Horizon Integration with Untrusted Active Directory Forests

For as long as Horizon and View have existed, if a Horizon Pod needed to give users access to Horizon based resources. All Active Directory domains had to have at least a one-way AD Trust with the Horizon Domain. The Horizon Domain would have to be Trusted to read the Domain objects in the User Domain.

Many organization's setup separate Active Directory Forests for security reasons, yet they want to give users Access through a singular Horizon Pod. In the past this was almost impossible.

Recently with the 2103 release of Horizon a very simple solution has been developed to allow users from Untrusted Active Directory Domains, access to Horizon resources in an alternate untrusted Active Directory Domain Forest .

In this session we will walk you through the process of configuring a Domain Bind account and configuring Horizon resources to facilitate this process

Part 1: Configuring Domain Bind and Instant Clone Engine Domain Accounts

VMware Horizon® Version 2111	
administrator	
EUC-LIVEFIRE ~	
Remember user name	
Sign in	

- 1. On your ControlCenter server
 - Open your Chrome Browser
 - In the Favourites Bar, launch the VMware Horizon shortcut
 - Login as username Administrator

- Login with the password VMware1!
- Select Sign in



- 2. In the Horizon Admin Console
 - In the left Inventory pane, under Settings, select Domains

VMware Horizon	• Pod	CI
C [*] Updated 09/12/2021, 10:14 AM Sessions Problem vCenter VMs Problem RDS Hosts Events System Health	O Domains Instant Clone Engine Domain Accounts Connection Server Instant Clone Engine Domain Accounts Connection Server Image: Add Clone Engine Domain Accounts Connection Server	
Monitor Dashboard Events Sessions	Domain User O euc-livefire.com administrator	

- 3. In the Horizon Admin Console
 - Under **Domains** area
 - Select the **Domain Bind** tab

instant Clone Er	rgine Domain Accounts	Connection Server	Domain Bind
Add Edit	Remove Ma	anage Auxiliary Accounts	
Status	Domain		Netbios

- 4. In the Horizon Admin Console
 - Under **Domains** area > **Domain Bind**
 - Select Add

Add Untrusted Do	omain	×
Asterisk (*) denotes required	field	
* DNS Name	corpPriv.local	•
* Netbios	corpPriv	(1)
* Protocol	LDAP	٩
Primary Service Account		
* Username	administrator@corpPriv.local	٩
* Password		=
Advanced Settings	·	>
	Cance	ОК

- 5. In the **Untrusted Domain** window
 - Add the following, next to:-
 - DNS Name: corpPriv.local
 - Netbios: corpPriv
 - Username: administrator@corpPriv.local
 - Password: VMware1!
 - Select OK

Manage A	uxiliary Accounts		×
Add Edit	: Remove		
User		Domain	
	No records availab	le.	
Add Auxilia	ary Account		ок
Asterisk (*) denot	es required field		
DNS Name	corpPriv.local		
* User Name	administrator		
* Password			
		Cancel	ок

- 6. In the Manage Auxiliary Accounts window
 - Select Add
 - In the Add Auxiliary Account window
 - Select OK
 - Select **OK**, to close the **Manage Auxiliary Accounts** window



- 7. In the Horizon Admin Console
 - Under **Domains** area
 - Select the Instant Clone Engine Domain Accounts tab

Domains	in Accounts Connection Se
Add dit Remo	lser
O euc-livefire.com a	dministrator

8. In Domains Area

• Select Add

Add Domain /	Admin		×
Full Domain Name	corpPriv.local	v	
* Username	administrator		
* Password			
		Cancel	ОК

- 9. In the Add Domain Admin window
 - Add the following next to:-
 - Full Domain Name: from the dropdown, select corpPriv.local
 - Username: type Administrator
 - Password: type VMware1!
 - Select OK

Part 2: Configuring a Desktop Pool Assignment for the Untrusted Active Directory Domain



- 1. In the Horizon Admin Console
 - In the left Inventory pane
 - Under Inventory, select Desktops

VMware Horizon		
Updated 09/12/2021, 10:14 AM Sessions Problem vCenter VMs Problem RDS Hosts Events	> 0 1 3	Add Edit Duplicate Delete
Monitor Dashboard Events Sessions	ž	ID Display Name ID ID ID W10INST

- 2. In the **Desktop Pools** area
 - Select Add

Add Pool		
() Туре	Automated Desktop Pool Manual Desktop Pool ①	0
User Assignment	C RDS Desktop Pool	
Storage Optimization Social Desktop Pool Identification		
Provisioning Settings		
vCenter Settings Desktop Pool Settings		
 Remote Display Settings Guest Customization 		
Pastira Camalata	• Cancel Previous	Next

3. In the Add Pool wizard

Select Next

Add Pool	*	
🕑 Туре	Instant Clone ①	6
	Full Virtual Machines	
2 vCenter Server		
	vCenter Server	
User Assignment	voerter.euc-livefire.com	
Storage Optimization		
Desktop Pool Identification		
Provisioning Settings		
Center Settings		1 - 1 of 1 row(s)
	Description	
Desktop Pool Settings		
Remote Display Settings		
Guest Customization		
	-	
BBB Descute Canadate		
		Cancel Previous Next

4. In the Add Pool wizard

- vCenter Server
 - Select Next

Add Pool			
Type vCenter Server	Plasting		0
3 User Assignment	Enable Multi-User Assignment Automatic assignment is not supported for multi-user assignment pools.		
Storage Optimization			
Desktop Pool Identification			
Provisioning Settings			
vCenter Settings			
Desktop Pool Settings			
Remote Display Settings			
Guest Customization			
		Cancel Previous Ne	78

5. In the Add Pool wizard

- User Assignment
 - Select the radio button next to Floating
 - Select Next

	A	
🕗 Туре	Storage Dolicy Management (D	6
	Storage Policy management of	
VCenter Server	 Use VMware Virtual SAN 	
	Do not use VMware Virtual SAN	
User Assignment	 Virtual SAN is not available because no virtual SAN datastores are configured. Use Separate Datastores for Replica and OS Disks 	
Storage Optimization		
Desktop Pool Identification		
Provisioning Settings		
VCenter Settings		
Darkton Dool Sattings		
a name		
Remote Display Settings		
Guest Customization		
D. Passfulla Complete	*	

6. In the Add Pool wizard

Storage Optimization

Select Next

🕗 Туре	Asterisk (*) denotes required field	
	* ID ()	
VCenter Server	CorpPrivW10	
	Display Name (j)	
User Assignment	W10_CorpPriv	
	Access Group (1)	
Storage Optimization	/	
Parlana Barthiantifantian	Description	
S Desktop Pool Identification		
Provisioning Settings		
VCenter Settings		
B Desktop Pool Settings		
Remote Display Settings		
Guest Customization		
B Passivita Complete	•	

7. In the Add Pool wizard

- Desktop Pool Identification, update the following areas:-
 - Under ID enter CorpPrivW10
 - Under Display Name enter W10_CorpPriv
 - Select Next

Add Pool - CorpPrivW10		
🕑 Туре	Asterisk (*) denotes required field Basic	٥
🔗 vCenter Server	Enable Provisioning Stop Provisioning on Error	
OUser Assignment	Virtual Machine Naming Virtual Machine Naming Specify Names Manually	
Storage Optimization	0 names entered	
Desktop Pool Identification	Naming Pattern w10CorpPriv.	
Provisioning Settings	Provision Machines	
VCenter Settings	Min Number of Machines 1 All Machines Up Front	
Desktop Poel Settings	Desktop Pool Sizing	
Remote Display Settings	* Maximum Machines	
Guest Customization	Spare (Powered On) Machines 1	
Ready to Complete	Virtual Device Add VTPM Device to VMs	
	Ca	ncel Previous Next

- 8. In the Add Pool CorpPrivW10 wizard
 - Provisioning Settings
 - Under Use a Naming Pattern enter w10CorpPriv
 - Under Display Name enter W10CorpPriv
 - Under Desktop Pool sizing > Maximum Machines enter 2
 - Select Next

Add Pool - CorpPrivW10		
Туре	Default image	
vCenter Server	Asterisk (*) Genotes required field * Golden Image in vCenter	
User Assignment	/RegionADI/vmvDiscovered virtual machine/w10Parent01a	
Storage Optimization	/Baseline Brewse	
Desiston Pool Identification	Virtual Machine Location	
	The centre subsection RegionAD1Am Browse	
Provisioning Settings	Resource Settings	
VCenter Settings	Cluster //RegionA01/host/RegionA01-COMP01 Browse	
Desktop Pool Settings	Resource Pool	
Remote Display Settings	RegionA01/host/RegionA01-COMP01/Resources Browse Datastores	
	1 selected Browse	
Guest Customization	Network Golden Image network selected Brawse	
Ready to Complete		
	Faunt Bro	daus bleve

- 9. In the Add Pool CorpPrivW10 wizard
 - vCenter Settings
 - Browse and submit to the following:- Under:-
 - Under Golden Image in vCenter: Browse to W10Parent01a and Submit
 - Under Snapshot Browse to /Baseline and Submit
 - Under VM Folder Location Browse to RegionA01 and Submit
 - Under Resource Settings > Cluster Browse to RegionA01-COMPO1 and Submit
 - Under Resource Settings > Resource Pool Browse to RegionA01-COMPO1 and Submit
 - Under Resource Settings > Datastores Browse to CorpLUN2 and Submit
 - In the **Warning** window select **OK**
 - Select Next

type	State	
	Enabled 💙	
vCenter Server	Connection Server Restrictions	
	None Browse	
User Assignment	Category Folder	
	None Brouse	
Storage Optimization	Client Restrictions D Evabled	
Desktop Pool Identification	Session Types	
	Desktop	Ø
Provisioning Settings	Log Off After Disconnect	
	Immediately 💙	
vCenter Settings	Allow Users to Restart Machines	
0.	No.	
Deskton Pool Settings	Aller: Teoreta Decision factions from Different Client Decises	
		0
Remote Display Settings	···· •	w
Activity seconds		
Guest customization		
Ready to Complete		

