Integrating the Horizon Universal Console with Workspace ONE

Part 1 - Completing Workspace ONE Integration Prerequisites

Part 1 contains 11 sections

- We will build an integrated Workspace ONE platform and then we will integrate Horizon Cloud services with this platform
- All of these sections have to be completed to complete further labs

Part 1:Section 1: Workspace ONE Access , Connector pairing pre-requisites



1. On your ControlCenter server

- Open your Workspace ONE Access, Admin console URL
 - Under **Username**
 - enter Administrator

- Under **Password**
 - enter VMware1!
- Select Sign In



- 2. In the Web Intelligent Hub Console
 - To the right,
 - select TA
 - From the dropdown
 - select Workspace ONE Access Console

← → C ① 🗎 aw-liveti	rernpod22.vidmpreview.com/ws1-admi
🕤 my-ip.livefire.lab/ip 🔤 Horizon	®Site 1 vm UAG-HZN-01a vm UAG-HZN
(R) Workspace ONE Access	Q Search for users, groups, or applicati
Monitor Accounts Resources	Integrations Settings
Authentication Methods	Connectors
Connectors	The VMware Workspace NE Access conn
Connectors (Legacy)	and virtual app integration.
Directories	
Connector Authentication Methods	NEW
Hub Configuration	Host
Identity Providers	T
Magic Link	
Okta Catalog	
People Search	

3. In the Workspace ONE Access Console

- Select Integrations
- Under Integrations
 - Select Connectors
- In the **Connectors** area
 - Select NEW

Connector Usage Confirmation	×
If you are planning to integrate with Horizon, Horizon Cloud with Single-Pod Broker, or Citrix, use the latest Workspace ONE Access Connector.	
• Latest Workspace ONE Access Connector This option is to migrate your existing directories and virtual apps to a new connector.	
CANCEL	ок

- 4. In the Connector Usage Confirmation window
 - Select the radio button, next to :-
 - Latest Workspace ONE Access Connector
 - Select OK

Confirm the latest Workspace ONE Connector		\times
Click confirm to use the latest Workspace ONE Access Connector. This will enable you to integrat Cloud with Single-Pod Broker, or Citrix.	e with Ho	rizon, Horizon
C/	ANCEL	CONFIRM

- 5. In the **Confirm the latest Workspace ONE Connector** window
 - Select CONFIRM

Add New Connector	Download Installer	×
1 Download Installer	Click the link below to log in to My VMware and download the connector installer. The link opens in a separate	
2 Download Configuration Pile	window so you can keep this wizard open.	
3 Summary	GD TO MYVWWARE.COM	
	CANCEL NEX	IT.

- 6. In the Add New Connector window
 - 1. Downloader Installer area
 - Select NEXT

Add New Connector	Download Config	guration File ×
1 Download Installer	Create a password for t installer.	he configuration file. You will need this password when you run the connector
2 Download Configuration File		
3 Summary	Password	VMwaret/VMwaret/
	Reenter Password	VMwarel/VMwarel/
	DOWNLOAD CONFIG	
		CANCEL BACK NEXT
4		
es-config.json	~	

- 7. In the Add New Connector window
 - 2. Download Configuration File area
 - Next to Password: enter VMware1!VMware1!
 - Next to Reenter Password: enter VMware1!VMware1!
 - Select DOWNLOAD CONFIGURATION FILE
 - note an es-config.json file gets downloaded
 - Select NEXT

Add New Connector	Summary	×
1 Download Installer	Transfer the installer and configuration file to your Windows server, and begin the installation.	
2 Download Configuration File	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.	
3 Summary		
	CANCEL BACK CLOS	E

- 8. In the Add New Connector window
 - 3. **Summary** window
 - Select CLOSE

	Open Always open files of this type
4	Show in folder
	Cancel
es-config.json	

- 9. On your ControlCenter server browser
 - Next to the **es-config.json**
 - Select the **Dropdown**
 - Select Show in folder



10. In the File Explorer window

- Select and right-click the es-config.json file
- Select Copy
- In the left pane
 - Select Desktop



- 11. In the File Explorer window
 - Desktop area
 - Select the **Software** shortcut
 - In the **Software** folder
 - Open the ACCESS folder

o Quick Copy Paste ccess	Cut Copy path Paste shortcut	Move Copy to * to *	Delete	Rename	New folder
Clipboa	rd	c	rganize		1
→ * ↑ □ >	Network → horizon-	01a.euc-livefire	.com → se	oftware ⇒	ACCESS >
🔮 Documents 🖈 '	 Name 	^		Da	ate modified
📰 Pictures 🛛 🖈	vidm Conn	ector HOL Proc	ess	3/	1/2021 7:46 A
hol	dualbootup	date.tar.gz		2/	25/2021 6:17
Site1	es-config.js	on		2/	21/2022 4:14
Site2	🍰 jre-8u201-v	vindows-x64.exe	1	10	/7/2020 9:49
System32	Workspace	ONE_Access_C	onnector_l	nst 2/	21/2022 2:39
This DC	🔘 Workspace	ONE-Access-C	onnector-l	nst 2/	21/2022 2:30
J SD Objects		View		>	
Desktop		Sort by			
Documents		Group by		5	
Downloads		Refresh			
Music		Refresh			
Pictures		Customize this	folder		
Videos		Paste			
Local Disk (C:)		Paste shortcut			

- 12. In the File Explorer window
 - ACCESS folder
 - Paste your es-config.json file
 - Close your File Explorer window

Part 1:Section 2: Installing and Configuring the Workspace ONE Access connector



- 1. On your ControlCenter server
 - On the Desktop.
 - Open the Remote Desktops\Site1 folder
 - Select and launch the WS1-Connector.RDP shortcut



- 2. On your WS1-Connector server
 - Open the **Software** Folder
 - Select the ACCESS Folder
 - Select and Launch
 - Workspace-ONE-Access-Connector-Installer-22.09.0.0.exe



- 3. On your WS1-Connector server
 - On the Open File Security Warning window
 - Select Run

😸 Workspace ONE Access Co	nnector - Installation Wizard	×
	Welcome to the Installation Wizard for Workspace ONE Access Connector 22.09.0.0	
8 Workspace ONE [®] Access	The Installation Wizard will install Workspace ONE Access Connector on your computer. To continue, click Next.	
Augura.	WARNING: This program is protected by copyright law and international treaties.	
	< Back Next > Cancel	

- 4. On the Workspace ONE Access Connector InstallShield Wizard
 - In the Welcome to the Installation Wizard for Workspace ONE Access Connector 22.09.0.0
 - Select Next

Workspace ONE Access Connector -	Installation Wizard	×
License Agreement		25
Please read the following license agreer	ment carefully.	S
VMWARE GENERAL TERMS		^
By downloading or using an Offer the terms of the Agreement.	ring, Customer agrees to be b	bound by
1. OFFERINGS.		~
I accept the terms in the license agreem	ient	Print
O I do not accept the terms in the license	agreement	
InstallShield		
	< Back Next >	Cancel

- 5. On the Workspace ONE Access Connector InstallShield Wizard
 - Licence Agreement window
 - Select the 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 The your servi	d. eature Description is Service is required if you ant to sync users from your tive Directory / LDAP servers. is feature requires 227MB on our hard drive.
Install to: C:\Program Files\	Change
InstallShield	Cancel

- 6. On the **Workspace ONE Access Connector InstallShield** Wizard
 - Service Selection window
 - Select Next

Specify Configuration File		
Select the configuration file that you d Access console and enter its password	lownloaded from the Workspace ONE d.	Ô
Click on Browse for the configuration file	.	
\\horizon-01a\software\ACCESS\es-co	Brows	e
Password:	4	
Enable FIPS		
See Installing VMware Workspace ONE	Access Connector 22.05.0.0. Visit the v	<u>ebsite</u> .
tallshield		

- 7. On the Workspace ONE Access Connector InstallShield Wizard
 - Specify Configuration File window
 - In the box in front of **Browse...**
 - type \\horizon-01a\software\ACCESS\es-config.json
 - Next to Password: type VMware1!VMware1!
 - Select Next



- 8. In the **Workspace ONE Access Connector InstallShield** Wizard
 - Select Default or Custom Installation window
 - Select the **radio button** next to **Custom**
 - Select Next

Workspace ONE Access Connector - InstallShield Wizard Specify Proxy Server Information Configure a proxy server that Workspace ONE Access services will use.	×	
Enable Proxy ?		0 1 0
InstallShield <back next=""></back>	Cancel	

- 9. In the Workspace ONE Access Connector InstallShield Wizard
 - Specify Proxy Server Information window
 - Select Next

Workspace ONE Access Connector - I	nstallShield Wiza	rd	X
Specify Syslog Server Information Provide Syslog details for configuring We	orkspace ONE Acce	ess services.	\bigcirc
Enable Syslog?			
InstallShield	< Back	Next >	Cancel

- 10. In the Workspace ONE Access Connector InstallShield Wizard
 - Specify Syslog Server Information window
 - Select Next

Workspace ONE Access Connector - InstallShield Wizard	×
Citrix configuration	15
Citrix multisite aggregation and keyword filtering configuration	Q
Enable Citrix StoreFront restricted PowerShell session	
Configuration Name	
Note: Enter the restricted PowerShell session file name without an extension	
Enable Citrix keyword filtering	
Select to use keyword filtering in Citrix virtual apps collections.	
Disable Citrix auto-loading of StoreFront modules	
Select to manual y load PowerShell modules in StoreFront for multisite aggregation and keyword filtering.	
InstallShield	
< Back Next >	Cancel

- 11. In the Workspace ONE Access Connector InstallShield Wizard
 - Citrix configuration
 - (leave default)
 - Select Next

😥 Workspace ONE Access	Connector - InstallS	hield Wizard		×
Install Trusted Root Cer	tificates			25
Upload Workspace ONE A	ccess Trust root certif	icates.		\otimes
Linked Trust Root Certifica	lec:			
i				
_				
TestalShield	Cert Details	Remove	!	Browse
Distance inclu		Back	Next >	Cancel
			next >	Cancer
No certificates			×	
No certificates are unloaded				
Do you still want to continue	•	any Trust root		
certificates?	e without installing	any nuscroot		
		-		
	Yes	No		

- 12. In the Workspace ONE Access Connector InstallShield Wizard
 - Install Trusted Root Certificates window
 - Select Next
 - In the **No certificates** page
 - Select Yes

Specify Ports	nector - Instalionielo Wizaro	
Specify ports for the Workspa	ce ONE Access services or use the default ports.	Q
ł		
Directory Sync Service Port	8080	
User Auth Service Port	8090	
Kerberos Auth Service Port	443	
Virtual App Service Port	8008	
InstallShield		
	< Back Next >	Cancel

- 13. In the Workspace ONE Access Connector InstallShield Wizard
 - Specify Ports window
 - Select Next

stall SSL Certificate fo	Kerberos A	auth Service			25
Instal a signed SSL certific signed certificate, a self-s	ate in PEM or gned certifica	PKCS#12 form te is auto-gene	at. If you do arated.	not install a	\approx
Would you like to use y	our own SSL (certificate?			
Click Browse and select the	certificate fil	e.			
				Browse.	

