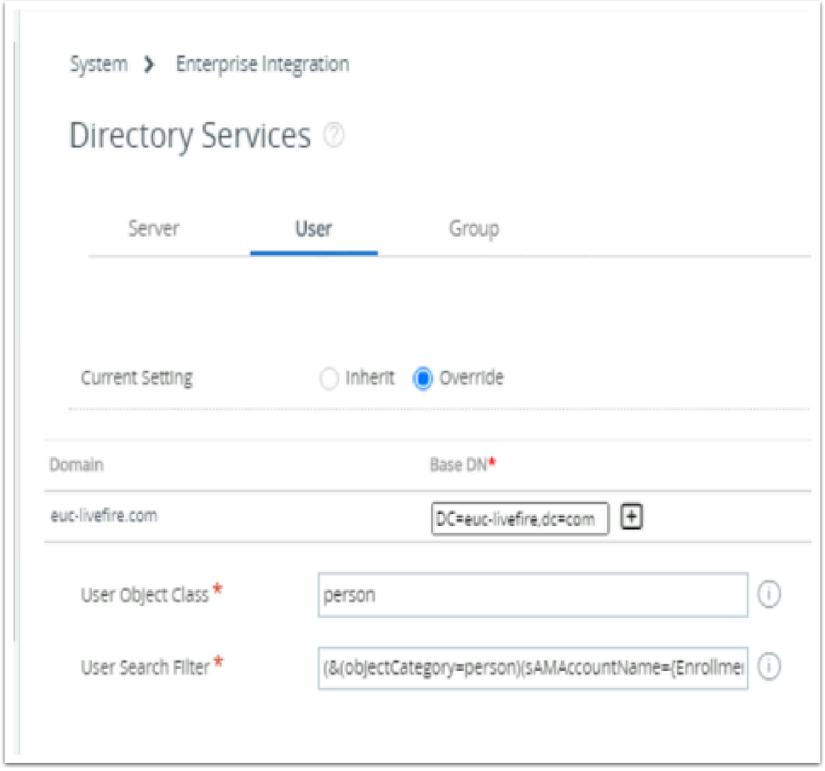


Directory Type *	LDAP - Active Directory
LDAP	
DNS SRV	ENABLED [✓ DISABLED]
Server *	controlcenter2.euc-livefire.com
Encryption Type *	[✓ NONE] SSL START TLS
Port *	389
Protocol Version *	3
Use Service Account Credentials	ENABLED [✓ DISABLED]
Bind Authentication Type *	ANONYMOUS BASIC DIGEST KERBEROS NTLM [✓ GSS-NEGOTIATE]
Bind Username	administrator
Clear Bind Password	□
Bind Password	•••••••• CHANGE

Domain	Server
euc-livefire.com	controlcenter2.euc-live

ADD DOMAIN

2. From the **Directory Services** Interface,
   - Under the **Server Tab , enable the** following .
     - Directory: **LDAP-Active Directory**
     - DNS SRV: **Disabled (default)**
     - Server : **ControlCenter.euc-livefire.com**
     - Encryption Type: **None**
     - Port: **389 (default)**
     - Protocol Version: **3 (default)**
     - User Service Account Credentials: **Disabled (default)**
     - Bind Authentication Type: **GSS-Negotiate (default)**
     - Bind User Name: **administrator**
     - Bind Password: **VMware1!**
     - Domain: **euc-livefire.com**