- 10. In the Add Pool CorpPrivW10 wizard
 - Desktop Pool Settings
 - Under Log off After Disconnect: from the dropdown select Immediately
 - Select Next

Tune			
1994	Remote Display Protocol		
ul anitar Canuar	Default Display Protocol		
VLOTION NOTAD	VMware Blatt	~	
	Allow Users to Choose Protocol		
Use Assignment	Yes	~	
	3D Renderer		
storage Optimization	Manage using v5phere Client	~	0
	Allow Session Collaboration Enabled		
Descop Poer Identification	Requires Wilware Blast Protocol.		
Provisioning settings			
vicentar settings			
Desktop Poel Settings			
Hemote Display Secongs			
Guest Castomization			
Ready to Lompiete			

11. In the Add Pool - CorpPrivW10 wizard

Remote Display Settings

Select Next

Туре	Asterisk (*) denotes require	sd field		C
	Domain			
vCenter Server	corpPriv.local(administr	ator)	~	
	AD Container			
User Assignment	OU=Sales		Browse	
	Allow Reuse of Existin	g Computer Accounts 🛛 🔘		
Storage Optimization	Image Publish Computer	Account		
1.577			۵	
Desktop Pool Identification	Use ClonePrep			
Provisioning Settings	Power-Off Script Name			
			Ø	
vCenter Settings	Power-Off Script Parame	ters		
Desktop Pool Settings	Example: p1 p2 p3	int Name		
		nys marina	0	
Remote Display Settings	Post Synchronization Sci	rint Parameters		
Guest Customization	Example: p1 p2 p3			
Peoplete Complete	 Use a customization s 	specification (SysPrep)		
many to comprese				C
	Name	Guest O5	Description	
		No records available.		

12. In the Add Pool - CorpPrivW10 wizard

- Guest Customization
 - Browse and submit to the following:- Under:-
 - Under AD Container: Browse to OU=Sales and Submit
 - Select the checkbox next to Allow Reuse of Existing Computer Accounts
 - Select Next

Туре	Z Entitle Users After Adding Pool	0
Construction in	Туре	Automated Desktop Pool
VLATER MENU	User Assignment	Floating Assignment
User Assignment	vCenter Server	vcenter.euc-livefire.com
Storage Optimization	Unique ID	Corp#nW10
	Description	
Desktop Pool Identification	Display Name	W10_Corpitriv
Provisioning Settings	Access Group	1
	Desktop Pool State	Enabled
vCenter Settings	Session Types	Deskop
Desktop Pool Settings	Client Restrictions	Disabled
	Log Off After Disconnect	Immediately
Remote Display Settings	Connection Server Restrictions	None
Guest Customitation	Category Folder	None
	Allow Users to Restart Machines	No
Ready to Complete	Allow Separate Desktep Sessions from Different Client Devices	No
	Default Display Protocol	VMware Blast
	Allow Users to Choose Protocol	705
	3D Renderer	Manage using vSphere Client
	VRAM Size	8.00 MB

- 13. In the Add Pool CorpPrivW10 wizard
 - Ready to Complete
 - Select the checkbox next to Entitle Users After Adding Pool
 - Select Submit

Add Entitlements			>
Add new users and groups w	ho can use the selected pool(s).		
Name	Domain	Email	

- 14. In the Add Entitlements window
 - Select Add

Find User or	Group			×
Туре		🗸 Users 🔽 Groups		
Domain	[corpPriv.local		v
Name/User Name	[Starts with	~ S2	iles
Description	[Starts with	v	
Find				
Name	User Name	Email	Description	In Folder
Sales	Sales/corpPriv.k	scal		corpPriv.local/Sales
4				
1				
				1-10[1:00()]
				Course Day

- 15. In the **Find User or Group** window
 - Next to **Domain**, from the dropdown, select **corpPriv.local**
 - Next to Name/User Name, to the right of Starts with, enter sales
 Select Find
 - Under Find select Sales
 - Select OK
 - Select OK



16. In the Desktop Pools area

Select CorpPrivW10

Resource Pool Resources		View Storage Accelerator Enabled	Transparent Page Sharing Scope Virtual Machine
Disk OS Disks		Refresh 7 day(s)	Guest Customization CionePrep
Guest Customization Domain and Account corpPriv.local(administrator)	t	Allow Reuse of Existing Computer Accounts Yes	AD Relative Distinguished Name OU=Sales
Current Image None			
Pending Image			
429	8383		
Golden Image in vCenter w10Parent01a ····		Snapshot Baseline ····	State Publishing
Operation Initial Publish			
Storage			
Free Space 82.13 GB		Capacity 99.75 GB	Use VMware Virtual SAN No
Datastore		Networks	
	ClonePrep		
	AD Relative Distinguished Name OU=Sales		
	State Published (I)		
	Host or Cluster RegionAD1-COMPD1 ····		

17. In the CorpPrivW10 area

- Under the **Summary** tab,
 - Scroll down to **Pending Image**
 - View the progress of the pool being Provisioned
 - To the right notice the State is Publishing
 - When complete this will report as **Published**
 - The page does not dynamically update. You will have to refresh periodically.
 - This can be done by selecting the **Refresh icon** in the top right-corner of the **Summary** page
 - You will need to have to wait until the Pool is **Published**



- 18. In the Horizon Admin Console
 - Under Inventory
 - Select Machines

	2	macriffes		
Problem vCenter VMs	2	vCenter RDS F	losts Others	
Problem RDS Hosts	1			
Events	2	Restart Desktop	Reset Virtual Machine	Recover Rebuild
System Health	2			
Monitor		Machine All		
Dashboard				
Events		Machine	Desktop Pool	DNS Name
Sessions		W10Inst3	WIDINST	w10inst3.euc-live
Help Desk			WIDINST	w10inst2.euc-live
Users and Groups			WIDINST	w10inst1.euc-live
Inventory	~	A W10inst4 A	WIDINST	w10inst4.euc-live
Desktops		A w10CorpPriv	2 CorpPrivW10	w10corpprtv-2.cc
Applications		w10CorpPriv	1 CorpPrivW10	w10corpprtv-1.co
Machines				
Settings				
Agent Version	Datastore	Status		
8.3.0-18287218	CorpLUN	Availabi	e	
	CorpLUN	Availabi	0	
8.3.0-18287218				
8.3.0-18287218	CorpLUN	Availabi	e	
8.3.0-18287218 8.3.0-18287218 8.3.0-18287218	CorpLUN	Availabi Availabi	e	
8.3.0-18287218 8.3.0-18287218 8.3.0-18287218 8.3.0-18287218	CorpLUN CorpLUN CorpLUN2	Availabi Availabi Availabi	e e	
8.3.0-18287218 8.3.0-18287218 8.3.0-18287218 8.3.0-18287218 8.3.0-18287218 8.3.0-18287218	CorpLUN CorpLUN CorpLUN2 CorpLUN2	Availabi Availabi Availabi Availabi	e e e	

19. In Machines area

- Look for your **CorpPrivW10** virtual Machines
- Wait until the **Status** is **Available**

File Home Sh	are View	
← → ~ ↑	This PC > Desktop > Remote Desktops	
1 Quick accord	^ Name	Date r
	5 AD2.CorpPriv.local.RDP	8/23/2
Desktop 🖈	AppVol.RDP	5/7/20
👆 Downloads 🖈	S AppVoIProv.RDP	7/30/2
🔮 Documents 🖈		5/7/20
📰 Pictures 🛛 🖈	between the second seco	5/7/20
hol	Norizon.RDP	3/1/20
Remote Desktop	NackagingVM.RDP	5/7/20
System32	NDSH01a.RDP	4/13/2
Working	SQL.RDP	4/3/20
- Working	NueSSO.RDP	1/12/2
This PC	NueSSO2.RDP	9/10/2
-	••••••••••••••••••••••••••••••••••••••	

- 20. On your Controlcenter server
 - Open the **Remote Desktops** Folder
 - Launch the Horizon.RDP shortcut
 - Note. you should automatically be authenticated with the account Administrator@euc-livefire.com



21. On the Horizon Desktop

- Select and right-click the **Start** button
- Select Run



- 22. In the **Run** window
 - Next to **Open:** enter adsiedit.msc
 - Select OK
 - If you were to open adsiedit for the first time you would have to follow the guides in the below Knowledge Base
 - https://kb.vmware.com/s/article/2012377

Image: ADSI Edit File Action View Help Image: ADSI Edit File Action View Help Image: ADSI Edit Image: ADSI Edit File Action View Help Image: ADSI Edit Image:			
ADSI Edit ADSI Edit Default naming context [loca OU=Application loo OU=Applications OU=Data Disks CN=ForeignSecurity OU=Groups OU=Hosts CN=LostAndFound CN=NTDS Quotas OU=Packages OU=Packages OU=Pople OU=Policies OU=Pople OU=Pople OU=Policies OU=SchemaUpdateL OU=Servers	Name CN=CorpPrivW10 CN=W10INST	Class pae-ServerP pae-ServerP pae-ServerP	

- 23. In the ADSI Edit window
 - **Expand** the inventory
 - Select OU=Server Groups
 - Select and right-click CN=W10INST

Attributes:		
Attribute	Value	^
pae-PendingParentV	<not set=""></not>	
pae-PendingParentV	<not set=""></not>	
pae-PendingVmTemp	<not set=""></not>	
pae-PostSyncScriptA	<not set=""></not>	
pae-PowerOffScriptA	<not set=""></not>	
pae-PrimingComputer	<not set=""></not>	_
pae-ProvisionScheme	<not set=""></not>	
pae-PublishEnabled	<not set=""></not>	
pae-RDSLoadBalanci	<not set=""></not>	
pae-RDSMaxSessions	<not set=""></not>	
pae-RDSMaxSession	<not set=""></not>	
pae-RecoveryDisabled	<not set=""></not>	
pae-RecurringMainte	<not set=""></not>	
pae-RecurringMainte ≮	<not set=""></not>	>
Edt		Filter