- 14. In the Workspace ONE Access Connector InstallShield Wizard
 - Install SSL Certificate for Kerberos Auth Service window
 - Next to: Would you like to use your own SSL certificate?
 - Select the Checkbox
 - Under , Click Browse and select the certificate file
 - Select Browse

😸 InstallShield			×
	software > certificates > v じ	Search certificates	<i>م</i>
Organize 🔻 New fo	lder		•
	Name	Date modified	Туре
Pasitan	App Volumes Certificates	2/14/2022 6:31 PM	File folde
Desktop	Certificate Bundle	3/30/2022 7:08 PM	File folde
Downloads	Mildcard2022	2/14/2022 4:50 PM	Personal
Documents :	Ŕ		
Pictures	*		
📃 This PC			
💣 Network			
			,
File	e name: Wildcard2022 V	PKCS #12 Certificate File (*	°.pfx, ∨
		Open Ca	ncel

- 15. In the **InstallShield** window
 - Browse to:
 - \\horizon-01a\software\certificates
 - Select Wildcard2022
 - Select Open

Instal a signed SSL certificate in PEM or signed certificate, a self-signed certifica- Would you like to use your own SSL Click Browse and select the certificate fit [\phorizon-01a\software\certificates\Wil	r PKCS#12 form ate is auto-gene certificate? ile.	at. If you do r rated.	not install a	S
Would you like to use your own SSL Click Browse and select the certificate fi \\horizon-01a\software\certificates\Wi	certificate? ile.			
Click Browse and select the certificate fi \\horizon-01a\software\certificates\\//i	ile.			
\\horizon-01a\software\certificates\Wil				
	ldcard2022.pfx		Browse	
Certificate Password:]	
allShield				

- 16. In the Workspace ONE Access Connector InstallShield Wizard
 - Install SSL Certificate for Kerberos Auth Service window
 - Next to: Certificate Password:
 - Enter : VMware1!
 - Select the Next

pecify Service Account	
the Kerberos Auth Service and the Virtual App Service.	
	Ŷ
The second second has been been been and the second s	
The user account must be in the form DOMAIN Username.	
User name:	
euc-livefire.com\administrator	Browse
Password:	
-	7
[
allchield	
allShield	

- 17. In the Workspace ONE Access Connector InstallShield Wizard
 - Specify Service Account window
 - Under User name: type
 - euc-livefire.com\administrator
 - Under Password:
 - type VMware1!

Select Next

🐙 Workspace ONE Access Connector - Installation	Wizard X
Ready to Install the Program	25
The wizard is ready to begin installation.	\otimes
Click Install to begin the installation.	
If you want to review or change any of your installat exit the wizard.	tion settings, dick Back. Click Cancel to
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
No of Trust root certificates :0	SSL Certificate : Custom
Testallibiald	
e Rark	Instal Cancel
COOC	instal Carter

- 18. In the Workspace ONE Access Connector InstallShield Wizard
 - **Ready to Install** window
 - Select Install

The Installation of the Workspace ONE Access Connector will take about 10 minutes to complete

😸 Workspace ONE Access Cor	nnector - Installation Wizard	×
	Installation Wizard Completed	
8	The Installation Wizard has successfully installed Workspace ONE Access Connector. Click Finish to exit the wizard.	
Workspace ONE" Access		
ALLINGUE.		
	Show the Windows Installer log	
	•	
	< Back Finish Cancel	

19. In the Workspace ONE Access Connector - InstallShield Wizard

- Installation Wizard Completed window
 - Select Finish

Part 1:Section 3: Configuring Directory Sync with Workspace ONE Access 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. In the Workspace ONE Access Admin console
 - Select Settings
 - Select User Attributes

Δ	Avi Vantage C	ontrol	m Hi	ZN Cloud	6	vcenter-01a	0
			6				
				(Custom	Attributes	
_				•			_
or w	vhen local users	are create	d. The	ise A	attribut	ur own attrik es.	outes to
					Name		
					e i	DD POW	

2. In the **User Attributes** console

- In the right area under Custom Attributes
 - Select

 ADD ROW 4 times

Add your own attributes to syn	to the directory. Go to the director	ry's attributes page to map t
attributes.		
Name		
objectGuid		
,		
managerDN		1
sid		1
netBios		1

3. In the **User Attributes** console

- Under Name
 - Add the following additional attributes

- note this is case sensitive :
- objectGuid
- managerDN
- sid
- netBios



- 4. In the User Attributes console
 - Under User Attributes
 - Select SAVE

← → C ☆ aw-live	firernpod22.vidmpreview.com/ n®Site 1 🚾 UAG-HZN-01a 🐨
(8) Workspace ONE Access	Q Search for users, groups,
Monitor Accounts Resources	Integrations Settings
Authentication Methods Connectors Connectors (Legacy)	Directories (1)
Directories	System Directory
Connector Authentication Methods	
Hub Configuration	
Identity Providers	

- 5. In the **Workspace ONE Access** admin console.
 - Select Integrations,
 - Select Directories

Add Directory Alerts Add Directory Alerts Add Directory Active Directory LDAP Directory LDAP Directory LDAP Directory LOAP Directory LOAP Directory LOAP Directory LOAP Directory LOAP Directory	c22-01a			
Alerts Add Directory Alerts Add Directory Active Directory LDAP Directory Local User Directory Local User Directory		¢	Tenant Admin 🗸	
Add Directory Active Directory LDAP Directory Local User Directory	Alert	5	Add Directory	
	Alerts	C	Add Directory Active Directory LDAP Directory Local User Directory	

6. In the **Directories** area

- To the right
 - Select Add Directory

- In the Add Directory dropdown
 - Select Active Directory

Add Directory	
Directory Name*	EUC-Livefire
	 Active Directory over LDAP Active Directory over Integrated Windows Authentication
Directory Sync and	Select at least one active directory sync host that syncs users from Active Dire

- 7. In the Add Directory Page,
 - Configure the following: next to
 - Directory Name: type EUC-Livefire
 - Ensure the Active Directory over LDAP radio button is selected
 - Scroll down to Bind User Details

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

- 8. In the Add Directory Page,
 - In the **Bind User Details** area
 - Enter the following 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



- 9. In the **Select the Domains** page,
 - euc-livefire.com (EUC-LIVEFIRE)
 - Select Next.

	canonicalName	~
employeeID	employeeID	~
managerDN		v
	manager	
managerid	Enter Custom Input	v
	Enter Custom Input	
petBios		~

10. On the Map User Attribute page

- Map the following attributes : next to:-
 - (what you enter here is case sensitive)
 - managerDN select custom input and type manager
 - netbios: select custom input type msDS-PrincipalName

	Enter Custom Input	
objectGuid	objectGUID	r i
organization	Enter Custom Input	-
	Enter Custom Input	
phone	telephoneNumber	~
profileUrl	Enter Custom Input	~
	Enter Custom Input	
sid		~
	objectSid	
	Prevk	ous Close Next

11. On the Map User Attribute page

- Map the following attributes :
 - Scroll down next to:-
 - objectGuid: select objectGUID
 - sid: select custom input type objectSid

sourceAnchor	objectGUID	~
title	title	~
userPrincipalName	userPrincipalName	~
	Previ	ious Close Next

12. On the Map User Attribute page

- Map the following attributes :
 - Scroll down next to:-
 - title : from the dropdown
 - select title
 - Validate that userPrincipalName maps to userPrincipalName
- Select Next

Select the groups you want to sync			
Enter the top-level group that you would like to groups to sync to the directory.	use as a filter. Cli	ck the Select Groups button to apply your filters, and se	elect specific
Sync nested group memoers Specify the top-level group	Select All	Groups to sync	1
br-euc-livefin do-com	_	Mapped Groups	× +

- 13. On the Select the Groups you want to sync page,
 - 1. select the green plus (+) to the right of the page,
 - 2. Under Specify the group DNs
 - enter dc=euc-livefire,dc=com
 - 3. Select the Select All writing
 - You will notice the **check box** now becomes available

Select the groups you want to sync					
Enter the top-level group that you would like to groups to sync to the directory.	use as a filter. Cli	ck the Select Group	os button to apply you	r filters, and select sp	ecific
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 Group	8		
dc=euc-livefire,dc=com		All groups in th	is DN are selected		
			Previous	Close Nex	đ

- 14. On the Select the Groups you want to sync page,
 - Under Select All
 - Select the 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-co LDAP filters with the DNs, append a semicolon to the DN, then enter the f CN-Users, DC-sales, DC-example, DC-com, (&(d)ed:Class-User)(object) any users from syncing, provide exclusion filters.	m. All users found under the t lter, for example, Jategory=Person)(UserAccou	0N are also sync ntControl=512))	ed. To use To exclude
Specify the user DNs			+
ouncorp.donEUC-Livefire.doncom		Test	× +
Add a filter to exclude users			+
	Previous	Close	Net

15. 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	Once per week	~				
Day	Sunday	~				
Time	23	¥: 55	,	~		
	Hint: Sync schedu	le runs in U	FC TimeZone.			

16. On the **Sync Frequency** window

Select Sync Directory

	Q Search for users, groups, or a	applications				New Navigation	•	Ø
85	Integrations Settings Directories (2)							
	Directory Name	Туре	Domains	Synced Groups	Synced Users	Last Sync	Alert	5
	System Directory	Local Directory	1	0	1			
	EUC-Livefire	Active Directory over LDAP	1	52	8	Oct 28, 2022 12:48:53 PM 🥝	1	

17. On the **Directories** window

- Refresh your browser window
 - Note the Synced Groups and Synced Users



18. In your Workspace ONE Access admin console

- Select Settings
 - Select Login Preferences
 - Under Login Preferences
 - Select EDIT



- 19. In the Login Preferences area
 - In line with:
 - Sync Group Members to the Directory When Adding Group
 - select the Checkbox



20. In the Login Preferences area

- In the bottom right
 - select SAVE



21. In the Workspace ONE Access console

- select Integrations
 - select Directories

ccess	Q Search for users, groups, o
sources	Integrations Settings
	Directories (2)
_	Directory Name
ethods	System Directory
C	EUC-Livefire

- 22. In the **Directories** area
 - select EUC-Livefire

la		
¢	Tenant Admin 🗸	
		*
	▼ Sync	
_	Sync with Safeguards Sync without Safeguards	
	Sync Settings	
	Delete Directory	

- 23. In the **EUC-Livefire** directory area
 - In the right corner
 - Next to Sync
 - select the **dropdown**
 - select Sync without Safeguards



- 24. On your ControlCenter server
 - On the **Desktop**
 - Open the Remote Desktops\Site1 folder
 - Launch WS1-Connector.RDP

Part 1:Section 4: Configuring the AirWatch Cloud Connector



- 1. On the **WS1-Connector** desktop
 - Open your chrome browser
 - In the address bar, enter dw-livefire.awmdm.com,
 - Login using your registered course email (
 - password VMware1!