System > Enterprise Integration

Directory Services

Current Setting ○ Inherit ● Override

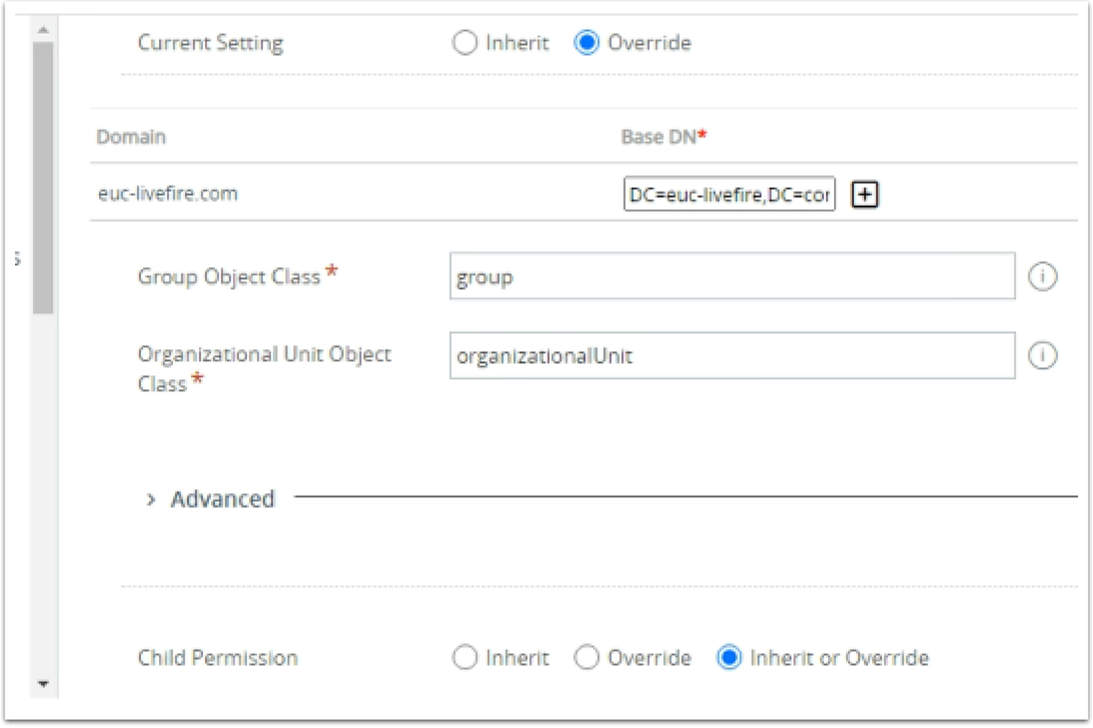
Domain	Base DN*
euc-livefire.com	DC=euc-livefire,dc=com

User Object Class * person

User Search Filter * (&(objectCategory=person)(sAMAccountName={Enrollme

3. From the **Directory Services** Interface,
   - Under the **User Tab , enable the** following .
   - Validate the following configuration is configured under the User Tab
     - Under **Base DN,** ensure that **DC=euc-livefire,DC=com** has automatically populated.
       - If not, click on the **+** icon and add **DC=euc-livefire,DC=com**

     - Next to **User Object Class**, ensure **person** is the property
     - Next to **User Search Filter**, ensure **(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))** is the string



Current Setting ○ Inherit ● Override

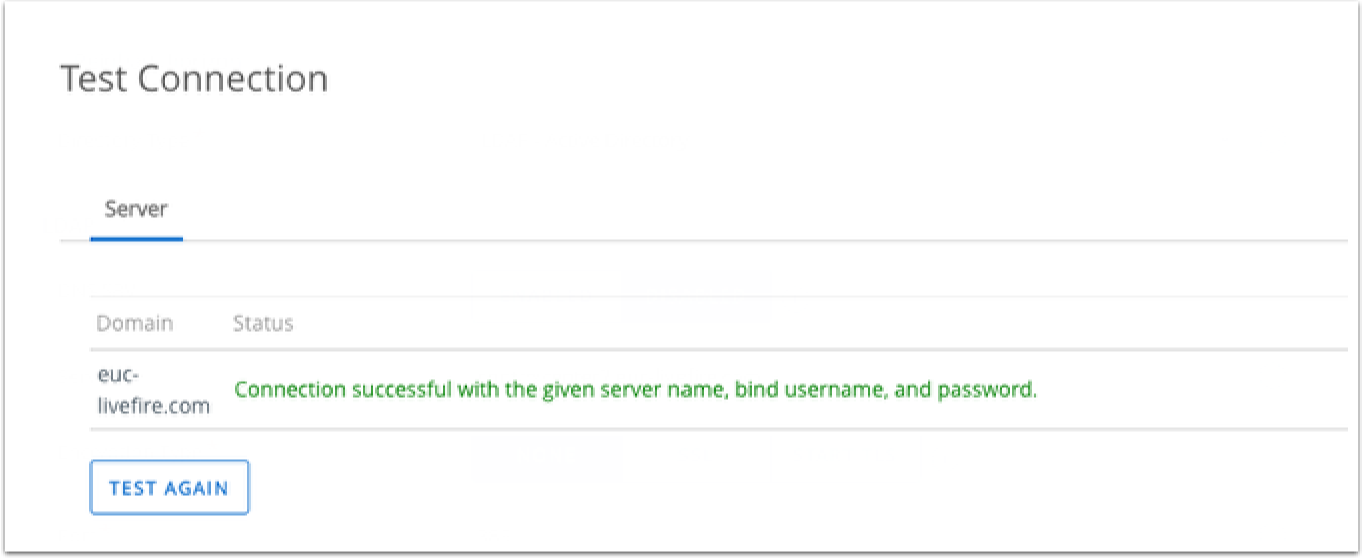
Domain	Base DN*
euc-livefire.com	DC=euc-livefire,DC=cor