- 24. In the **CN=W10INST Properties window**
 - Scroll down until you find the pae-ProvisionScheme attribute
 - Select the **pae-ProvisionScheme** attribute
 - Select Edit

String Attribut	te Editor		×
Attribute: Value: ModeA	pae-Provision Scheme		
Clear]	ОК	Cancel

- 25. In the **String Attribute Editor** window
 - In the Value area, type ModeA
 - Select **OK**, to close the window
 - Select **OK**, to close the **CN=W10INST Properties** window
 - Close the ADSI Edit window

Part 3. Configuring VMware App Volumes for the Untrusted Active Directory Domain



- 1. On the ControlCenter Server
 - Open your Chrome browser
 - From the Favourites bar, select the App Volumes Manager shortcut

VMware	App Volumes™
Username:	administrator
Password:	
Domain:	EUC-LIVEFIRE V
Login	
Customer Experience	Improvement Program (CEIP)
You have decided to pa provides VMware with i problems, and to advisi collected through CEIP Assurance Center at ht	ticipate in the Customer Experience Improvement Program ("CEIP"). This program iformation that enables VMware to improve its products and services, to fix you on how best to deploy and use our products. Details regarding the data and the purposes for which it is used by VMware are set forth at the Trust & p://www.vmware.com/trustvmware/ceip.html

- 2. In the App Volumes Manager login page
 - Next to **Username:** enter **Administrator**
 - Next to **Password:** enter **VMware1!**
 - Select Login
 - Select **OK** to close the **Customer Experience Improvement Program(CEIP)** window

	EUC-LIVEFIRE\Administrate				
ACTIVITY	CONFIG	URATION			
Attachments	Writables				
	Create	Import	🔁 Re	scan	
. Users, Groups, Comput	ters or Organ	nizational U	nits can	be	
		Filter			

3. In the App Volumes Manager Admin console

• Select the **Configuration** Tab

VMware App	Mware Holizon → Thorizon → App volumes Mana → 040 → vcenter → Access → 0eM → Holizon chent EUC-LIVEFIRE\Administrator Logour					
INVEN	TORY [DIRECTORY	INFRASTRUCTURE	ACTIVITY	CONFIGURATION	
License	AD Domains	Admin Roles	Machine Managers	Storage	Managers	Settings
Settings						
Configuration se	ttings for App Volum	nes Manager.				
General						

4. In the App Volumes Manager Admin console

- In the **Configuration** Area
 - Select the AD Domains Tab

TIVITY	CONFIGURATIO	CONFIGURATION		
storage	Managers	Settings		
		Register Domain		
I OUs.				

5. In the AD Domains area

• Select Register Domain

INVENTORY	DIRECTORY	INFRASTRUCTURE	ACTIVITY	CONFIGURATION	
License AD Domains	Admin Roles	Machine Managers	Storage	Managers	Settings
egister Active Direct	ory Domain				
Active Directory Domain Name:	corpPriv.local		Fully qualified Active (Example: vmware.com	Directory domain name	
Domain Controller Hosts:			This may be left blank Example: adserver.vmv	(to use any Domain Contro are.com, 10.107.XX.XXX, 10.	ller) 107.XX.XX
LDAP Base:			This may be left blank Example: OU=engineer	(to use all of Active Directo ing,DC=vmware,DC=com	ry)
Username:	Administrator		This may be a user wi Example: administrator	ith read-only access	
Password:			Password is stored er	crypted	
Security:	LDAP (insecure)) ~	Requires correspondi	ng ActiveDirectory configura	tion
Port.	389		This may be left blank	(to use default port)	
Cancel					Regis
_					

- 6. In the AD Domains area
 - Enter the following next to:
 - Active Directory Domain Name: corpPriv.local
 - Username: Administrator
 - Password: VMware1!
 - Security: LDAP(insecure)
 - Port: 389
 - Select Register

			Boar			
r	CONFIGUR	ATION				
3	Managers	Settings				
	Assign Role	e Hage Roles	l			
Lui	INVENTORY	DIRECTORY	INFRASTRUCTURE	ACTIVITY	CONFIGURATION	^ 0
Licen	ase AD Dom	ains Admin Roles	lachine Managers	Storage	Managers	Settings
Admi	nistrator Roles					Manage Roles
Roles g	rant administrative priv	vileges to the members of	Active Directory groups.			
Importa • Only u	nt information: isers in these groups v	vill be able to login to the I	Manager.			
Role:		Administrators	-	_		
Searc	ch Domain:	All	*			
Searc	ch Groups:	administrator		Contains 🗸	Search	- 1
		Search all domains i	in the Active Directory forest			
Choo	se Group:	CORPPRIVAdministrator	\$	~	←	
Cance	əl					Assign

7. In the App Volumes Manager consoles

- Select the Admin Roles tab
 - Select Assign Role
 - Enter and select the following next to:
 - **Role:** from the dropdown select **Administrators**
 - Search Groups: Administrator
 - Select : Search
 - Choose Group: from the dropdown select CORPPRIV\Administrators
 - Select Assign

Part 4 Testing the Desktop Pool of users from an Untrusted Domain



- 1. On your ControlCenter Server
 - Launch your Horizon Client

📮 VMwa	re Horizon Client	
	horizon.euc- livefire.com	

- 2. From your Horizon Client
 - Select the horizon.euc-livefire.com POD

🖒 https://horizon.euc-livefire.com						
clint@corpPriv.local	clint@corpPriv.local					
•••••	••••••					
Cancel Login						

- 3. In the Horizon Client Login window
 - In the **Username** area
 - Enter clint@corpPriv.local
 - In the **Password** area
 - Enter VMware1!
 - Select Login



- 4. In the Horizon Client login
 - Select the W10_CorpPriv entitlement

Part 5: Deploying Horizon Enrollment services to facilitate Single Sign-On with Workspace ONE Access



Introduction:

When logging in through Workspace ONE Access to a Horizon Desktop the user does not have a single sign on experience .

We will now configure Horizon Enrollment services in the Untrusted Domain



- 1. On your **ControlCenter** server
 - Open the Remote Desktops Folder
 - Launch TrueSSO2.RDP shortcut
 - Login as corpPriv\administrator and enter the password VMware1!
 - On the Server Manager Interface select Manage > Add Roles and Features

Add Roles and Features Wizard		×
Before you begin	DESTINATION SERV TRUESSO2.corpPriv.lo	(ER ical
Before You Begin Installation Type	This wizard helps you install roles, role services, or features. You determine which roles, role services, features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.	or
Server Selection Server Roles	To remove roles, role services, or features: Start the Remove Roles and Features Wizard	
	Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.	
	To continue, click Next.	
	Skip this page by default	
	< Previous Next > Install Cance	1

- 2. On the **Before you begin** window
 - Select Next



- 3. On the Select installation type window,
 - Ensure the radio button in front of Role-based or feature-based installation is selected
 - Select Next

Add Roles and Features Wiz	ard			-		×
Select destination	on server			DESTIN/ TRUESSO	ATION SER LeorpPriv.le	VER
Before You Begin Installation Type Server Selection	Select a server or a virtual Select a server from th Select a virtual hard di	hard disk on which e server pool sk	to install roles and features.			
Server Roles Features Confirmation	Server Pool					
	TRUESSO2.corpPriv.local	192.168.110.82	Microsoft Windows Server 2	2019 Datacente	ŧf	
	1 Computer(s) found This page shows servers th and that have been added	hat are running Wind I by using the Add S	dows Server 2012 or a newer n ervers command in Server Mai	elease of Wind	ows Serv	rer, nd
	newly-added servers from	which data collection	vious Next >	Install	Cance	el

- 4. On **Select destination server** window (accept the defaults)
 - Select Next



- 5. On the Select server roles window,
 - Select the check box in front of Active Directory Certificate Services,
 - When prompted for the Add Features window, select Add Features box,
 - Then select Next

🚵 Add Roles and Features Wizard		- 🗆 ×
Select features		DESTINATION SERVER TRUESSO2.corpPriv.local
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select one or more features to install on the selected server. Features Image: Select one of the selected server. Image: Select one one of the selected server. Image: Select one one one one of the selected server. Image: Select one	Description .NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	< Previous Ne	xt > Install Cancel

- 6. On the **Select features** window
 - Select Next



- 7. On the Active Directory Certificate Services window
 - Select Next

🛓 Add Roles and Features Wiz	rd	- 🗆 ×
Select role servi	ces	DESTINATION SERVER TRUESSO2.corpPriv.local
Before You Begin	Select the role services to install for Active Directory Certificate	rvices
Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
	< Previous Next	Install Cancel

- 8. On the Select role services window
 - Select Next

- 9. On the Confirm Installation selections window,
 - Select the checkbox next to Restart the destination server automatically if required,
 - On the Add Roles and Features Wizard window select Yes
 - Select Install

You will have to wait a short while before moving on to step 10

Add Roles and Features Wizard		-		×
Installation progre	ess	DESTINA TRUESSO2	ATION SER	VER
	View installation progress			
	Feature installation			
	Configuration required. Installation succeeded on TRUESSO2.corpPriv.loca	d.		
Features	Active Directory Certificate Services		inatio	20
Role Services Confirmation	server Configure Active Directory Certificate Services on the destination server Certification Authority			
Results	Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools			
	You can close this wizard without interrupting running tasks. View task pr page again by clicking Notifications in the command bar, and then Task D Export configuration settings	ogress or o Jetails.	open this	5
	< Previous Next > C	lose	Cance	el

- 10. On the **Installation progress** page,
 - Select the Configure Active Directory Certificate Services on the destination server hyper-link

AD CS Configuration	- 🗆 ×				
Credentials	DESTINATION SERVER TRUESSO2.corpPriv.local				
Credentials Role Services	Specify credentials to configure role services				
	To install the following role services you must belong to the local Administrators group:				
	Standalone certification authority				
	Certification Authority Web Enrollment Online Responder				
	To install the following role services you must belong to the Enterprise Admins group:				
	Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service				
	Credentials: CORPPRIV\administrator Change				
	More about AD CS Server Roles				

11. On the **Credentials** window

Select Next

AD CS Configuration		_		×
Role Services		DESTINAT TRUESSO2.0	ION SER	VER
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service			
	More about AD CS Server Roles			
	< Previous Next >	Configure	Cance	el .