If you are unclear what your registered course email is. Go back to your lab document you configured and filled in on Day 1, in the introduction

If you have not completed this, then please do

	Cropp A Samp Horsey Da	a a
BETTING SETTING WORTON Dervices WORVORS	Graps > Al Settings C Hub Configuration	Groups & Settings
Set > Syster > Device > Apps > Conte	m es & Users	netr@vmware.com System Getting Sarted Branding Enterprise Integration Description
System Enterpr Certific Conten Cloud C Directo Email (S	erprise Integra rise Integration Services ate Authorities t Gateway connector ry Services SMTP)	ation ©

- 2. In the UEM Admin Console
 - Navigate to Groups & Settings > All Settings
 - Under Settings select System > Enterprise Integration
 - Under Enterprise Integration
 - select Cloud Connector

General Advance	d	
Current Setting	🔘 Inherit 🛞 Override	
Enable ArWatch Cloud Connector	ENABLED DISABLED Enables secure connection to enterprise components	
Enable Auto Update	ENABLED DISABLED Enabling Auto Update will seamlessly update the ArrWatch Cloud Contentor installed on your server after the corresponding AirWatch ConsShow More	
Child Parentistion +	Children and a Channels and a Relation of Cannels	

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



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

Password for the settings to a AirV	AirWatch Cloud Connect Vatch Cloud Connector (A	tor (ACC) certificate. You will (CC) server.	need this to import th
Your password n	nust be at least 6 charact	ers in length.	
Password *		Show	
Confirm		Show	
Password *			

- 5. On the **Download AirWatch Cloud Connector (ACC-installer.exe)**
 - Type VMware1! in the Password and Confirm Pasword boxes.
 - Select DOWNLOAD



- 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!
 - select Next
 - Select Next
 - Select Install
 - Select OK
 - Select Finish
 - Select Yes
 - Wait for the **WS1-Connector** server to reboot
 - RDP to the server and re-login

Workspace ONE" UEM	
Username nikko.guildan@gmail.com <table-cell> Remember Password</table-cell>	
Log In	
Login as a different user Trouble logging in	

- 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

Groups & Set	tings			
Groups	s & Settings			
Ma	anage advanced console-wide			
Gr	oups eate and manage custom named (
C.	eute une manage coston namea (
All	Settings tup, installation, Console settings,			
Co	onfigurations			
Es	tablish the foundational settings, c			
ne	ed to drive your business forward			
System				
-				
Enter	prise Integration			
Enterpris	Enterprise Integration Services			
Certificat	Certificate Authorities			
Content (Sateway			
Cloud Co	nnector			
Directory	Services			
Email (SN	ITP)			
VMware 1	funnel			
V/Murana 1	Fuenal Drawn			

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

• Under Enterprise Integration, select Cloud Connector

oud Connec to the VMware Er	tor Installer 🕁 nterprise Systems C	onnector Guide.		
O Inherit only	Override only	Inherit or Override		
	Reached Cloud C	onnector running version 20.	5AVE	TEST CONNECTION onnector (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 1:Section 5: Workspace ONE UEM & Active Directory Integration



- 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

LDAP - Active Direct	tory				÷
ENABLED					
controlsentes auc.li	uefire coro				
NONE	SSL :	START TLS	D		
389					
2					
2					
ENABLED C					
ANONYMOUS	BASIC	DIGEST	KERBEROS	NTLM	GSS-NEGOTI/
administrator					
0					

- 2. From the **Directory Services** Interface,
 - Under the Server Tab , enable the following .
 - Directory Type*: LDAP-Active Directory
 - DNS SRV: **Disabled (default)**
 - Server : ControlCenter.euc-livefire.com
 - Bind User Name: administrator
 - Bind Password: **VMware1!**
 - Domain: euc-livefire.com

System > Enterprise	Integration		
Server	User	Group	
Current Setting		Override	
Domain		Base DN*	
euc-livefire.com		DC=euc-livefire,dc=com	
User Object Class *	person		1
User Search Filter *	(&(objectC	ategory=person)(sAMAccountName=(Enrolime	()

- 3. From the Directory Services Interface,
 - Under the User Tab ,
 - Validate the following configuration is configured
 - Under Base DN,
 - ensure that **DC=euc-livefire,DC=com** has automatically populated.
 - If not, click on the + icon
 - 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	O Inherit () Override
Domain	Base DN*
euc-livefire.com	DC=euc-livefire,DC=cor
Group Object Class *	group
Organizational Unit Object Class *	organizationalUnit
> Advanced	
Child Permission	O Inherit Override 💿 Inherit or Override
t Connection	×
vefire.com Connection successful with the give password.	ven server name, bind username, and
Connection successful with the give password.	ven server name, bind username, and
vefire.com Connection successful with the give password.	ven server name, bind username, and
vefire.com Connection successful with the give password. TEST AGAIN Jser Group Jomain euc.ivefire.co v	ven server name, bind username, and
vefire.com Connection successful with the give password. TEST AGAIN Jser Group Jomain euc.ivefire.co v	ven server name, bind username, and

- 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
 - select Save
 - Scroll to the bottom of the page
 - Select TEST CONNECTION



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

Settings		
 Devices & Users 		
~ (General	
(Enrollment	
	Friendly Name	
	Lookup Fields	
	Message Templates	~
	Notifications	

- 6. Let's ensure users can enroll their devices using Active Directory credentials.
 - Under Settings ,
 - select **Devices & Users**
 - Select > General
 - Select > Enrollment

evices & Users >	General	
Authenticatic	Management Mo	Terms of Us
Current Setting	🔿 Inherit	🔘 Override
	1	
SAVE		

- 7. Under the **Enrollment** area
 - Select the **Override** radio button
 - Scroll down.

Authentication Models)	Z Basic Z Directory [Authentication Proxy	
Source of Authentication for Intelligent Hub	WORKSPACE ONE U	WORKSPACE O	
Devices Enrollment Mode *	Open Enrollment (O Registered Devices O	niy
) Inherit or Overri	de		
SA	VE		

8. Under the **Enrollment** area

- In line with Authentication Modes(s)
 - ensure the the **Directory** check box is selected
- In line with 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

Part 1:Section 6: Workspace ONE Access and Workspace ONE UEM Integration



- 1. In your Workspace ONE UEM Admin console
 - Navigate to Groups and Settings > All Settings > System > Enterprise Integration> Workspace ONE Access > Configuration

System > Enterprise Integration
Workspace ONE Access ⊘
Server
Establish trust between users, devices and the hybrid cloud for a seamless user experi-
CONFIGURE

- 2. Under the *Server* area,
 - Select CONFIGURE



- 3. On the Connect to Workspace ONE Access window,
 - Select CONTINUE

Connect to Worl	kspace ONE Access
	Overview 2 Credentials
This will help you	establish the connection between VMware Unified Endpoint Management and Workspace C
Tenant URL*	https://aw-hznadvintrnelpod20march.vidmpreview.com
Username *	administrator
Password *	••••••
	If you have forgotten your password, you can recover it on the Workspace ONE . password link has expired, please contact Workspace ONE UEM support.
Test to confirm V	Vorkspace ONE UEM and Workspace ONE Access are communicating securely.
TEST CONNEC	TION
	ificate ·
Test to confir	m Workspace ONE UEM and
TEST CON	NECTION
-	
Test connec	tion successful!
BACK	SAVE

- 4. On the **Connect to Workspace ONE Access** window enter the following:
 - Tenant URL: Your Tenant eg. https://aw-livefirehorizonrn.vidmpreview.com/

- User Name: Your Tenant Admin account
- Password: Your Tenant Password
- Select **TEST CONNECTION** to ensure Tenant configuration has been entered successfully.
- Select **SAVE** and close the settings window

🖏 Works	pace ONE UEM
GETTING STARTED	Groups
MONITOR	Configurations
DEVICES	
ACCOUNTS	
### APPS & BOOKS	
CONTENT	
EMAL	
TELECOM	
н	ZNADVINTRNELPOD26
> (>) ttin 2	Sroups & Settings > Configurations
	GO TO CONFIGURATIONS

- 5. In the Workspace ONE UEM admin console
 - 1. Select GROUPS & SETTINGS
 - 2. Select Configurations
 - 3. In the **Group & Settings > Configurations** window
 - Select GO TO CONFIGURATIONS

> ⊘	Groups & Settings > Configurations (i) Establish the foundational settings, customizatio
	Q Enter a name or category
>	Groups & Settings >
Ø	Configurations (i)
	Establish the foundational settings, custo
	Q int
	Configuration Name
	Intelligent Hub
	Microsoft Intune® App Protection Po
	Categories
	Dell Integration

- 6. Under **Configurations**
 - In the Enter a name or category area
 - Type Int
 - Under Configuration Name
 - Select Intelligent Hub



7. Under Hub Services

Select GET STARTED

Activate Hub Se	ervices	×
A Tenant has already be	een configured for Workspace ONE Access.	
Tenant URL	https://aw- hznadvintrnelpod20march.vidmpreview.com	
Do you want to use this	same Tenant to activate Hub Services?	
	NO	s

- 8. In the Activate Hub Services
 - Select YES

Part 1:Section 7: Workspace ONE Hub Services Integration with Workspace ONE Access



- 1. On your ControlCenter server
 - Open a new tab on your Browser
 - Paste your custom Workspace ONE Access URL in the address bar
 - Launch your custom Workspace ONE Access URL
 - In the Select Your Domain window

- Ensure **System Domain** is selected
- Select Next

Workspace ONE*	
Username	
Password System Domain	
Sign in	
Forgot Password?	
Change to a different domain	
vm ware [.]	

- 2. In the Workspace ONE Access login
 - Under **Username**
 - Enter your custom SysAdmin username
 - Under **Password**
 - Enter VMware1! (hopefully that is what you have changed it to)
 - Select Sign in



- 3. In the Web version of Intelligent Hub
 - In the top right corner
 - Select and right-click your Sysadmin Initial Icon
 - Select Workspace ONE Access Console



- 4. In the **Workspace ONE Access admin** console
 - Select Integrations
 - Select Hub Configuration

-	K 🛞 Workspace ONE Access 🛛 🗙 🗍 Gr			
w-livefirernpod22.vidmpreview.com/ws1-admin/#/works				
Horizon®	Site 1 🛛 UAG-HZN-01a 💆 UAG-HZN-01b 🔀			
cess	Q Search for users, groups, or applications			
ources	Integrations Settings			
	Hub Configuration			
	Review and edit settings to configure er			
hods	Hub Services			
	Hub Services lets you provide employee Services to deliver helpful, new features			
	00			
	Unified App Catalog			
	Highlight commonly used apps, promote as part of a campaign, display frequently			
	apps and more.			
	LAUNCH			

- 5. In the **Hub Configuration** window
 - Under Hub Services
 - Select LAUNCH



- 6. In the **Optimize the Intelligent Hub Experience** window
 - Select BEGIN



7. In the Welcome to Hub Services

- Review the associated options.
- In Section 8: We will configure Hub Services

Part 1:Section 8: Configuring Workspace ONE Hub Services



1. In Workspace ONE Hub Services

- Select the **Branding** section
 - Find Logos > Organization Logo , to the right select UPLOAD
 - In the left pane,
 - Under Quick access, select Desktop
 - Select Software
 - Select and open Logo
 - Select vmware livefire.png
 - Select Open
 - Scroll down
 - and select SAVE

Workspace ONE Hub Services		
Home Templates App Catalog Branding	People Allow employees to discover the Versions are not available for this feat	
Custom Tab Employee Self-Service Notifications	Global Settings These default settings will be us	
Passport People Virtual Assistance New Hire Welcome	People	
System Settings	SAVE	

2. In the Workspace ONE Hub Services page

- In the left pane, select **People**
- Under People area,
 - next to Enable People,
 - move the **toggle** to the right
- Select **SAVE**

Workspace ONE Hub S	ervices		LOG OUT OF HUB SE
Home Templates App Catalog Branding	Custom Tab Define an additional tab in In VERSION: GLOBAL ~	teligent Hub.	
Custom Tab	You may still add a versio	n to use in a temptate even if the feature is off at the global level.	
Notifications Passport	Global Settings These default settings will be	used by Intelligent Hub unless overriden by a template assignm	ient.
Virtual Assistance	Indicate whether to enable a	custom tab by default for your organization.	
New Hire Welcome	Enable Custom Tab		
System Settings	Android and IOS		
	Web		
	Open Link in (Web)	New Tab Hub Embeddied iFrame Specify if the URL should open in a new browser tab or an Frame embedde Frame is selected, ensure the webpage is Frame compatible.	ed inside Hub Web. If
	Title	EUCLF	
	URL	https://www.Livefire.solutions	
	Position	First Last	
	SAVE		