Group Object Class *: group

Organizational Unit Object Class *: organizationalUnit

Child Permission ○ Inherit ○ Override ● Inherit or Override

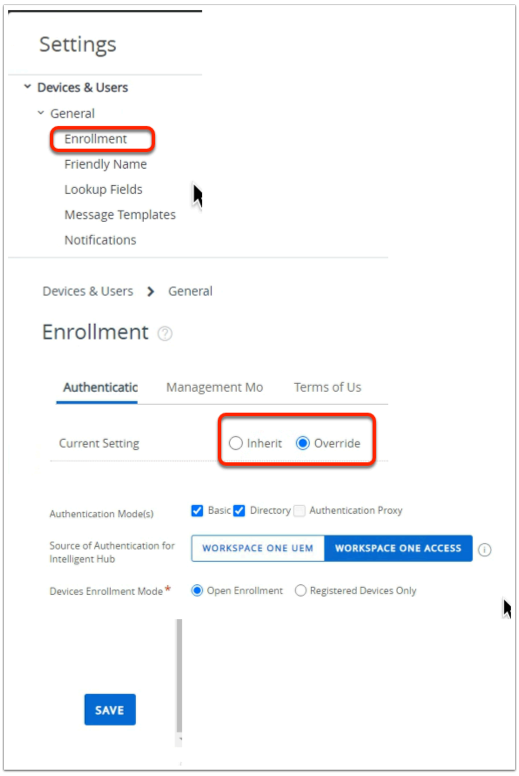
4. From the **Directory Services** Interface,
   - Repeat these steps for the third tab **Group**
     - Under Base DN, notice validate that **DC=euc-livefire,DC=com,** is entered.
     - **Scroll** to the bottom of the page and select **Save**
     - Select **TEST CONNECTION**



Test Connection

Domain	Status
euc-livefire.com	Connection successful with the given server name, bind username, and password.

5. You should have a **Test Connection** window launch saying **Connection successful....**
   - **Select CANCEL to close the window**



Current Setting ○ Inherit ● Override

Authentication Mode(s) ☑ Basic ☑ Directory □ Authentication Proxy

Source of Authentication for Intelligent Hub: WORKSPACE ONE UEM | **WORKSPACE ONE ACCESS**

Devices Enrollment Mode* ● Open Enrollment ○ Registered Devices Only

6. Let's ensure users can enroll their devices using Active Directory credentials.
   - Under Settings , select **Devices & Uses**
   - **Select** > General
   - Select > **Enrollment**
   - Under the **Enrollment** area
     - Select the **Override** radio button
     - Scroll down
       - Next to **Authentication Modes(s)** ensure the the **Directory** check box is selected
       - Next to Source of Authentication for Intelligent Hub, select **Workspace ONE ACCESS**
     - Scroll down
       - Select **SAVE**
   - Close the **Settings** window, by selecting the **X** on the right of the window.