- 12. On the **Role Services** page,
 - Select the Certificate Authority checkbox
 - Select Next

🔁 AD CS Configuration	- 🗆 ×
Setup Type	DESTINATION SERVER TRUESSO2.corpPriv.local
Role Services Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	 Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates. Enterprise CA Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. Standalone CA Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
	More about Setup Type
	< Previous Next > Configure Cancel

- 13. On the Specify the setup type of the CA window ,
 - Select the radio button next to Enterprise CA

Select Next

AD CS Configuration	- 🗆 ×
СА Туре	DESTINATION SERVER TRUESSO2.corpPriv.local
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	 Specify the type of the CA When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy. Root CA Root CA Root CAs are the first and may be the only CAs configured in a PKI hierarchy. Subordinate CA Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.
	More about CA Type
	< Previous Next > Configure Cancel

14. On the **CA type** window

- Ensure the Subordinate CA radio button is selected,
- Select Next



15. On the **Private Key** window,

- Ensure the radio button next to Create a new private key is selected
- Select Next

AD CS Configuration			-		×
Cryptography fo	r CA		DESTINAT TRUESSO2.0	TION SER	VER
Credentials Role Services	Specify the cryptographic options				
Setup Type	Select a cryptographic provider:		Key length:		
CA Type	RSA#Microsoft Software Key Storage Provider	v	2048		¥
Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	Select the hash algorithm for signing certificates issued by SHA256 SHA384 SHA512 SHA1 MD5 Allow administrator interaction when the private key is	s accessed	by the CA.		
	More about Cryptography Previous	>	Configure	Cance	el

- 16. On the Cryptography for CA window select the following
 - Under Cryptographic Provider: RSA#Microsoft Software Key Storage Provider
 - Next to Key Length: 2048
 - Hash Algorithm: SHA256
 - Select Next


- 17. On the Specify the Name of the CA window
 - Observe the CA naming convention
 - Select Next

		- 0
Certificate Rec	quest	DESTINATION SERVE TRUESSO2.corpPriv.loc
Credentials Role Services Setup Type CA Type	Request a certificate from parent Co You require a certificate from a parent certification a issue certificate. You can request a certificate from i a file to submit to the parent CA.	A huthority (CA) to allow this subordinate CA to an online CA or you can store your request to
Private Key Cryptography	Send a certificate request to a parent CA: Select: CA reame	↓
Certificate Request	Computer name Parent CA:	Select
Confirmation Select	Certification Authority ?	×
Results CA	corpPriv-AD2-CA AD2.corpPriv.local	ESSO2-CA.req parent CA to make this CA operational.
<		>
	OK Cancel	Configure Cancel
AD CS Configuration		- 🗆 ×
AD CS Configuration	uest	
AD CS Configuration	uest Request a certificate from parent CA	DESTINATION SERVER TRUESS02.corpPriv.local
AD CS Configuration Certificate Requ Credentials Role Services Setup Type CA Type	LIEST Request a certificate from parent CA You require a certificate from a parent certification author are certificate. You can require a certificate from an or	- C X DESTINATION SERVER TRUESSO2.corpPrivilecal
AD CS Configuration Certificate Requ Credentials Role Services Setup Type CA Type Private Key Credentials	Lest Request a certificate from parent CA You require a certificate from a parent certification authorizes and the submit to the parent 2 certificate from an or a fit to submit to the parent CA.	- C X DESTINATION SERVER TRUESSO2.corpPrivilocal
A D CS Configuration Certificate Requ Credentials Role Services Seture Type CA Type Private Key Cryptography CA Name Certificate Seture 100	Lest Request a certificate from parent CA You require a certificate from a parent certification authoristic entificate from an or a file to submit to the parent CA. Send a certificate request to a parent CA: Sector and Cartificate from a content of the content form C C nome	- C X DESTINATION SERVER TRUESSO2.corpPrividecal
A D CS Configuration Certificate Requ Credentials Role Services Setue Type CA Type Private Key Cryptography CA Name Certificate Database	Request a certificate from parent CA You require a certificate from a parent certification authorized entificates. You can request a certificate from an or a file to submit to the parent CA: Select Canane Computer name Parent CA: [AD2.corpPriv_Joca1.corpPriv_AD2-CA]	- C × DESTINATION SERVER TRUESSO2.corpPriviocal nty (CA) to allow this subordinate CA to fine CA or you can store your request to Select.
AD CS Configuration Certificate Requir- Credentais Role Sarvices Setup Type CA Type Private Rey Cryptography CA Name Certificate Database Confirmation Confirmation Confirmation Confirmation	Request a certificate from parent CA Nor require a certificate from a parent certification author issue certificates. Nor can requere a certificate from an or a file to submit to the parent CA: Seriest Computer name Period CA (aD2.compPrin.local.compPrin-FBU File ame: [CITUISSO2.compPrin.local.compPrin-TBU	- C × DESTINATION SERVER TRUESSO2.corpPividecan rhy (GA) to allow this subordinate CA to finer CA or your can store your request to Select. e ESSO2-CAreq
AD C3 Configuration Certificate Requirements Credentials Abis Services Setup Type CA Type Private Key Cryptography Canton Results Configure Database Configure Databa	Alegan Sector Control	- C × DESTINATION SERVER TRUESSO2.corpPrivideod inty (CA) to allow this subordinate CA to find CA or you can store your request to inty (CA) to allow this subordinate CA to find CA or you can store your request to set StoreCAreq parent CA to make this CA operational.
AD C3 Configuration Ceretrificate Requirements Credentials Role Services Setur Type CA Type Private Rey Cryptography CA Name Certificate Distances Configure Database Configure Database	Request a certificate from parent CA No require a certificate from parent certification actua tasse certificate software certificate from as ore a flex to submit to the parent CA. 	- C × DESTINATION SERVER TRUESSO2.corpPrivideod

18. On the Request a certificate from parent CA,

- Select the radio button next to Send a certificate request to a parent CA:
- To the right of the **Parent CA** box, click the **Select** button
- Select **OK** accept the Default
- Select Next

AD CS Configuration		-		×
CA Database		DESTINA TRUESSO2.	CorpPriv.	IVER local
Credentials	Specify the database locations			
Role Services	Certificate database location:			
CA Type	C:\Windows\system32\CertLog			
Private Key				
Cryptography	Certificate database log location:			
CA Name	Citations systems (certuag			
Certificate Request				
Certificate Database				
Confirmation				
Progress				
	More about CA Database			
			6	
	< Previous Next >	Configure	Canc	21

- 19. On the CA Database window,
 - Select Next



20. On the **Confirmation** window

Select Configure

Results			DESTINATION SERVER TRUESSO2.corpPriv.local
	The following roles, role services, or fi	eatures were configured:	
Setup Type CA Type Private Ray Cryptography CA Name Certificate Request Certificate Request Certificate Database Confirmation Progress Results	Certification Authority More about CA Configuration	Configuratio	n succeeded
Add Roles and Features Wizz nstallation prog	erd TPCSS View installation progress	Previous Next >	Close Cancel
Add Roles and Features Witz nstallation prog Before You Begin Installation Type Server Selection Server Selection	vrd TFCSS View installation progress Peture installation Configuration required. Instal	Previous Next >	Close Cancel
Add Roles and Features Wizz Installation prog Endore You Begin entaulizion Type Satives Roles Features Adv CS Role Services Continue sion Result	red TOPSS View installation progress Topfguation required, install Configuration required, install Add extreme Directory Certificates 5 Role Administration Too Role Administration Too	Previous Next > Intro succeeded on TRUESS ces encies role services are confis obs ate Services Tools rity Management Tools	Clase Cancel Can

- 21. On the **Results** window
 - Select Close
 - On the Installation progress window,
 - Select Close