- 3. In the Workspace ONE Hub Services page
 - From the left menu,
 - Select the Custom Tab.
 - Next to Enable Custom Tab,
 - move the **toggle right**.
 - Next to Web
 - move the **toggle right**.
 - Next to **Title**
 - enter: **EUCLF** (Best practice is not use a label longer than 6 characters).
 - Next to **URL**:
 - enter https://www.Livefire.solutions
 - Next to Position,
 - enable the **First radio button**.
 - Select **SAVE**

0	-	Ľ	×
	☆		:
	≣	Readin	ig list
LOG OUT OF HUB SERVICES	Tena	nt Adn	nin
			1

4. To the top right of the Workspace ONE Hub Services page
Select LOG OUT OF HUB SERVICES



- 5. In the **Workspace ONE Access** Console
 - Under Integrations
 - Select People Search



6. In the **People Search** area

- Next to Directory,
 - from the dropdown
 - Select the EUC-Livefire
 - Select NEXT

People Search onfigure settings for the Intelligent Hub People tab, 1	which allows employees to search for colleagues and view details such	as photos ar
Select a directory		
 Select user attributes 		
Select and map the user attributes to display Search page will not remove them from direc	on the People tab. Mapped attributes are displayed on the Directory S tory mapped attributes. To modify user attributes, go to User Attribute	Sync Settings es
Mapped User Attribute Name	Active Directory Attribute Name	
Mapped User Attribute Name Default Attributes	Active Directory Attribute Name	
Mapped User Attribute Name Default Attributes Use title *	Active Directory Attribute Name	
Mapped User Attribute Name Default Attributes title * managerDN *	Active Directory Attribute Name	manag
Mapped User Attribute Name Default Attributes title * managerDN * distinguishedName *	Active Directory Attribute Name	manag
Mapped User Attribute Name Default Attributes title * managerDN * distinguishedName * objectGuid (Custom)	Active Directory Attribute Name	manag
Mapped User Attribute Name Default Attributes title * managerDN * distinguishedName * objectGuid (Custom) sid (Custom)	Active Directory Attribute Name	manag
Mapped User Attribute Name Default Attributes title * managerDN * distinguishedName * objectGuid (Custom) sid (Custom)	Active Directory Attribute Name	manag
Mapped User Attribute Name Default Attributes title * distinguishedName * objectGuid (Custom) sid (Custom) NEXT	Active Directory Attribute Name	manas

- 7. In the **People Search** page
 - Step 2 Select User attributes
 - note the attributes
 - Scroll down
 - In the bottom left
 - Select NEXT

ces	Integrations Settings			
	People Search Configure settings for the Intelligent Hub People tab, which allows employe			
ls	> Ø Select a directory			
	>			
	 Select users and sync to directory 			
	Select users by entering the distinguished names (DN). To include Services People tab.			
	User DNs ou=corp.dc=EUC-Livefire.dc=com Ex: "CN=admin.CN=users.DC=mycompany.DC ADD			
	SAVE & SYNC SAVE			

- 8. In the **People Search** page `
 - Step 3 Select users and sync to directory
 - review the User DNs
 - It should read
 - ou=corp,DC=euc-livefire,DC=com
 - Select **SAVE & SYNC**

burces	Integrations Settings
	People Search Configure settings for the Intelligent Hub People tab, w
notis	SYNC DIRECTORY SYNC PHOTOS DELETE
	Sync Status Directory and photo sync runs in the background. Vie
	Last directory sync 🛆 Oct 28
	Last photo sync () Not sta
	Photo sync frequency Manua
	VIEW SYNC LOG

- 9. Under People Search
 - Select SYNC DIRECTORY

Part 1:Section 9: Enrolling Intelligent Hub on Microsoft Windows 10





- 1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the Site1 folder
 - Select the W10Client-01a RDP client and
 - Sign-in with
 - username: mark@euc-livefire.com
 - Password: VMware1!
 - To the right of the **Start** button
 - in the **search** area,
 - start typing intel
 - Select the Workspace ONE Intelligent Hub
 - Please Note! If the Workspace ONE Intelligent Hub does not load,
 - From the RUN > Services.msc > Start the Airwatch service
 - Attempt to **re-launch** the hub



- 2. Under Email or Server Address,
 - Enter https://dw-livefire.awmdm.com
 - Select Next

•••	Groups & Settings > Groups	🗙 🐤 Login Salesforce 🛛 🗙 🔷 Favorites Inte
$\ \ \leftarrow \ \ \rightarrow \ \ G$	습 â dw-livefire.awmdn	n.com/AirWatch/#/AirWatch/Menu/ConfigAndSettings/Gro
Apps 💿	UEM M Gmail 🗘 Access	Snagit Keyboard S
🖏 Works	pace ONE UEM	HorizonINTRN
GETTING STARTED	Groups All Settings	Organization Group HorizonINTRN Group ID HorizonINTRN Settings
MONITOR	Configurations	Manage dvanced console-w
Workspace ONE In	ntelligent Hub	
	Email o https	r Server Address //dw-livefire.avemdm.com
	Group	D
	Horiz	IONINTRN
		Next
		Cancel

- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE** UEM tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select NEXT



- 4. In the **Workspace ONE Intelligent Hub** under
 - Under Select Your Domain
 - Select euc-livefire.com
 - Select Next
 - Under the **Username** area
 - Enter Mark
 - Under the **Password** area
 - Enter VMware1!
 - Select Sign in



- 5. In the Workspace ONE Intelligent Hub
 - Select I Agree



- 6. On the **Congratulations** window,
 - Select Done
 - Re-open the Intelligent Hub
 - Select Get Started

Step 2 : Enrolling W10Ext-01a on Site 1 with the Active Directory Domain User Jill



- 1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the Site1 folder
 - Select the W10EXT-01a.RDP client and
 - Sign-in with

A

- username jill@euc-livefire.com
- Password VMware1!
- To the right of the **Start** button in the search area, start typing **intel**
- Select the Workspace ONE Intelligent Hub
 - Please Note! If the Workspace ONE Intelligent Hub does not load,
 - From the **RUN** > **Services.msc** > Start the **Airwatch s**ervice
 - Attempt to **re-launch** the hub



- 2. Under Email or Server Address,
 - Enter https://DW-livefire.awmdm.com
 - Select Next



- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE** UEM tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select NEXT



- 4. In the Workspace ONE Intelligent Hub under
 - Under Select Your Domain
 - Select euc-livefire.com
 - Select Next
 - Under the **Username** area
 - Enter Jill
 - Under the **Password** area
 - Enter VMware1!
 - Select Sign in



- 5. In the Workspace ONE Intelligent Hub
 - Select I Agree



- 6. On the **Congratulations** window,
 - Select Done
 - Re-open the Intelligent Hub
 - Select Get Started

Step 3 : Enrolling W10Client-02a on Site 2 with the Active Directory Domain User Fernando



- 1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the Site2 folder
 - Select the W10Client-02a RDP client and
 - Sign-in with
 - username fernando@euc-livefire.com
 - Password VMware1!
 - Select OK
 - To the right of the **Start** button in the search area, start typing **intel**
 - Select the Workspace ONE Intelligent Hub
 - Please Note! If the Workspace ONE Intelligent Hub does not load,
 - From the RUN > Services.msc > Start the Airwatch service
 - Attempt to re-launch the hub

Workspace CNE Intelligent Hub		-		х
			Ô	
	0			
	Sec. 20			
	Email or Server Address			
	https://dw-livefire.awmdm.com			
	Next			

- 2. Under Email or Server Address,
 - Enter https://dw-livefire.awmdm.com
 - Select Next

•••	Groups & Settings > Groups	🗙 🐤 Login Salesforce	🗙 📔 🤤 Favorites Inte		
$\ \ \leftarrow \ \ \Rightarrow \ \ \mathbf{G}$	습 @ dw-livefire.awmdm	.com/AirWatch/#/AirWatch/Menu	/ConfigAndSettings/Groi		
🚻 Apps 👘	UEM 附 Gmail 🗯 Access	Snagit Keyboard S			
🕲 Works	Workspace ONE UEM HorizonINTRN				
GETTING STARTED	Groups	Organization Group HorizonINTRN Group ID			
MONITOR	Configurations	HorizonINTRN	dvanced console-w		
Workspace ONE In	stelligent Hub				
Email or Server Address					
	Group	D			
	Horiz	onINTRN			
		Next			
		Cancel			

- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE** UEM tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select NEXT



- 4. In the **Workspace ONE Intelligent Hub** under
 - Under Select Your Domain
 - Select euc-livefire.com
 - Select Next
 - Under the **Username** area
 - Enter Fernando
 - Under the **Password** area
 - Enter VMware1!
 - Select Sign in



- 5. In the Workspace ONE Intelligent Hub
 - Select I Agree



- 6. On the Congratulations window,
 - Select Done
 - Re-open the Intelligent Hub
 - Select Get Started

Step 4: Enrolling W10Ext-02a on Site 2 with the Active Directory Domain User Tom



- 1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the Site1 folder
 - Select the W10EXT-02a.RDP client and
 - Sign-in with
 - username tom@euc-livefire.com
 - Password VMware1!
 - To the right of the **Start** button in the search area, start typing **intel**
 - Select the Workspace ONE Intelligent Hub
 - Please Note! If the Workspace ONE Intelligent Hub does not load,
 - From the RUN > Services.msc > Start the Airwatch service
 - Attempt to **re-launch** the hub



- 2. Under Email or Server Address,
 - Enter https://dw-livefire.awmdm.com
 - Select Next

•••	Groups & Settings > Groups	🗙 🐤 Login Salesforce 🛛 🗙 🔷 Favorites Inte
$\ \ \leftarrow \ \ \rightarrow \ \ G$	습 â dw-livefire.awmdn	n.com/AirWatch/#/AirWatch/Menu/ConfigAndSettings/Gro
Apps 💿	UEM M Gmail 🗘 Access	Snagit Keyboard S
🖏 Works	pace ONE UEM	HorizonINTRN
GETTING STARTED	Groups All Settings	Organization Group HorizonINTRN Group ID HorizonINTRN Settings
MONITOR	Configurations	Manage dvanced console-w
Workspace ONE In	ntelligent Hub	
	Email o https	r Server Address //dw-livefire.avemdm.com
	Group	D
	Horiz	IONINTRN
		Next
		Cancel
- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE** UEM tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select NEXT



- 4. In the **Workspace ONE Intelligent Hub** under
 - Under Select Your Domain
 - Select euc-livefire.com
 - Select Next
 - Under the **Username** area
 - Enter tom
 - Under the **Password** area
 - Enter VMware1!
 - Select Sign in



- 5. In the Workspace ONE Intelligent Hub
 - Select I Agree



- 6. On the **Congratulations** window,
 - Select Done
 - Re-open the Intelligent Hub
 - Select Get Started

Part 2. Integrating Workspace ONE Access with Horizon Cloud services

In Part 2 , we will work through the requirement to setup a federation with Horizon Cloud Services and Workspace ONE Access.

The approach to federating Horizon Cloud Services with Workspace ONE Access differs from the approach we following with on-premises Horizon PODS

Part 2: Integrating Workspace ONE Access with Horizon Cloud services



- 1. In the Workspace ONE Access Console
 - Select Settings
 - Under Settings
 - Select OAuth 2.0 Management



- 2. In the **OAuth 2.0 Management** window
 - Select ADD CLIENT

Res	sources	Integrations	Settings					
	OAU save	th 2.0 M	anageme	ent > 4	dd (Client		
t	A secre	et will be availab	e and autogenera	ated when yo	u click sav	ve		
	Access type*				Service Client Token 🗸			\sim
	Client ID*				HZNxxINTCorp Characters allowed are: alphanumeric (A-Z, a-z, 0-			0-
					9) period sign (@). 2	(.), underscore (_) 56 characters ma	, and hyphen (-) an x.	id at
	Scope	E .			Admin			
	Access	token time-to-liv	e (TTL) *		3	hours		\sim
	Idle to	ken TTL			10	days		\sim
	Token type				Bearer			

3. In the Add Client interface

- Configure the following information next to:-
 - Access Type*,
 - select Service Client Token
 - Client ID*,
 - type HZNXXINTCorp
 - (xx is your POD ID)

Select SAVE

Resources Integrations Settings					
OAuth 2.0 Management > HZN22INTCorp					
Client Information					
Copy the shared secret before leaving this page, or you will need to regenerate the secret.					
Client ID HZN22INTCorp					
Shared Secret					
<pre>* "new 1 - Notepad++ [Administrator] iie Edit Search View Encoding Language Settings Tools Macrc</pre>					

- 4. In the **OAuth 2.0 Management** window
 - **COPY** the **Client ID**
 - **COPY** the **Shared Secret**
 - Save to Notepad++ on the ControlCenter server

Don't move from this page until you have saved the **Client ID** and **Shared Secret**



- 5. On your Site 1 profile Chrome browser
 - On the **Favourites** bar
 - Select HZN Cloud

My VMware Cr	edentials	
Username		
Password		C
Remember m	ne	

- 6. On the **Welcome to VMware Horizon**® page
 - Under My VMware Credentials, enter the following
 - In the **Username** area,
 - type your, assigned Horizon Cloud email
 - In the **Password** area,
 - type , VMware1!
 - Select LOGIN

vMware Horizon®	
Active Directory Credentials	
Username	
Password	۵
EUC-LIVEFIRE	~

- 7. On the **Welcome to VMware Horizon**® page
 - Under Active Directory Credentials, enter the following
 - In the **Username** area,
 - type Administrator

- In the **Password** area,
 - type , VMware1!
- Select LOGIN

ead about new and existing features below and visit our community site for tij	ps, tricks, and to ask any questions!
January 2022: • LDAPS can now be selected as the protocol when registering Active Dir it and the pods are on this release's manifest level. To request enablem 2006085 • Unified Access Gateway logs can now be sent to a syslog server Dynamic Environment Nanager can now distinguish between internal ar • Session data for users connecting through Universal Broker will now she A notice will now be shown in the Horizon Universal Broker will now the • A notice will now be shown in the Horizon Universal Broker will now the • When using image Management Service (IMS) with Horizon pods, you C • Windows Server 2018 is now a supported OS for Horizon pods Select "What's New" from the Help menu to view these notes at any time. I	ectory. This feature is available when your tenant is explicitly enabled for int, you must file a support request as described in VMware KB article vid external users when connecting through Universal Broker w breakdown of logon segments instrator if the Unified Access Gateway is upgraded and there may be a IP addresses an now select which pods the multi-pod images are copied to Previous Notes

- 8. In the What's New in Horizon Cloud window
 - Turn off the toggle next to :-
 - Continue to show this Notification
 - Select CLOSE



- 9. In the Horizon Universal Console
 - Expand Settings
 - Under Settings,
 - Select Broker

(-							
🗅 🔒 cloud	horiz	on.vmware.com/h	orizonadmin/#/	app/bro	oker/overview				
y-ip.livefire.lab/ip	vm	Horizon®Site 1	NSX manager	🍦 Ap	p Volumes Site 1	M UA	3-HZN-01a	UAG-HZ	N-01b
Iniversal Conso	le	Q Users 🗸	Search he						
	~	Dreker							
	>	Blokel				~			
tops & Apps	>	Overview	Network Ran	ges	Client Restr	ictions	Identity	& Access	
	>	Universal	Broker 🧷						
	~								
tings		Status 🔵 EM	ABLED						
tory									

10. In the **Broker** area

Select the Identity & Access tab

✓ 1.	Provide Workspace ONE Acces	ss Cloud Tenant	
	Add an existing Workspace ONE A	Access cloud tenant.	
	Workspace ONE Access Cloud Tenant *	Add existing cloud tenant	_ (ì
		https://aw-livefirernpod22b.vidmpreview.com	-
	Provide the following information f	from the Workspace ONE Access console.	
	OAuth Client ID *	HZN22INTCorp	í
	Shared Secret *	Gbnu322YRUqk7obpZ39udPLkKuPRScFF	í
	I have read and agree to the Tern	ns of Service.	
	NEXT		

- 11. In the Workspace ONE Access and Intelligent Hub window
 - 1. Provide Workspace ONE Access Cloud Tenant section
 - Enter the following next to:
 - Workspace ONE Access Cloud Tenant*
 - select Add existing cloud tenant cloud tenant.
 - Under Add existing cloud tenant cloud tenant.

- enter your assigned Access tenant FQDN
- Next to : -
 - OAuth Client ID * : enter your recorded Client ID
 - Shared Secret * : enter Your Shared Secret
- Select the check box, next to :-
 - I have read and agree to the Terms of Service.
- Select NEXT



- 12. In the Workspace ONE Access and Intelligent Hub window
 - · In the following sections:-
 - 2. Complete Workspace ONE Access and Horizon Prerequisites section
 - Note the following requirements before you carry one:
 - Expand the Provide Workspace ONE Access Cloud area above step 2.:
 - Note your tenant information
 - Select NEXT

www Horizon Universal Console					
Intelligent Hub with Workspace ONE Access provides your end users with a single destination for company resources. Follow these steps to activate Intelligent Hub.					
< Assign Desktops & Apps >	Intervention of the second sec				
 Settings ~ General Settings 	✓ ⊘ Provide Workspace ON	IE Access Cloud Tenant			
Active Directory Users & Groups Roles & Permissions	Region Tenant Name	Preview aw-livefirehznrnpod21			
Capacity	URL.	https://aw- ivefirehznrnpod2l.vidmpreview.com			
Getting Started	> ⊘ Complete Workspace C	ONE Access and Horizon Prerequisites			
Broker	✓ 3. Activate Intelligent Hub)			
	ACTIVATE				
> 🥥 Provide Work	> Ø Provide Workspace ONE Access Cloud Tenant				
> 🥥 Complete Wo	> O Complete Workspace ONE Access and Horizon Prere				
✓ 3. Activate Intel	 Activate Intelligent Hub 				
⊖ in Progres	⊖ In Progres				

13. In the **Workspace ONE Access and Intelligent Hub** window

- · In the following section:-
 - 3. Activate Intelligent Hub
 - Select ACTIVATE



14. In the **Workspace ONE Access and Intelligent Hub** window

- Under the Workspace ONE Access Cloud Tenant area
 - select the **checkbox** next to
 - I have verified that end-users can access virtual desktops and apps in Intelligent Hub.
 - Select CONFIRM

Favorites Intelligent Hul	🗴 🗙 🛛 🔅 VMware Workspace ONE 🛛 🗙 📄 🗰 Workspace ONE Intelligence 🗙 🛁 Horiz
< → C ☆ (■)	doud.horizon.vmware.com/horizonadmin/#/app/broker/access
🔢 Apps 🕤 my-ip.livefire.	lab/ip 🧮 Horizon®Site 1 📫 App Volumes Site 1 🧰 UAG-HZN-01a 🗯 UAG-HZN-01b 📀 vCenter
	Onboard VMware Cloud Services Platform to unlock more capability!
vmw Horizon Universal Console	Q, Users ↓ Search here
 Monitor Assign Desktops & Apps Inventory Settings General Settings Active Directory 	Broker Overview Network Ranges Client Restrictions Identity & Access Authentication Workspace ONE Access and Intelligent Hub REMOVE TENANT
Users & Groups Roles & Permissions Capacity Licenses Getting Started	Workspace ONE Access Cloud Tenant To require end users to authenticate to and access desktops and apps using Workspace ONE Intelligent Region Preview

15. In the **Broker** window

- Notice you now have an Authentication tab next to Identity & Access
- Select the Authentication Tab

ersal Conso	1e	Q Users V Search here
s & Apps	« > > >	Broker Overview Network Ranges Client Restrictions Identity & Access Authentication Authentication Configure and manage two-factor authentication and Intelligent Hub access for end users.
ions		Workspace ONE Intelligent Hub Enforcement () //

- 16. In the **Broker** window
 - Under the **Authentication** tab
 - Next to Workspace ONE Intelligent Hub Enforcement
 - select the **Pencil Icon**



- 17. In the Edit Intelligent Hub Enforcement window
 - Next to Enforce Intelligent Hub
 - Select the **toggle** and move it to the right

Edit Intelligent Hub Enforcement ×					
Force internal or external end users to authenticate to and access desktops and apps using the intelligent Hub app.					
Enforce Intelligent Hub	•				
Allow Different Intelligent Hub Redirection for internal and external users	•				
Enforce for end users	Internal Users 🔲 External Users				
	CANCEL	AVE			

- 18. In the Edit Intelligent Hub Enforcement window
 - Select SAVE

Part 3 : Testing client integration with the Universal Broker platform

In this part of the we will test our configuration and view how this works

This part also serves as an introduction to Part 4 as to why we need VMware Horizon TRUESSO

Part 3: Testing client integration with the Universal Broker platform



- 1. On your ControlCenter server
 - Open your Remote Desktops folder
 - Open the Site 1 folder
 - Launch w10Client-01a.RDP

Windows Security ×					
Your credentials did not work					
Your system administrator does not allow the use of saved credentials to log on to the remote computer 172.16.30.40 because its identity is not fully verified. Please enter new credentials. mark@euc-livefire.com					
••••••					
The logon attempt failed More choices					
ОК	Cancel				

- 2. In the **Windows Security** window
 - Under mark@euc-liveifire.com
 - enter VMware1! as the password
 - Select OK



- 3. On the W10client-01a desktop
 - Launch your Chrome browser
 - In the Chrome browser address bar
 - enter your Assigned Workspace ONE ACCESS Url
 - e.g. https://aw-livefirernpod25.vidmpreview.com/

- On your keyboard
 - select ENTER

5 W10Client	01 - 172.16.30.40 - Remote Desktop Connection
Revelation -	VMware - Workspace ONE × +
and year and	← → C a w-hznadvintmelpod20march.vidmpreview.com/authcontrol/auth/request
Microsoft Bolge	
Canad Canad Pand	0
selfaure (92.68.01.	Workspace ONE"
6	System Domain 🗸
a Georgia Chaesna	System Domain euc-livefire.com
A North	Next
ebyer	vmware

- 4. In the **Workspace ONE** auth page
 - Under Select Your Domain
 - From the **dropdown**
 - Select euc-livefire.com
 - Select Next

	Workspace ONE*	
U N	isername Aark	
F	assword	
١.	euc-livefire.com	
	Sign In	
	Forgot password?	
	Change to a different domain	
	vm ware:	

- 5. In the **Workspace ONE** auth page
 - Under **username**
 - type Mark
 - Under **password**
 - type VMware1!
 - Select Sign In

Workspace ONE Intelligent Hu	b
=	Apps
CO EUCLF	
Savorites	Q Search Apps
8 Apps	New Apps All Apps Categories V
People	
E For You	New Apps
Support	Corp25-Asst corp25hzn Internet Explorer
Mark Debio	All Apps

- 6. In the Intelligent Hub console
 - Note that now you have your Desktop Entitlement and Published Application
 assignments
 - Launch your CorpXX-HZN
 - XX is representative of your assigned POD ID



- 7. In the Horizon Client window
 - Select Launch

		×
Password Request		
We need your password to sign in to Corp20-HZNb.		
Password		
	Cancel	Sign In

- 8. In the Password Request window
 - Note that you have not received a Single Sign-On experience
 - For Password-based authentication we can solve this
 - With any other authentication method, only the use of VMware Horizon TRUESSO will solve this
 - Select Cancel