Part 6: Deploying and Configuring Horizon TRUE SSO

					Conse	
🚡 File	Action	View	Favorites	Window	Help	
(i)	New				Ctrl+N	
	Open				Ctrl+O	
	Save				Ctrl+S	
6	Save As					
	Add/Rer	move Sna	p-in		Ctrl+M	
	Options			_		
	1 C:\Wir	ndows\\	compmgn	nt.msc		
1	2 C:\Wir	ndows\\	services.m	sc		
1	Exit					
					dd or Po	mayo F
				, r	ad or Ke	move 5
You can s extensible	elect sna t snap-in	s, you car	his console configure	from those a which extens	svailable on sions are ena	your comp bled.
Available	snap-ins					Selecte
Snap-in			Vendor	^		Co
Activ	eX Cont	rol	Microsoft	Cor		
Auth Certi	orization ficate Te	manager	Mcrosoft	Cor	_	
Certi	ficates		Microsoft	Cor		
Cert	fication /	Authority	Microsoft	Cor		
Comp Comp	ponent S outer Ma	ervices	Microsoft	Cor	Add >	
Devic	ce Manag	ger	Microsoft	Cor		
THE DOC	manager	nent	PREFOSIOR	and		
		Cer	tification A	uthority		×
Select the o	omputer you	ward this shap	into manage	`		
	in will always	manage		L		
This shap-		the computer the	tis console is run	n (m)		
 Local 	computer: (
* Local	computer: (-	_		Browse	
Local Allow orby a	the palacted	computer to b save the core	e changed when	n launching from th	e command line. 1	
Local Alow only a	the selected	computer to b save the cons	e changed when ole.	n launching from th	e command line. 1	2
Local Alow only a	the selected	f computer to b save the core	e changed wher cle	n launching from th	e command line. 1	2
Local Alow only a	the selected	Computer to b save the cons	e changed when	n launching from th	e command line. 1	2
Local Alow only a	computer: (f computer to b save the cons	e changed when	n launching from th	e command line. 1	2
Incel Alow only a	the selected pples if you	computer to b seve the cons	e changed when cle. < Back	n launching from th	e command line. 1 Cancel	his Hob
Local Alow only a	computer: (Computer to b asive the cons	e changed wher ele. < Back	Finah	e command line. 1	ha Heb
Alexe A	computer: (computer to b save the cons	e changed wher ole. < Back Add or Rem or examined on you	Pisah	Erouse a command line. 1 Cancel gure the selected set	ha Help
Yee are selected as a series of the ser	the selected gallet if you way to fire the two you can on the	computer to b assee the cons oursele from the influence which ex-	e changed wher cle. < Back Add or Rem or exalidite on you	Peak	Erouse a command line. 1 Cancel pure the selected set	Help
Vec on which a single control of the single	the selected goldes if you require for the major to for the selected of the selected o	computer to b assee the cons operate from the eliging e shakes index torong Con.	e changed wher ole. < Back Add or Rem or exclusion are subject on you	Preat	Errors e command line. 1 Cancell gure the selected set	has heb hose heb hose heb hose hose hose hose hose hose hose hose
Yes are shown	the selected polies if you agains for the file, you can on a and in factors if implaces if	Computer to b serve the comp serve the comp may exhibe a	e changed wher de. < Back Add or Rom or evaluation on yea	Freah I	Encer e command line. 1 Cancel gare the selected set	has has of snap-Has. For bit Extensions
The set up - Construction of the set of th	the selecter gaples if you agains for the selecter is the selecter gaples if you against the selecter is the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement in the selecter is implement i	Computer to b serve the comp may be a server the comp may be a server the comp may be a server to be made to b	e changed where de.	Peak	e command line. 1 Cancel	Independent
Vers are select or of a select or of	the selected goine for free mounter of your sector for free mounter of the sector of t	computer to b save the cons and the construction of the influence which are ender to a save the con- ment of the con- transition of the co- transition of	e changed wher de. < Back Add or Rem Add or Rem a chanded a make a changed a changed a make a changed a changed a make a changed a changed a changed a changed a changed a changed a changed a changed a changed a changed a changed a	Freah	e command line. 1 Cancel	han bar Na Magana Ar Martin Karana Martin Martin Martin Martin Martin Martin Martin Martin
Var. data select an order of order of o	the selected splitter if you be selected as a splitter if you be selected as a splitter if you be selected as a splitter if you be splitter if you	computer to b save the cons and the cons induces of the const induces of the const induces of the const induces of the const instant for an instant for an i	e changed wher de. < Back Add or Rem Add or Rem Remaining are made	Final:	e command line. 1 Cancell gure the selected set	Meterson Annual An
Version enfects are only an analysis Version and an analysis and an analysis Computer Compute	the selected splitter if you be an intervention of the selected selected in the implant of the i	Computer to b save the cons average han the integra which as which to const the toget to con- transit to co- transit to co- tr	 changed where ide. < Buck. Add or Rem or available on year or available on	Preach Preach CONE Seap-ins or consult and confusion in the field and res	e command line. 1 Cencel guer the selected set	ha ha decarses for <u>All Doleners</u> Revol Revol Revol
Version and a final sector of the sector of	computer, (the selected police if you be adjusted by the selected by	computer to b save the cons average from the computer from the matching we while the safe to ar- issent to ar- treast to ar-	< Back	Final: 1 Toronto and Constitution of Soup into a Constitution of Constitutio of Constitutio of Constitution of	e commend line. 1 Cancell gare the selected set sufferette Cancell	he he of news he New Dawn New Dawn New Dawn
The sensitive type Allow	the solution of the solution o	computer to b save the cons average from the computer from the methy end of the constitution of the consti	< Back	Prest	Cancel	ha ha Ne Contract of any set of any set of New Sector New Sector N
Alexandromerican and a second and a sec	vapore for the selection of the selectio	Computer to b serve the Comp serve the Comp and the Comp	e changed where < Back Add or Rem or available on your Add or Rem or Add or Add or Rem or Add or A	Neurching from the	Carcel	ha ha defenses. For Marketones Same Same Same Same Same Same Same Same

- 1. In this section we will create a certificate template for Horizon TRUESSO
 - On your TRUESSO2 server select Start > Run > type mmc
 - Select File > Add/Remove Snap-in...
 - Select the Certificate Authority services snap-in, select Add
 - In the Certificate Authority window,
 - Select the Local computer radio button
 - Select Finish
 - Select **OK** to close the **Snap-ins** window

Certification Aut	hority (Local)	
× - comPriv-TRU	JESSO2-CA	
Revoked	Cartificator	
S Issued Ce	utificator	
Issued Ce	Pressente	
Pending I	Requests	
Failed Kee	quests	
Certifi	Manage	
	New	>
	View	>
	New Window from Here	
	New Taskpad View	
	Refresh	
	Export List	
	Help	

- 2. Expand the corpPriv-TRUESSO2-CA inventory
 - Select Certificate Templates,
 - right-click and select Manage

R Certificate Templates (AD2.corp	Template Display Name	Schema Vers
	CEP Encryption	1
	Code Signing	1
	Computer	1
	Cross Certification Authority	2
	Directory Email Replication	2
	Domain Controller	1
	Domain Controller Authentication	2
	EFS Recovery Agent	1
	Enrollment Agent	1
	Enrollment Agent (Computer)	1
	Exchange Enrollment Agent (Offline requ	1
	Exchange Signature Only	1
	Exchange User	1
	2 IPSec	1
	IPSec (Offline request)	1
	Kerberos Authentication	2
	Key Recovery Agent	2
	OCSP Response Signing	3
	RAS and IAS Server	2
	Root Certification Authority	1
_ (Router (Offline request	1
· ·	Smartcard Logon	1
· · ·	Semantic and Lines	1
	Subordinate Certification Authority	1
	Irust List Signing	1
1	(W) Hear	1

3. In the **Certificate Template** Console

• Find and select the **Smartcard Logon** template



- 4. Right-click the **Smartcard Logon** template
 - Select Duplicate Template

	Prop	perties	of New	Template	
Subject I	Vame	Ser	ver	Issuance I	Requirements
Superse	ded Templa	tes	Ed	ensions	Security
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Show re	e options a in Compatil sulting char	valiable ar bility Settin nges	e based o igs.	n the earliest op	erating system
Certificati	on Authorit				
- Contineed	of the second	7			
Window	s Server 20	112 R2		~	
Certificate	e recipient				
Window	s 8.1 / Win	dows Sen	ver 2012 F	R: ~	
These settin template.	ıgs may not	prevent e	arlier oper	ating systems fr	om using this
These settin template.	igs may not OK	prevent e	arlier oper Cancel	ating systems fr	om using this Help
These settin template.	ogs may not OK		arlier oper Cancel	ating systems fr	om using this
These settin template.	ogs may not OK Resulting the	prevent e	arlier oper Cancel	ating systems fr	om using this Help
These settin template.	ogs may not OK Results dia	prevent e	arlier oper Cancel	ating systems fr	om using this Help
These settin template.	ogs may not OK Resulting the Merce project with Adverse project with adverse of the adverse of t	prevent e	arlier oper Cancel	ating systems for Apply	em using this
These settin template.	OK Resulting the optimized and	prevent e	arlier oper Cancel	ating systems fr	m using this
These settin template.	ogs may not OK Resulting dat Monty hundle with a mind of the state of the state of the state of the state of	prevent e	arlier oper Cancel	ating systems fr	Help
These settin template.	ogs may not OK Resitting day 6 toto: 10 toto:	prevent e	arlier oper Cancel	ating systems fi	em using this
These settin template.	oga may not OK Resetta del Maria	prevent e	Cancel	ating systems fr	Hep
These settin template.	ingis may not OK Resisting data Mana data seriari Mana data seriar	prevent e	afier oper	ating systems fin	Help
These settin template.	OK OK Reating day Many and a state reading and a state Reating and a state Reading and a state Reading and a state		afier oper	ating systems fin	m using this
These settin template.	OK Restrict of the second seco	prevent e	arlier oper	Apply	m using the
These settin template.	ings may not OK Management Manage	prevent e mars m second control second control seco	affer oper	Apply	m using this
	OK Reating the View of the second second view of the second second second second view of the second	prevent e	arlier oper	ating systems fr	m using the
	OK Reading of Advances of Ad		Cancel	Apply	m using this
	OK Reality of the second secon		Cancel	ating systems fr	Heb

- 5. In the **Properties of New Template** window in the **Compatibility** tab under **Certificate Authority**
 - Change from Windows 2003 to Windows 2012 R2
 - When prompted for the **Resulting changes** window
 - Select OK.
 - Under Certificate recipient change Windows XP / Server 2003 to Windows 8.1 / Server 2012 R2

- When prompted for the **Resulting changes** window
 - Select OK.