- 9. On your ControlCenter server
 - Revert back to your Workspace ONE Access Admin Console
 - Select the Settings tab
 - Under Settings
 - Select Login Preferences
 - Under Login Preferences

• Select EDIT

Workspace ONE Access login page in iFrame	es	
Cache passwords	٩	
Customize sign-in prompt	١	

10. Under Login Preferences

- Scroll down
- Next to Cache passwords
 - Select the Checkbox



11. Under Login Preferences

- To the bottom right. corner of this window
 - Select **SAVE**



12. On the Controlcenter server

- Revert back to your W10Client-01a.rdp session
 - Sign out of your existing Intelligent Hub session
 - Close your browser



- 13. On the **W10client-01a** desktop
 - If necessary
 - Close your Chrome browser
 - Re-Launch your Chrome browser
 - In the Chrome browser address bar
 - enter your Assigned Pod broker ID
 - e.g. brokerXX.euc-livefire.com
 - XX represents your assigned POD ID

- On your keyboard
 - select ENTER

5 W10Client	01 - 172.16.30.40 - Remote Desktop Connection
0	VMware - Workspace ONE × +
negaran	← → C a aw-hznadvintmelpod20march.vidmpreview.com/authcontrol/auth/request
Meresek töge	
Cantrol Rand	0
selfaure 192-168-11.	Workspace ONE"
\bigcirc	System Domain
Geogle Chrome	euc-livefire com
	Next
atayar	vmware

- 14. In the **Workspace ONE** auth page
 - Under Select Your Domain
 - From the **dropdown**
 - Select euc-livefire.com
 - Select Next

	Workspace ONE*	
U N	isername Aark	
F	assword	
١.	euc-livefire.com	
	Sign In	
	Forgot password?	
	Change to a different domain	
	vm ware:	

- 15. In the **Workspace ONE** auth page
 - Under **username**
 - type Mark
 - Under **password**
 - type VMware1!
 - Select Sign In

	Q Apps Wwww.intelligent Hub x +
pilo Bas	← → C # am-hznadvintme/pod20march.vidmpreview.com/catalog-portal/ui#/apps
2	Pavorites Apps People For You Support.
ensk By:	Q Search Apps
anted Facel	New Apps All Apps Categories -
e e	New Apps
481.01_	
	Calculator Calculator Carp20-HZNb Corp20-
	Calculator Harizon

- 16. In the Web version of the Intelligent Hub
 - Under **Apps**
 - Launch your **Desktop Assignment**

Open VM	/ware Horizon Client?	
https://a	aw-hznadvintrnelpod20march.vidmpreview.com wants to open this application.	
Z Alwa	ways allow aw-hznadvintmelpod20march.vidmpreview.com to open links of this type in the associ	ated app
	Open VMware Horizon Client	Cancel
VMware H	Horizon Client	_
مہ	Drive Sharing	
مہ	Do you want to share your removable storage and local files when using remote desktops and applications?	
	Permit access to your removable storage and local files C:\Users\Mark	
	For more choices, go to Settings > Drive Sharing	
	Do not show this dialog again	
	Allow Deny	

17. In the Open VMware Horizon Client?

- Next to Always allow YOURSERVER.vidmpreview.com to open links of this type in the associated app
 - select the **Checkbox**
- Select Open VMware Horizon Client
- When prompted by the VMware Horizon Client for Drive Sharing
 - Select Allow



- 18. In your Horizon Client Session
 - Note that you were not prompted a second time for a password
 - This will only work provided you authenticate with a password on Workspace ONE Access and Password caching remains enabled.
 - Password Caching was disabled in **Workspace ONE Access** as a default configuration for security reasons.
 - We will now look at Part 4 and the implementation of VMware Horizon TRUESSO to allow for a single sign on experience, irrespective of the Authentication method, even when Password Caching feature is disabled.

Part 4: Integration VMware Horizon TRUESSO with Horizon Cloud services

When using Horizon with Workspace ONE Access and a 3rd Party Authentication method, the only way we can get a good user experience with Single Sign-On is to deploy Enrollment Services also known as TRUESSO.

We will not be deploying Horizon Enrollment services but integrating it with Horizon Cloud and seeing how it works with Workspace ONE Access.

Part 4 Section 1: Deploying a Workspace ONE UEM - Certificate Profile



- 1. On your ControlCenter server
 - Switch to your **custom UEM Saas Tenant**
 - If necessary, authenticate using your Saas Admin credentials



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

Certificate	
Enable Workspace ONE UEM certificate provisi authentication adapters.	oning for use with Works
Certificate Provisioning	ENABLE

- 3. In the Workspace ONE Access area
 - Below Certificate
 - Next to Certificate Provisioning
 - Select ENABLE

Certificate	
Enable Workspace ON Mobile SSO. Export th Workspace ONE Acces	E UEM certificate provisioning for use with Workspace ONE Access and e issuer certificate on this page so that you can establish trust with is authentication adapters.
Certificate	Type Pfx
	Valid Fro 5/16/2020
	Valid To 5/18/2040
	Thumbp 86C33DC6D225BD01B536AD684BA191AD234EEB30
Issuer Certificate	EXPORT
This type of want to ke	of file can harm your computer. Do you Discard Discard Discard
📮 VidmAirWat	chRootcer ^

- 4. In the Workspace ONE Acces window
 - Scroll down to the Certificate area
 - Select EXPORT
 - At the bottom of your browser
 - select Keep
 - Note this will download :-
 - VidmAirWatchRootCertificate.cer
 - To close the **Settings** window
 - Select X



- 4. From the UEM Console
 - Navigate to Devices > Profiles & Resources > Profiles
 - Select > ADD > Add Profile



- 5. In the Add Profile window
 - Select Windows > Windows Desktop > User Profile

• Next to Name* enter: W10 - SCEP - SSO .

Managed By	HZNServicesADVINTMarchRNELPOD20	
Smart Groups	All Devices (HZNServicesADVINTMarchRNELPOD20)	×
	Start typing to add a group	٩
Exclusions	NO YES	
	VIEW DEVICE ASSIGNMENT	

- 6. In the **General** tab,
 - Scroll down to Smart Groups
 - Select All Devices(YOUR SAAS Tenant)

· · · · · · · · · · · · · · · · · · ·	
General	
VPN	
Credentials	
Windows Hello	
Single App Mode	SCEP
Web Clips	CONFIGURE
Exchange ActiveSync	
SCEP	
Exchange Web Services	

7. In the Add Profile window

- In the left inventory menu
 - Navigate down to the SCEP tab
 - Select SCEP
- In the SCEP area
 - Select CONFIGURE

ind Paylood	SCEP	
General VPN	Credential Source	AirWatch Certificate Authority
Credentials	Certificate Authority *	AirWatch Certificate Authority
Windows Hello Single App Mode	Certificate Template *	Single Sign-On
Web Clips	Key Location	Software
SCEP (1)		
	0 0	

- 8. In the **SCEP** window
 - Change the following:
 - Next to :
 - Key Location: from the dropdown
 - select Software
 - At the bottom right of the window
 - Select SAVE AND PUBLISH

reself in text scalors	Enencry Name User
Added Science	H2NServicesADVINTMarchRNELP0020 VM Mark
Added	H2NServicesADVINTMarchRNELPO020 VM Jill
Added	HZNServicesADVINTMarchRNELPO020 VM Fernando
Added	H2NServicesADVINTMarchRNELPOD20 VM Tom

- 9. In the View Device Assignment page
 - Confirm your devices are showing
 - In the bottom right corner
 - Select PUBLISH

Part 4 Section 2: Configuring Workspace ONE Access for Certificate Authentication



- 1. On your ControlCenter
 - Switch to your custom Saas **Workspace ONE Access** tenant
 - In the **Workspace ONE** Login
 - Under Select Your Domain
 - Select System Domain,
 - Select Next
 - Under Username
 - type administrator
 - Under Password
 - type VMware1!
 - Select Sign in

)1a 📮 Horizon Clie	ent 🔘 UEM 🤹 Access	
		ТА
	TA Tenant Admin	
	Workspace ONE Access Console	
	Manage Hub Experience	-
	Account	
	Sign out	G

- 2. In the Intelligent Hub Console
 - Top right corner
 - Select the **TA** icon
 - Select Workspace ONE Access Console

	pouzzo.wumpreview.com/wsr-aummy.
S my-ip.livefire.lab/ip 🧰 Horizon®Site	1 🚾 UAG-HZN-01a 🚾 UAG-HZN-01
 VMware Verify will reach end-of-availat migration paths. New updates available. Learn what's new 	bility date (EoA) and end-of-support (EoS) w in <u>Workspace ONE Access SaaS release</u>
(R) Workspace ONE Access	Q Search for users, groups, or ap
Monitor Accounts Resources	Integrations Settings
Authentication Methods Connectors	Authentication Met
Directories	
Connector Authentication Methods	Important: When you disable an au
Hub Configuration	policy rules to select another auth
Identity Providers	CONFIGURE
Magic Link	Authentication Method
Okta Catalog	
People Search	
UEM Integration	Certificate (cloud deployment)
	Device Compliance (with Works)

2. In the Workspace ONE Access admin console

- Navigate to the Integrations tab
 - In the Integrations area, validate you are in Authentication Methods
 - Next Certificate (Cloud Deployment)
 - Select the **pencil icon**

Certi	ificate (cloud deployment)
Enable	Certificate Adapter ()
	Yes
Root ar	nd intermediate CA certificates (j)
SELEC	
Upload	led CA Certificates
-	
User Id	entifier Search Order (j)
upn] s	subject

- 3. In the **Certificate (Cloud Deployment)** page
 - Below Enable Certificate Adapter
 - Below Root and Intermediate CA Certificates
 - select SELECT FILE...

Image:	Cipen.								×		
Image: Section	0 - + + 🕹 × Th	is PC > Downloads >			~ (0	Search Downloads		,p		
Image: Street	Deservice - New Feide										
 wind wind wind wind wind wind wind wind		Narra A	Data readilized	Tops	See						
Image:	Quick access	duration	SOLUTION IN ALL ARE	Challen -							
No	Desktop 🖉	download	2/5/2022 12/06 204	File folder							
Winter	🐥 Deveniceds 🛛 🖈	usadeology 2011	204/2022 12:03 444	File folder							
Image: State Stat	🖹 Decuments 🛛 🥓	AirWatch Cloud Connector 21.11.0.3 Inst.	3/7/2022 12:51 PM	Application	26,254.63						
Output Image: Distribution in the configure i	E Fichares 🚽	 desitop.ini 	2/16/2022 10:59 AM	Configuration sett	1.63						
Bit B	Cartificate Bundle	🗵 download.sip	3/4/2022 10:06 AM	Compressed (sipp	17 68						
Image: State Stat	Stat	as-comfigition	3/TV2022 T1:56.4M	JSON File	2.68						
Image: Control of the selected file?	58x2	SectionN(Q3N2NkZTktNThnZC001Tk3L	3/16/2022 10:11 AM	MSRCINCIDENT Nie	1.63						
Image: State of the state	Sectorn 32	SectionNpQ3N2NkZTktNThhZC00/Tk3L	3/8/2022 0:57 PM	MSRCINCIDENT Riv	1.63						
Image: Strate Image: Strate <td< th=""><th></th><th>Wdrwfu/WatchRootCertificate.cer</th><th>3/11/2022 1/36 PM</th><th>Security Cetalicate</th><th>1.63</th><th></th><th></th><th></th><th></th><th></th><th></th></td<>		Wdrwfu/WatchRootCertificate.cer	3/11/2022 1/36 PM	Security Cetalicate	1.63						
Provent Book and	THE PC										
Interest Structure Stru	ab Objecti										
Browneds Market Mare	Destoop										
Write	Decuments										
Weiler Franker	Downloads										
The field in the f	Music										
Interference Statestytestytestytestytestytestytestytes	 Picture 										
Terrent Valuation Adapter Are you sure you want to upload the selected file? NO YES	Tideos										
Next Image: Interface Image: Interface Update Authentication Adapter X Are you sure you want to upload the selected file? NO	Local Disk (Cr)										
The restrict (Mathematical Street (%) (Mathema	Network										
Perene Valuation Adapter version are you sure you want to upload the selected file?											
The resex To be a constrained of the selected file?											
Update Authentication Adapter	Tin er	and Market Market Market Sciences					All Play II IV				
Update Authentication Adapter × Are you sure you want to upload the selected file?	1010	and and an					PR FIRE (.)				
Update Authentication Adapter X Are you sure you want to upload the selected file?							Open	Cancel			
Update Authentication Adapter × Are you sure you want to upload the selected file?											
Update Authentication Adapter × Are you sure you want to upload the selected file? NO YES											
Update Authentication Adapter × Are you sure you want to upload the selected file? NO YES											
Are you sure you want to upload the selected file?	Lload	ata Authan	tionti	~ ~ ^ ~	do not	~	r.				1.1
Are you sure you want to upload the selected file?	Upa	ate Authen	ucau	on ac	Japt	е	r				X
Are you sure you want to upload the selected file?	- 1					_					
Are you sure you want to upload the selected file?											
Are you sure you want to upload the selected file?											
Are you sure you want to upload the selected file?											
NÖ YES	Are v	ou sure vou want	to uplo	ad the s	selecte	d	file?				
NO YES						-					
NO YES											
NO YES											
NO YES											
NO YES											
NO YES											
NO YES											
								N	0	YES	
											-