	Properties	of New	Template	x
Subject Name	Ser	ver	Issuance R	equirements
Superseded Te	emplates	Exte	nsions	Security
Compatibility Gen	eral Request	Handling	Cryptography	Key Attestation
Template display n	ame:			
TrueSSO Templat	e			
Template name: TrueSSOTemplati Validity period: 1 hours Publish certifica Do not auto Directory	e v ate in Active Di matically reenn	Renewal	l period: hours ✓	exists in Active
	Certifi	cate Tem	plates	×
The renewal period (6 automatically set the r To change the renewa	weeks) is larger renewal period t I or validity peri	than the ma o the maxim od to a diffe	num allowed. num allowed (0 h rent value, click	To ours), click OK. Cancel.
			ОК	Cancel

- 6. Select the General tab,
 - Under Template display name: type TrueSSO Template,
 - You will notice Template name gets filled in automatically.
 (Don't edit the TemplateName)
 - Under Validity period change the period from 1 years to 1 hours
 - When prompted by the Certificate Templates Box
 - Select OK
 - The **Renewal period** will automatically change from **6 weeks** to **0 hours**

Subject N	Vame	Sen	ver	Issuance R	lequirements
Superse	ded Templa	ates	Exte	insions	Security
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Purpose:	Signa	ture and s	martcard lo	igon	~
	De	lete revok	ed or expire	ed certificates (d	lo not archive)
	Inc	lude symm	etric algorit	thms allowed by	the subject
	Arc	hive subie	ect's encryp	tion private kev	
Allow priv	rate key to	be export	-d		
Allow priv	vate key to	be exporte	ed		
Allow priv	vate key to vith the san	be exporte	ed		
Allow priv	vate key to vith the san natic renev	be exportente ne key val of smar	ed t card certif	ficates, use the	existing key if a
Allow priv	vate key to with the sam matic renew cannot be	be exporte ne key val of smar created	ed t card certif	ficates, use the	existing key if a
Allow priv	vate key to with the sam natic renev cannot be	be exporte ne key val of smar created	ed t card certif	ficates, use the	existing key if a
Allow priv Renew v For autor new key Do the follov	vate key to with the san matic renew cannot be ving when t	be exportent ne key val of smar created the subject	ed t card certif t is enrolled	ficates, use the	existing key if a private key
Allow priv Renew v For autor new key Do the follov associated v	vate key to vith the san natic renev cannot be ving when t vith this cer	be exportent ne key val of smar created the subject tificate is u	ed t card certif t is enrolled used:	ficates, use the	existing key if a private key
Allow priv Renew w For autor new key Do the follow associated w Enroll sul	vate key to vith the san natic renev cannot be ving when t vith this cer oject withou	be exportence of the subject tificate is ut the subject tificate is ut the subject tificate is the subject tificate is the subject subject tificate is the subject subject tificate is the subject sub	ed t card certif t is enrolled ised: any user ii	ficates, use the I and when the p nput	existing key if a private key
Allow priv Allow priv Renew v For autor new key Do the follov associated v Enroll sul	vate key to with the sam matic renev cannot be ving when t with this cer oject withou ne user dur	be exported ne key val of smar created the subject tificate is u ut requiring ing enrollm	ed t card certif t is enrolled ised: any user in ent	ficates, use the I and when the p nput	existing key if a private key
Allow priv Renew w For autor new key Do the follow associated v Enroll sul Prompt tf Oprompt tf	vate key to vith the san natic renev cannot be ving when t vith this cer oject withou ne user dur ne user dur ne user dur	be exported ne key val of smar created the subject tificate is u ut requiring ing enrollm ing enrollm	ed t card certif t is enrolled used: any user in ent ent ent and rec	ficates, use the I and when the p nput quire user input	existing key if a private key when the
Allow priv Renew w For autor new key Do the follov associated v Enroll sul Prompt th Private ko	vate key to vith the sam natic renev cannot be ving when t vith this cer oject withou ne user dur ne user dur ne user dur y is used	be exportent ne key val of smar created the subject thicate is u ut requiring ing enrollm ing enrollm	ed t card certif t is enrolled used: any user in ent ent and red	ficates, use the I and when the p nput quire user input	existing key if a private key when the

- 7. Select the Request Handling tab change the following next to :-
 - Purpose: change: Signature and encryption to Signature and smartcard logon.
 - When prompted, select Yes
 - Select the **checkbox** in front of **Allow private key to be exported**
 - Select the checkbox in front of For automatic renewal of smartcard certificates, use the existing key if a new key cannot be created
 - Select the radio button in front of Prompt the user during enrollment

Prop	perties	of New	Template	×
Subject Name	Sen	ver	Issuance R	equirements
Superseded Templat	tes	Ede	nsions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Provider Category:	Key	Storage Pr	ovider	~
Algorithm name:	RSA	1		~
Minimum key size:	2048	3		
Choose which cryptogra Requests can use a C Requests must use a	phic prov ny provide one of the	riders can b er available following p	on the subject's providers:	ests s computer
Providers:	What	t's This?		
Microsoft Software K	iey Storag	e Provider		•
Request hash:	SHA	256		~
Use alternate signati	ure format			
ОК		Cancel	Apply	Help

- 8. Select the **Cryptography** tab change the following next to
 - Provider Category: Key Storage Provider
 - Minimum key size: 2048
 - Request hash: SHA256

Pro	operties of Nev	v Template	×
Compatibility General	Request Handling	Cryptography	Key Attestation
Superseded Temp	lates E	densions	Security
Subject Name	bject Name Server Issuance F		lequirements
Do not store cet#	icates and requests i rocation information i	n the CA databasi	o 06
OK	Cancel	Apply	Help

9. Select the Server tab,

- Select the checkbox in front of Do not store certificates and requests in the CA database
 - You will notice that **Do not include revocation information in issued certificates** is selected automatically.
- Uncheck the check box next to Do not include revocation information in issued certificates

General	Compatibility	Reques	t Handling	Crypto	graphy	Key At	testation
Super	seded Template	s	Extensions		Security		Server
	Subject Name			ssuanc	e Requir	ements	
Require	the following fo	r enrollm	ent:				
	certificate manag	ger appro	val				
🗹 This	number of auth	orized sig	anatures:	1			
-							
lf y	ou require more	than one	signature, a	sutoenro	ollment is	not allo	wed.
Pol	cy type required	in signat	ure:				
Ap	plication policy						~
App	lication policy:						
Ce	rtificate Reques	t Agent					~
15:51	uance policies:				_		
						Add	ł
						Rem	ove
Require	e the following fo	r reenroli	ment:				
⊖ Sar	e criteria as for	enrollmer	vt.				
Vali	d existing certific	ate					
	Allow key based	renewal	Ö				
Rec	quires subject inf uest.	formation	to be provid	led with	in the ce	rtificate	
leq							
*Contr	ol is disabled due	e to <u>com</u>	patibility setti	ngs.			

- 10. Select the Issuance Requirements tab, configure the following:
 - Select the checkbox : This number of authorized signatures and change the value to 1 in the box
 - Under **Policy type required in signature**
 - Ensure the **Application policy** is selected (default config)
 - Under Application Policy
 - Select Certificate Request Agent from the dropdown
 - Under the **Require the following for reenrollment**
 - Select the Valid existing certificate radio button

mpatibility	General	Request Ha	anding	Cryptography	Key Attestation		
Subject I	Vame	Server	r	Issuance F	Requirements		
Superse	ded Templa	ates	Exte	ensions	Security		
Group or use	er names:						
Authen Adminis Domain Enterpr	ticated Usi strator n Admins (C ise Admins	CORPPRIV-LD	lomain /	Admins) rise Admins)			
elect Us Select thi	ers, Cor	nputers, S type:	[Service	Add e Accounts,	Remove or Groups		×
Users, G	roups, or	Built-in se	curity p	principals		Object	Types
From this	location:						
From this bject Typ	location: pes						>
From this bject Typ elect the	location: pes types of	objects yo	u want	to find.			>
From this bject Typ ielect the biect type	location: pes types of es:	objects yo	u want	to find.			>
From this bject Typ bject type bject bject bj	location: pes types of es: uit in sec envice Ac computers roups sers	objects you unity princip counts	u want bals	to find.			>

- 11. On the **Security** tab in the **Group or user names:** area
 - Select Add
 - To the right of the **Select this object type:** box
 - Select the **Object types** button
 - Select the checkbox next to Computers,
 - Select OK

operties of New Template	× ended Pu
Select Users, Computers, Service Accounts, or Groups	>
Select this object type:	
Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
corpPriv.local	Locations
Enter the object names to select (examples):	
TRUESSO2	Check Names
	K Canaal

- 12. In the Enter the object names to select
 - Type TRUESSO2
 - To the right select **Check Names**
 - Select OK

ompationity	General	Request Handling	Cryptography	Key Attestation
Subject I	Vame	Server	Issuance R	equirements
Superse	ded Templa	ates D	tensions	Security
Group or use	er names:			
Adminis Comain Comai	strator Admins (C ise Admins SSO2 (COF	CORPPRIV\Domain (CORPPRIV\Enter RPPRIV\TRUESSO	Admins) prise Admins) (2\$)	_
Permissions	for TRUES	iS02	Add	Remove
Full Contro	ol			
Read				
Write				
Enroll				
Autoenrol	I			
	emissions	or advanced settin	gs, click	Advanced

13. For the **Permissions for TRUESSO2**

- Ensure that the permission **Read** and **Enroll checkboxes** are selected.
- Select **OK** to close the **TrueSSO Template Properties**,

Console Root Certification Authors CorpPriv-TRUE Revoked Cort Issued Cert Pending Re Failed Requ Certific	ority (Local) SSO2-CA ertificates ifficates equests uests Tomplator Manage		Name Directory Email Replication Domain Controller Authentication Kerberos Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Catificate Template to Issue
	View New Window from Here New Taskpad View Refresh Export List Help	>	Subordinate Certification Authority Administrator

14. Switch to the **Certificate Authority Console**

- Select and right-click the Certificate Templates container,
- Select New > Certificate Template to Issue

Enable Certificate Templates		
Select one Certificate Template to enable Note: If a certificate template that was re information about this template has been All of the certificate templates in the orgate For more information, see <u>Certificate</u>	e on this Certification Authority. ecently created does not appear on this list, you may need to wait until replicated to all domain controllers. anization may not be available to your CA. <u>re Template Concepts.</u>	
Name	Intended Purpose	^
RAS and IAS Server	Client Authentication, Server Authentication	
Router (Offline request)	Client Authentication	
Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
TrueSSO Template	Smart Card Logon, Client Authentication	
Trust List Signing	Microsoft Trust List Signing	
User Signature Only	Secure Email, Client Authentication	
VMware Certificate	Server Authentication, Client Authentication	
VMware-SSL	Server Authentication, Client Authentication	

15. In the Enable Certificate Templates window,

- Select your TrueSSO Template
- Select OK

Agent	1
gent	1
cont (Computer)	
Duplicate Template	
All Tasks	>
All TUSKS	
Properties	
Help	
chacodon	
Agent	2
se Signing	3
erver	2
tion Authority	1
	Duplicate Template Duplicate Template All Tasks Properties Help Help Control of the se Signing enver tion Authority

- 16. Switch back to the **Certificate Templates** Console
 - Select and right-click the Enrollment Agent (computer) template
 - Select Properties

Enrollme	nt Agent (Comput	er) Properties		~ ×
General	Request Handling	Subject Name	Extensions S	ecurity
Templa	te display name:			
Enrollm	ent Agent (Compute	r)		
Minimur	m Supported CAs: V	Vindows 2000		
Templa	te name:			
Machin	ne Enrollment Agent			
Validity 2 Publ	years years Jo not automatically Directory	ve Directory reenroll if a duplic	penoa: weeks	dists in Active
	ОК	Cancel	Apply	Help

17. In the Enrollment Agent Properties window

• Select the **Security** tab

eneral	Request Handling	Subject Name	Extensions	Security	
Group	or user names:				
	thenticated Users omain Admins (CORP terprise Admins (COF RUESSO2 (CORPPR	PRIV\Domain Ac RPPRIV\Enterpris IV\TRUESSO2\$	dmins) se Admins) ;)		
² emiss	ions for TRUESSO2		Add Allow	Remove	1
Full (Read	Control d				
Enm	•				
Enro	cial permissions or ac	dvanced settings,	, click	Advanced	

- 18. Select Add and add the TRUESSO Computer account with Read and Enroll permissions .
 - Select **OK** to close the **Enrollment agent** properties

Console Root Certification CorpPriv- Revo Ssue Pend Failer Certification Certification Certification Certification Certification Certification Certification Certification Certification Certification Certification Certification Certification Certification	Authority (Local) -TRUESSO2-CA ked Certificates d Certificates ing Requests d Requests ficate Templates Manage New	>	Name TrueSSO Template Directory Email Replication Domain Controller Authentication Kerberos Authentication EFS Recovery Agent Basic EFS Domain Controller Web Course Certificate Template to Issue	Inte Sm Din Clie File Enci Ser Clie
	View New Window from Here New Taskpad View Refresh Export List Help	>	User Subordinate Certification Authority Administrator	Chi Enc <a Mir</a

19. Switch back to the **Certificate Authority Console** select

- Right-click the Certificate Templates container,
- Select New > Certificate Template to Issue

Enable Certificate Templates						
Certification Authority. eated does not appear on this list, you may need to wait until d to all domain controllers. nay not be available to your CA. ate <u>Concepts.</u>						
Intended Purpose	^					
Client Authentication						
Private Key Archival						
Certificate Request Agent						
Code Signing						
<all></all>						
Certificate Request Agent						
Certificate Request Agent						
Certificate Request Agent						
Secure Email						
Secure Email	~					
	Certification Authority. Pated does not appear on this list, you may need to wait until d to all domain controllers. Pay not be available to your CA. Pay not be avai					

20. In the **Enable Certificate Templates** window

- Select the Enrollment Agent (Computer) template
- Select OK



- 21. We will now configure the CA for non-persistent certificate processingOn the **TrueSSO2** server
 - Select and right-click the **Start** button
 - Select Command Prompt (Admin)



22. In the Administrator: Command Prompt enter the following commands

certutil -setreg DBFlags +DBFLAGS ENABLEVOLATILEREQUESTS

```
C:\Windows\system32>certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\euc-livefire-CONTROLCENTE

R2-CA\CRLFlags:

Old Value:

CRLFlags REG_DWORD = 2

CRLF_DELETE_EXPIRED_CRLS -- 2

New Value:

CRLFlags REG_DWORD = a (10)

CRLF_DELETE_EXPIRED_CRLS -- 2

CRLF_REVCHECK_IGNORE_OFFLINE -- 8

CertUtil: -setreg command completed successfully.

The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>_
```

23. Configure CA to ignore offline CRL errors

•

certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE

C:\Windows\system32>net stop certsvc The Active Directory Certificate Services The Active Directory Certificate Services	service is stopping. service was stopped successfully.
C:\Windows\system32>net start certsvc The Active Directory Certificate Services The Active Directory Certificate Services	service is starting. service was started successfully.

- 24. Restart the CA service. From the command prompt run:
 - net stop certsvc
 - net start certsvc



- 25. On the TrueSSO2 server desktop
 - Launch the **software** shortcut
 - In the Software folder, open the Horizon\2106 folder.
 - Select and launch the VMware-Horizon-Connection-Server-x86_64-8.4.0-19067837.exe

Open File	- Security War	ning	\times
Do you	want to run t	nis file?	
	Name:	"Horizon-Connection-Server-x86_64-8.3.0-18294467.ex	e
	Publisher:	VMware, Inc.	
	Type:	Application	
	From:	\\horizon\software\Horizon\2106\VMware-Horizon-Co	·
		Run Cancel	
Alwa	ys ask before o	pening this file	
•	While files fr harm your co <u>What's the ri</u>	om the Internet can be useful, this file type can potential omputer. Only run software from publishers you trust. <u>sk?</u>	ly

- 26. On the **Open File Security Warning** window
 - Select Run

😾 VMware Horizon Conn	ection Server ×
vm ware [,]	Welcome to the Installation Wizard for VMware Horizon Connection Server
	The installation wizard will install VMware Horizon Connection Server on your computer. To continue, dick Next.
vMware Horizon	Copyright (c) 1998-2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
Product version: 2106	< Back Next > Cancel

- 27. On the **Welcome** window
 - Select Next

👷 VMware Horizon Connection Serv	rer	\times
License Agreement		
Please read the following license agre	eement carefully.	
VMWARE END USER LICENSE	AGREEMENT	^
PLEASE NOTE THAT THE TERM AGREEMENT SHALL GOVERN Y REGARDLESS OF ANY TERMS	IS OF THIS END USER LICENSE YOUR USE OF THE SOFTWARE, THAT MAY APPEAR DURING THE	1
INSTALLATION OF THE SOFT	ANC.	
IMPORTANT-READ CAREFULLY USING THE SOFTWARE, YOU (I AGREE TO BE BOUND BY THE AGREEMENT ("EULA"). IF YOU [THE INDIVIDUAL OR LEGAL ENTITY) TERMS OF THIS END USER LICENSE DO NOT AGREE TO THE TERMS OF THIS	~
IMPORTANT-READ CAREFULLY USING THE SOFTWARE, YOU (I AGREE TO BE BOUND BY THE AGREEMENT ("EULA"). IF YOU I	THE INDIVIDUAL OR LEGAL ENTITY) TERMS OF THIS END USER LICENSE DO NOT AGREE TO THE TERMS OF THIS ement	~
IMPORTANT-READ CAREFULLY USING THE SOFTWARE, YOU (I AGREE TO BE BOUND BY THE AGREEMENT ("EULA"). IF YOU I I accept the terms in the license agree I do not accept the terms in the license	THE INDIVIDUAL OR LEGAL ENTITY) TERMS OF THIS END USER LICENSE DO NOT AGREE TO THE TERMS OF THIS ement agreement	*

- 28. On the **License agreement** window
 - Select the radio button next I accept the terms in the license agreement,
 - Select Next

Destinati	on Folder	
Click Ne:	t to install to this folder, or click Change to install to a different folder.	
	Install VMware Horizon Connection Server to:	
	C:\Program Files\VMware\VMware View\Server\	Change
	-	

- 29. On **Destination Folder** window
 - Select Next

😾 VMware Horizon Connection Server	×
Installation Options	
Select the type of Horizon Connection Server instance you want to install.	
Select the type of Horizon Connection Server instance you want to install.	
Horizon Standard Server Horizon Replica Server Horizon Enrolment Server	
Perform an Enrollment Server instance install. This is used for True SSO.	
Enrollment Server only uses IPv4 protocol for establishing all connections.	
This server will be configured for a Horizon environment.	
< Back Next > Cancel	

30. On the Installation Options window select Horizon Enrollment Server
Select Next

P viviware Piorizon Connection Server			
Firewall Configuration			
Automatically configure the Windows Fi connections.	irewall to allow inco	ming TCP protocol	
In order for Horizon Enrollment Server must be allowed through the local Win 32111 (View Framework channel).	to operate on a ne dows Firewall servi	etwork, specific inco ce. The incoming T	oming TCP port CP port is
Configure Windows Firew	all automatically		
O Do not configure Window	is Firewall		

- 31. On Firewall configuration window
 - Select Next

🛃 VMware Horizon Connection Serv	er	×
Ready to Install the Program		
The wizard is ready to begin installation	on.	
VMware Horizon Connection Server w	ill be installed in:	
C:\Program Files\VMware\VMware Vi	ew\Server\	
Click Install to begin the installation or	Cancel to exit the wizard.	
	< Back Install	Cancel

32. Select Install

👹 VMware Horizon Connect	ion Server	\times
vmware [,]	Installer Completed	
	The installer has successfully installed VMware Horizon Connection Server. Click Finish to exit the wizard.	
	Next Steps:	
	Show the documentation	
VMware		
Horizon		
Product version: 2106	< Back Finish Cancel	

- 33. On the Installer Completed Window
 - Select Finish

Programs and Features
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel
File Explorer
Run
3 Shut down or sign out
Desktop
Run ×
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK Cancel Browse

34. On the **TrueSSO2** server

- Select and right-click the **Start Button**,
- Select Run,
- Type MMC,
- Select OK

	~	-	UEM		
File		Con	sole1 - [Console Root]		
~	-	File	Action View Favorites Window	Help	
			New	Ctrl+N	
1	1		Open	Ctrl+O	
	٦		Save	Ctrl+S	
			Save As		
			Add/Remove Snap-in	Ctrl+M	
			Options		
			1 C:\Windows\\dnsmgmt.msc		
			2 C:\Windows\system32\dsa.msc		
			3 C:\Windows\\certsrv.msc		
			4 C:\Windows\\compmgmt.msc		
			Exit		
Ċ					

35. In the **Console** window

• Select File > Add/Remove Snap-in..