- 4. In the File Explorer window
 - In the Quick Access Menu
 - Select Downloads
 - Select the VIDMAirWatchRootCertificate.Cer certificate
 - Select Open
 - In the Update Authentication Adapter window
 - select YES

Certificate (cloud deployment)	×
Enable Certificate Adapter ① Yes	Î
Root and intermediate CA certificates ① SELECT FILE	Ŀ
Uploaded CA Certificates CN=HZNADVINTRNELPOD22B (1DAE77894C4A9505039E71B82FD5 ×	
User Identifier Search Order Upn subject	
Validate UPN Format ①	k
Yes Request Timeout ()	
CANCEL	'E

5. In the Certificate (cloud deployment) window

- In the bottom right corner
 - select SAVE



- 6. In the Workspace ONE Access Console
 - Under Integrations

Select Identity Providers

- In the Identity Providers area
 - Select Built-in

5	Q Search for users, gr	roups, or applications	New I
es	Integrations Settings		
	Connector Authentication Methods	Select a directory first to see a list of available authentication methods.	
	Authentication Methods	Select which authentication methods the IdP will use to authenticate users.	
S		Authentication Methods	Associate Authentica
		Password (Local Directory)	
		Certificate (cloud deployment)	•
	Network	Select which networks this IdP can be accessed from. Choose from the availa	able network ranges from th

- 7. In the **Built-In** Identity Providers window
 - NOTE :
 - In the Authentication Methods area
 - The checkbox next Certificate (cloud deployment) is already enabled
| cess | Q Search for users, g | roups, or applications | |
|---------|------------------------|--|--|
| sources | Integrations Settings | | |
| | Back to IdP List | | |
| | | Identity Provider Name | Built-in |
| | | | |
| thods | | Users | Select which users can auth System Directory |
| | Built-in | | EUC-Livefire |
| _ | Type: EMBEDDED | | |
| | Status: Enabled | | 4 |
| | | Password (Local Directory) | |
| | | Certificate (cloud deployment) | |
| | Network | Select which networks this IdP can be ac | |
| | | ALL RANGES | |
| | KDC Certificate Export | Download Certificate | |
| | | Export the KDC server root certificate for | |
| | | Save Cancel | |

- 8. In the **Built-In** window
 - In the **Users** area
 - Next to **EUC-Livefire**
 - select the **checkbox**
 - In the **Network** area
 - Next to **ALLRANGES**
 - select the checkbox
 - At the bottom of the page.
 - Select Save

VMware venity will reach New updates available. L	earn what's ne	niity date (EoA) w in <u>Workspac</u>
(A) Workspace ONE	E Access	Q Searc
Monitor Accounts	Resources	Integration
Web Apps Virtual Apps <u>Virtual Apps</u> Collections	Polic Manage	CIES access policie
Policies	ADD PC	ED
	P	elicy Name

- 9. In the Workspace ONE Access Admin console
 - Select the **Resources** tab
 - In the **Resources** area
 - Select Policies

VMware Verify will reach New updates available. Le	end-of-availability date (EoA) and end-of-support arn what's new in <u>Workspace ONE Access SaaS</u>
(8) Workspace ONE	Access Q Search for users, groups
Monitor Accounts	Resources Integrations Settings
Web Apps Virtual Apps Virtual Apps Collections	Policies Manage access policies to establish trust
Policies	EDIT DELETE
	Policy Name
	default_access_policy_set

- 10. In the Workspace ONE Access Admin console
 - Under the **Policies area**
 - Next to default_access_policy_set
 - Select the radio button
 - Select EDIT

You c	an create a list of rule	es to access the applications	selected. For each rule, sele
type (use th	of devices that can a ne application before	ccess the applications, the au reauthenticating.	th methods, and the maximu
	ALL RANGES	Web Browser	Password (cloud depl
	ALL RANGES	Workspace ONE App	Password (cloud depl

- 11. In the **Edit Policy** window,
 - In the left column
 - Select Configuration
 - To the left of Web Browser,
 - Select All Ranges

	Rule applies to all users if no group(s) selected
and user is registering FIDO2 authenticator	No No
Then perform this action	Authenticate using
then the user may authenticate using *	Certificate (cloud deployment)
If the preceding method fails or is not applicable, then	Password (cloud deployment)
If the preceding method fails or is not applicable, then	Password (Local Directory)
CANCEL	

12. In the **Edit Policy Rule** window

- Next to then the user may authenticate using *
 - select Certificate (cloud deployment)
- Next to if preceding method fails or is not applicable, then *

- select Password (cloud deployment),
- Select ADD FALLBACK METHOD
 - Next to if preceding method fails or is not applicable, then *
 select Password (Local Directory)
- Select **SAVE** at the bottom of the window

pe of devices that can be the application befor	access the applications, the au re reauthenticating.	ith methods, ar
Network Range	Device Type	Authenticati
# ALL RANGES	Web Browser	Certificate (c
# ALL RANGES	Workspace ONE App	Password (c

- 13. In the **Edit Policy Rule** window
 - Select + ADD POLICY RULE

RATION	Add Policy Rule
If a user's network range is	ALL RANGES
and the user accessing content from *	Windows 10
and user belongs to group(s)	Q, Select Groups
	Rule applies to all users if no group(s) selected.
and user is registering FIDO2 authenticator	No No
Then perform this action	Authenticate using
then the user may authenticate using *	Certificate (cloud deployment)
If the preceding method fails or is not applicable, then	Password (cloud deployment)
If the preceding method fails or is not applicable, then	Password (Local Directory)
CANCEL	

- 14. In the **Edit Policy Rule** window
 - Next to: -
 - and user accessing content from*
 - select Windows 10
 - then the user may authenticate using*
 - select Certificate (cloud Deployment)
 - if the preceding method fails or is not applicable, then
 - select Password (cloud deployment)
 - Select + ADD FALLBACK METHOD
 - if the preceding method fails or is not applicable, then
 - Select Password (Local Directory)
 - At the botom right hand side of the page
 - Select **SAVE**

Configuration	
You can create a list o type of devices that c use the application be	f rules to access the applications : an access the applications, the au fore reauthenticating.
etwork Range	Device Type
ALL RANGES	Web Browser
ALL RANGES	Workspace ONE App
# ALL RANGES	Windows 10
Network Range	Device Type
# ALL RANGES	Windows 10
# ALL RANGES	Web Browser
# ALL RANGES	Workspace ONE App

15. In the **Edit Policy** window

- Next to ALL RANGES for Windows 10
 - Select the 6 DOTS and drag to the top
- Select **NEXT** on the **Edit Policy Page**

Edit Policy	Summary				×
1 Definition	Definition				i
2 Configuration	Name				
3 Summary	default_access_policy_set				Ш
•	Description Default access policy set				ļ
	Applications				
	Configuration				
	Policy Rule 1 If a user's network range is ALL RANGES and the user is accessing content from Windows 10 and the user belongs to the group(s) All Users then the user may authenticate using Certificate (cloud deployment) Fallback method 1: Password (cloud deployment)				
		CANCEL	BACK	SAVE	

16. On the **Edit Policy** Page.

- Summary tab
 - 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 4 Section 3: Log into a Windows 10 Desktop and demonstrate the limitation

Clipboard		Organize	New		Open	
` <mark> </mark> → Rer	mote Desktops > Site1	Windows Security				×
iess ads # ants # ite Bundle	Name CaptureVM.RDP DEMProfiler-01a.RDP Horizon-01a.RDP PackagingVM.RDP RDSH-01a.RDP TrueSSO-01a.RDP W10Client-01a.RDP w10EXT-01a.RDP w10EXT-01a.RDP w10Master-01a.RDP	Your system adm credentials to log because its ident credentials. mark@euc-livefit	ntials did no ninistrator does n g on to the remo tity is not fully ve re.com	t work not allow the us te computer 1 rified. Please e	se of saved 72.16.30.40 nter new	
cts	SWS1-Connector.RDP	The logon attem More choices	pt failed			
ents		0	к	с	ancel	
ads						

- 1. On the ControlCenter server Desktop,
 - Open the Remote Desktops folder,
 - Select the **W10Client-01a.RDP** shortcut
 - Log in as mark@euc-livefire.com,
 - enter the password VMware1!,
 - Select OK

If there are any existing Horizon Desktop sessions , Workspace ONE Access logins still open. Log out and close all sessions and browsers

0	Run		×
Ũ	Type the name of a program, f resource, and Windows will op	older, document, or Interneten it for you.	et
O	een: mmc This task will be created w	vith administrative privilege	v s.
	ОК	Cancel Browse	
	✓ Type here to search		0
ᡖ Co	nsole1 - [Console Root]		
🚡 File	Action View Favorites	Window H	
\$	New	Ctrl+N	
-	Open	Ctrl+O	
	Save	Ctrl+S	
	Save As		
	Add/Remove Snap-in	Ctrl+M	
	Options		
	Recent File		
	Exit		

- 2. On W10Client-01a desktop
 - Select Start > Run,
 - Next to **Open**, type **mmc**,
 - Select OK
 - In the Console, select Add/Remove Snap-in

ip-in	Vendor	^		Console Root		Edit Exter
ActiveX Control	Microsoft Cor			💭 Certificates - Current User	Down	
Authorization Manager	Microsoft Cor				Remo	
Certificates	Microsoft Cor					
Component Services	Microsoft Cor					Move
CompManagem	Microsoft Cor					The second
Device danager	Microsoft Cor		Add >			Movel
Disk Management	Microsoft and		Hud P			
Event ewer	Micro Lore Cor					
Folder	Microsoft Cor					
Group y Object	Microsoft Cor					
IP Security Monitor	Microsoft Cor					
IP Security Policy M	Cor					
Link to Web Address	Microsoft Cor	¥				Advand
ription:						

- 3. In the Add or Remove Snap-ins window
 - Select Certificates,
 - Select Add
 - Select OK



- 5. Expand Certificates Current User
 - Expand Personal
 - Select Certificates
 - Note you have an enrolled certificate. If you dont have a certificate,
 - Follow steps 6 8.
 - If you have an enrolled certificate
 - Carry on from step 9



6. On your W10Client-01a desktop

- In the right bottom corner of your Taskbar
 - To the left of the **Network** icon
 - Select the UP arrow



- 7. On your W10Client-01a desktop
 - Select and right-click the Intelligent Hub icon
 - Select **Sync**



- 8. In the **Certificates** snap-in
 - Under Personal
 - Select Certificates
 - In the **Toolbar**
 - Select Refresh

 ← → ○ ŵ ⊕ https://aw-livefirehorizonintrn.vidm ⊕ https://aw-livefirehorizoni ⊙ https://aw-livefirehorizoni ⊙ https://aw-livefirehorizoni > https://aw-livefirehorizoni	npreview.com/ Intrn.vi Intrn.vi Intrn.vi powered by Mice
	intrn.vi intrn.vi irrn.vidm powered by Micr
	Intrn.vi rn.vidm powered by Mici
My Feed	powered by Mic
https://cas.vidmpreview.com/cas. X + → C C	1-
	REST/landing?EAB_CALLBA
Select a certificate Select a certificate to authenticate yourself to cas.vidmpreview.cor	am/443
Subject Issuer	Serial
Mark HZNServicesADVINT	019645

- 9. On your W10Client-01a Desktop
 - Open a **browser** on your windows 10 desktop
 - In the address bar enter the URL of your Saas Access Tenant
 - In the **Select a certificate** window
 - Select OK

(Favorites	Apps People	For You	Support		
	Q Search A	Apps				
		Net	w Apps All	Apps Cate	egories 🗸	
N	lew Apps					
	_					
	0			<u>e</u>	· /	
	Calculator	Corp20-HZNt	o Intern	et Explorer	Paint	
		C Haring			C Harizon	🗖 Ho

- 10. On the Workspace ONE console,
 - In the **Apps** tab
 - Select Calculator

🕜 F	avorites	Apps People F	or You Support		
	Q Search	Apps			
					×
New App	25	Password Reque	st ign in to Calculator.		
		Password			
	0			Cancel	ign In
c	alculator	Corp20-HZNb	Internet Explorer	Paint	WordPa
🙄 Horizo	m •••	📮 Horizon 🛛 🚥	📮 Horizon 🔹	😅 Horizon 🔹	•• 📮 Horizon

11. In the Intelligent Hub

- Notice we are getting a Password request.
 - We used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password Auth method, to pass on to the Horizon Agent.
 - We will now move forward with Configuring HORIZON TRUESSO
- Select **Cancel** to close the **Password Request** window.
- Logout and close all windows on W10Client-01a

Part 5. Integrating Horizon TRUESSO with the Horizon Universal Console

Part 5 Section 1: Integrating Horizon TRUESSO with Horizon Universal Console



- 1. On your ControlCenter server
 - On your **Site 1** Browser
 - Open a new Tab
 - Select Horizon Site 1

VMware Horizon*	
administrator	
EUC-LIVEFIRE ~	
Remember user name	
Sign in	
vmware	

- 2. On VMware Horizon login
 - In the **Username** area
 - type Administrator
 - In the **Password** area
 - type VMware1!
 - Select Sign In

Profiles & Resources > Profiles	×	VMware H	lorizon®: Cluster-HOR	× +
← → C ☆ 🗎 horizor	n-01a.euc	livefire.co	m/admin/#/main/da	ishboard
🔛 Apps 🕤 my-ip.livefire.lab/ip	🔤 Horiz	on@Site 1	🔹 App Volumes Site	1 🚾 UAG-HZN-01
VMware Horizon	1.			
C Updated 03/12/2022, 10:59 AM	~			
Sessions	Q	Syste	m Health	
Problem vCenter VMs	Q			
Problem RDS Hosts	Q			
Events	4			
System Health	Q			
Monitor	~			
Dashboard				
Events				
Sessions				
Help Desk				
Users and Groups				
Inventory	~			
Desktops				
Applications				
Farms				
Machines				
Settings	~	VIEW		
Servers				
Domains		Total	Sessions ()	
Dendune Linnenten und Linnen				

- 3. In the Horizon Admin console
 - In the **Dashboard** area
 - Select VIEW

Components			×
0	Connection Servers Gateway:	iervers Event Database	TrueSSO
Issues	Status Name Version	Description No problem detected.	Services Statu
Components (0)			
RDS Farms (0)			
VSphere (0)			
Other Components (0)			
		Bows per	⊨ Hegt 20 ♥ 1-1 of traves
			ок

- 4. In the ${\mbox{Components}}$ window
 - Select TrueSSO

Components						×
	Conn	ection Servers	Gateway Servers	Event Detabase	TrueSSD	
0					C	Ø
Issues	Status	Managed Domain	Enrollment Servirts)	Certificate Authorities	Template	Descr
	0	Øeuc-liveFire.com	Orvesso 61a euclivefre	Oeuclivefire-TRUESSO-01a-C	ØtrudS0Te	OK
Components (0)						
RDS Farms (0)						
VSphere (0)						
Other Components (8)						
				Novo per page	20 ¥ 1-1 eft	10000
						ок

- 5. In the **TrueSSO** area of Components
 - Note that Enrollment and Sub-ordinate CA servers have been deployed and configured
 - To Close the **Components** window
 - Select OK

Horizz
,

- 6. On your ControlCenter server
 - On your **Site 2** Browser
 - Open a new Tab
 - Select Horizon Site 2

VMware Horizon*	
administrator	
EUC-LIVEFIRE ~	
Remember user name	
Sign in	
vmware:	

- 7. On VMware Horizon login
 - In the **Username** area
 - type Administrator
 - In the **Password** area
 - type VMware1!
 - Select Sign In

VMware Horizon®: Cluster-HOF	× +		
← → C û 🗎 horizon-l	02a.euc-li	vefire.com/admin/%	/main/dashboard
🔛 Apps 😒 vCenter02a 👼 UAG	-H2N-02a	🚾 UAG-H2N-026	💠 App Volumes Site 2 📲
VMware Horizon*			
C Updated 03/12/2022, 11:10 AM	× (Current Maalth	
Sessions	0	System Health	
Problem vCenter VMs	2		
Problem RDS Hosts	Q		
Events	4		
System Health	٥		
Monitor	~		
Dashboard			
Events			
Sessions			
Help Desk			
Users and Groups			
Inventory	~		
Desktops			
Applications			
Farms			
Marbinar			
Patrices			
settings	Ť	VIEW	
Servers			
Domains		Total Carciner	

- 8. In the Horizon Admin console
 - In the **Dashboard** area
 - Select VIEW

Components							×
0	Connector View Service	s Status - Vie	Gatewa w Sessions D	y Servers etail	Event Database	Tru	esso C ©
Issues	Status	Name	Version	Description			Services Statu
	° 0	HORIZON-01A	8.4.0	No problem dete	cted.		0
Components (0)							
RDS Farms (0)							
VSphere (0)							
Other Components (0)							
	×					Rows per page 🔝 💌	+ 1-1af1ran(s)
							OK

- 9. In the **Components** window
 - Select TrueSSO

Components						×
	Conn	ection Servers	Gateway Servers	Event Database	TrueSSO	
0					C	۲
issues	Status	Managed Domain	Enrollment Server(s)	Certificate Authorities	Template	Desce
	0	@euc-livefire.com	⊘truesso-01a.euc-livefir	e. @euc-livefire-TRUESSO-01/	⊷ ©TrueSSOTe	OK
Components (0)						
RDS Farms (0)						
VSphere (0)						
Other Components (0)						
				Rovs per p	ge 20 ♥ 1-1 of	1 reves
					1	OK

- 10. In the TrueSSO area of Components
 - Note that **Enrollment** and **Sub-ordinate CA** servers have been deployed and configured
 - To Close the **Components** window
 - Select OK

	×	New Tab	×	+					
х ^г р		Horizon®Site 1	🔶 App Volumes Site 1	uAG-HZN-01	UNG-HZN-016	S vCenter	🚺 Avi Vantage Con	sL. 🔫 HZN Cloud	
									_
							_	_	
						- C	200		
							500	GIE	
								<u> </u>	

- 11. On your ControlCenter server
 - **Revert** to your **Site 1** browser
 - **Open** a new tab
 - Select the HZN Cloud shortcut

Welcome to	
VMware Horizon®	D
My VMware Credentials	
Username	
Password	٩
Remember me	
LOGIN	

- 12. On the **Welcome to VMware Horizon**® page
 - Under My VMware Credentials, enter the following
 - In the Username area, type your, assigned Horizon Cloud email
 - In the **Password** area, type , **VMware1!**
 - Select LOGIN

VMware Horizoi	n®
Active Directory Credentials	
Username	
Password	٥
EUC-LIVEFIRE	~

- 13. On the **Welcome to VMware Horizon**® page
 - Under Active Directory Credentials, enter the following
 - In the **Username** area, type **Administrator**
 - In the **Password** area, type , **VMware1!**
 - Select LOGIN



14. In the Horizon Universal Console

- Expand Settings
 - Select Active Directory

Secondary DNS Server IP: Default OU: Join Username:	192.168.210.10 ou=computers,ou=corp,dc=e administrator
True SSO Configuration Horizon pods on VMware SDDC SYNC	

15. In the Active Directory area

- In the True SSO Configuration area
 - Next to Horizon pods on VMware SDDC
 - Select SYNC

Part 5 Section 2: Testing to see if TRUESSO works

O Apps Www.e Intelliger	ettub x +				v -	o x	
← → C # avit	anadvintmelpod20m	arch vidmpreview.cr	om/catalog-portal/u#/apps		18	\$ \$ I	
Favorite	Apps	People For	You Support			MD	
-	_						
Q	Search Apps						
_		(
		New Apps	All Apps Cal	tegories ¥			
New Apps							
0		9.0		<u></u>	A		
		00		· · /			
Calculato	r Co	(p20-HZNb	Internet Explorer	Paint	WordPad		
🙄 Harizon	••• 🗢 Hold	•••	🖵 Horizon 🛛 🚥	🖓 Horizon 🚥	🙄 Horizon		
AirvetchAgertmi	~					Show all X	
- ,							
		_					100 B 80 B

- 1. On your **ControlCenter** server,
 - Switch to your **Remote Desktops** session to **W10Client-01a.RDP** session.
 - If necessary, login again with
 - Username : Mark@euc-livefire.com
 - Password: VMware1!
 - *Sign out* of any existing sessions,
 - **close** all windows



- 2. On your **W10Client-01a** desktop,
 - Open your browser
 - Enter your custom Workspace ONE Access URL

Select a certificate Select a certificate to authenticate	yourself to cas.vidmpreview.com	x443	×
Subject	Issuer	Serial	
Mark	HZNServicesADVINT	019645	
Certificate information		OK Car	ncel

- 3. On the Select a certificate window,
 - Select OK

Q Search	Apps	New Apps	All Apps
		New Apps	All Apps
os			
θ	3		Ø
alculator	Corp20	-HZNb	Internet Explo
on •••	Horizon		📮 Horizon
	aiculator	alculator Corp20	alculator Corp20-HZNb

- 4. In the Intelligent Hub
 - Under Apps
 - Select CorpXX-HZN
 - where XX is your assignment



5. On the W10Client-01a

• Note that you have now observed a Single sign-on session

- Possibly launch a RDSH session from your Workspace ONE Access console
- This concludes this lab
- After initiating the TRUESSO SYNC, the initial testing of this Horizon Cloud Connector and version of Horizon 2209. I took up to 10 minutes for the SYNC, to take effect. Keep trying until it works