Manual and State					
Vendor	^		Console Root		Edit Extensions
Microsoft Cor					Remove
Microsoft Cor					TVLING YC
Microsoft Cor					
Microsoft Cor					Move Up
Microsoft Cor					Maura Davia
Microsoft Cor	Ad	id >			Move Down
Microsoft Cor	~				
Microsoft Cor					
Microsoft Cor					
Microsoft Cor					
Microsoft Cor					
Microsoft Cor					
Microsoft Cor	~				Advanced
	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor

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

rtificates snap-in	
This snap-in will always manage certificate	es for:
O My user account	
O Service account	
Computer account	
	< Back Next > Cancel
ect Computer	< Back Next > Cancel
ect Computer	< Back Next > Cancel
lect Computer Select the computer you want this snap-in	< Back Next > Cancel
lect Computer Select the computer you want this snap∔n This snap-in will always manage:	< Back Next > Cancel to manage.
lect Computer Select the computer you want this snap-in This snap-in will always manage: (@) Local computer: the computer this	< Back Next > Cancel to manage. console is running on)
lect Computer Select the computer you want this snap-in This snap-in will always manage: (a) Local computer: (the computer this (b) Local computer; (the computer this)	< Back Next > Cancel to manage. console is running on)
lect Computer Select the computer you want this snap-in This snap-in will always manage: © Local computer:	< Back Next > Cancel to manage. console is running on) Browse
lect Computer Select the computer you want this snap-in This snap-in will always manage:	<back next=""> Cancel to manage. console is running on) Browse changed when launching from the command line. This</back>
lect Computer Select the computer you want this snap-in This snap-in will always manage: © Local computer; the computer this O Another computer: This selected computer to be console only applies if you save the console	Ket Cancel It to manage. It is numing on) Browse
lect Computer Select the computer you want this snap-in This snap-in will always manage: (a) Local computer: the computer this Another computer: Another computer: Another computer to be of only applies if you save the console	console is running on) changed when launching from the command line. This
lect Computer Select the computer you want this snap-in This snap-in will always manage: O Local computer: the computer this Another computer: Another computer: I allow the selected computer to be c only applies if you save the console	Cancel Cancel to manage. console is running on) Browse. changed when launching from the command line. This e.
lect Computer Select the computer you want this snap-in This snap-in will always manage: ① Local computer: the computer this △ Another computer: ☐ Alow the selected computer to be c only applies if you save the console	console is running on) browse changed when launching from the command line. This e.
lect Computer Select the computer you want this snap-in This snap in will always manage:	< Back
lect Computer Select the computer you want this snap-in This snap-in will always manage:	< Back Next > Cancel Ito manage. Ito manag
lect Computer Select the computer you want this snap-in This snap-in will always manage:	< Back Next > Cancel Into manage. Into manag
lect Computer Select the computer you want this snap-in This snap-in will always manage:	< Back

37. Select Computer account radio button

- Select Next
- Select Finish
- Select OK

~ 📮	Ce	Certific ertificates (Lo Personal	ate Templates ocal Computer)				
	_	C					
>		Truste	All Tasks	>	Request New Certificate		
>		Enter	View	>	Import		
>		Interr					
>		Truste	New Window from Here		Advanced Operations	>	
>	~	Untru	New Taskpad View				
>	1	Third	-				
>		Truste	Refresh				
>		Client	Export List				

- 38. Expand the Certificates console inventory
 - Select and right-click the **Personal** container.
 - Select All Tasks > Request New Certificate



- 39. On the **Certificate Enrollment > Before you Begin** window
 - Select Next

Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based Certificate enrollment policy may already be configured for you.	on predefined certificate templates.
Configured by your administrator	
Configured by you	Add New

40. On the Select Certificate Enrollment Policy window

• Select Next

			-		×	- 5 ×
📮 Ce	rtificate Enrollment					
F	Request Certificates					
						ns 🕨
	You can request the following types of certifica click Enroll.	ates. Select the certificates you wa	nt to request, a	nd then		
	Active Directory Enrollment Policy					
	Computer	③ STATUS: Available		Details •	•	
	Enrollment Agent (Computer)	③ STATUS: Available		Details •	-	
-	Show all templates					
			Enroll	Cane	el	
-			cinon	cane		

41. On the **Request Certificates** windows

- Select the checkbox in front of Enrollment Agent (Computer)
- Select Enroll

neave birectory chronine	nt Policy		
Enrollment Agent (Com	puter) 🖌 STATUS: Suc	ceeded	Details 🗸
			Finish
ued To	Issued By	Expiration Da	Finish

42. On the Certificate Installation Results window,

- Ensure the enrollment was successful
- Select Finish.

	1
 Certificates (Local Computer) 	
Personal	
Certificates	
> Trusted Root Certification Author	rities
> Enterprise Trust	
> Intermediate Certification Author	rities
> Trusted Publishers	
> Intrusted Certificates	
> Third-Party Root Certification Au	thorities
> Trusted People	
> Client Authentication Issuers	
> Preview Build Roots	
> Test Roots	
> 🧮 Remote Desktop	
> Smart Card Trusted Roots	
> Irusted Devices	
> VMware Horizon View Certificate	s
VMware Horizon View Enrollment	t Server Trusted Roots
> Windows Live ID Token Issuer	
> WindowsServerUpdateServices	
5	
> Intermediate Certification Author	Find Certificates
> Trusted Publishers	The connector.
> Ontrusted Certificates	All Tasks > Find Contificates
> I hird-Party Koot Certification	the second se
> Irusted People	View > Import
Client Authentication Issuers	New Window from Here
> Preview Build Roots	New Tackpad View
> est Roots	Terew Tookpool View
> Kemote Desktop	Refresh
> Smart Card Trusted Koots	Export List
> Inusted Devices	
> viviware Horizon View Certific	Help
Windows Live ID Taken Issues	
> Windows Live ID Token Issuer	
> windowsserverupdateServices	

43. On your **TrueSSO2** server

• Select your Certificate services Snap-in,

- Select and right-click the last container in the inventory VMware Horizon View Enrollment Server Trusted Roots,
- Select All Tasks > Import

v	elcome to the Ce	rtificate Im	port Wizard	l
Th	s wizard helps you copy cer s from your disk to a certific	rtificates, certifica cate store.	ate trust lists, and o	ertificate revocation
A an co	ertificate, which is issued b d contains information used nnections. A certificate stor	y a certification a to protect data o e is the system a	uthority, is a confir or to establish secu rea where certifica	mation of your identi re network tes are kept.
	itore Location			
	Current User			
	Local Machine			
То	continue, dick Next.			

44. On the **Welcome** window

select Next

← ;	🖗 Certificate Import Wizard	>
	File to Import	
	ареалу вле не ува манско протк.	
	File name:	
	Whorizon.euc-livefire.com\software\Horizon\enroll.cer Browse	
	Note: More than one certificate can be stored in a single file in the following formats:	
	Personal Information Exchange- PKCS #12 (.PFX,.P12)	
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
	Microsoft Serialized Certificate Store (.SST)	
	Next Canc	el

45. In the **File to import** window

- Under File name, type the following \\Horizon.euc-livefire.com\software\Horizon\ enroll.cer
- Select Next

@ # 0	ertificate Import Wizard	*	
0.1.1			
Cert	ficate Store Certificate stores are system areas where ce	rtificates are kept.	
_	Windows can automatically select a certificat	e store, or you can specify a location for	
	Automatically select the certificate sto	re based on the type of certificate	
	Place all certificates in the following strength	xe	
	VMware Horizon View Enrolment Ser	ver Trusted Roots Browse	
		Next Cancel	
			×
< ₽	Certificate Import Wizard		
	Completing the Certif	icate Import Wizard	
	The certificate will be imported after	er you dick Finish.	
	You have specified the following se	ettings:	
	Certificate Store Selected by Use Content	 VMware Horizon View Enrollment Serve Certificate 	r Trusted Roo
	File Name	\\Horizon.euc-livefire.com\poftware\Ho	rizon\enroll.ce
	۲		>
		Finish	Cancel
Certificate	e Import Wizard X		
1	The import was successful.		
	ОК		
·			

46. In the **Certificate Store** window accept the defaults and

- Select Next.
- On the **Summary** page select **Finish**.
- When Prompted that The Import was succesful select OK

	or jeen meares (cocars	computer) (vinivare Ho
File Action View Favorites Window Help		
🔿 🖄 📷 🥉 🐂 🔛 🖻 🖬		
Console Root	Issued To	Issued By
Certificates (Local Computer)	47815b94-9cc2-4fc	Trian in Procession Pecci
4 🧾 Personal		Open
Certificates		All Tasks 🕨
Trusted Root Certification Authorities		Cut
Enterprise Trust		Com
Intermediate Certification Authorities		Сору
Instead Publishers		Delete
Director Certification Authorities		Properties
Trusted People		Help
Client Authentication Issuers		Trop
Remote Desktop		
Certificate Enrollment Requests		
Smart Card Trusted Roots		
Trusted Devices		
VMware Horizon View Certificates		
VMware Horizon View Enrollment Server Trusted Roots		
Certificates		
Description: Certificate purposes Brable all purposes for this certificate Disable all purposes for this certificate		
 Enable only the following purposes 		
Enable only the following purposes Note: You may only edit certificate purposes that are allowed the certification path. If The purpose is the purpose of the purpose.	by	
Drake only the following purposes Note: You may only odd certificate purposes that are allowed the entification path. Genere Authentication Code Signing Secure Entail Time Scharping	by ^	
Inske en/i the following purposes Nete: You rung only old certificate purposes that are allowed server Automatication Gener Automatication Gode Signing Secure Shall Time Stapping Monosoft Trust List Signing	^	
Trable only the following purposes Toble true usey only doll certificate purposes that are aloned the certification path. Server Authentication Cocks Signing Secure Enal Time Stamping MonoselT Time Stamping MonoselT Time Stamping MonoselT Time Stamping	by ^	
Checke only the following purposes Note: You may only odd certificate purposes that are aloned the certification path. Server Aufentication Code Signing Goude Enail There Stanning Microsoft Thrust List Signing	by	
Tende only the following purposes Note: You may only edd certificate purposes that are allowed the certification path. Code Spring Code Spring Code Spring Menosoft Trust List Spring Menosoft Trust List Spring Kenosoft Trust List Spring Menosoft Trust List Spring Add Purpose	by A a a a a a a a a a a a a a	
Checke only the following purposes Note: You rung only old certificate purposes that are allowed the certification path. Server Authentication Code Signing Code Signing Monosoft Trust Last Sign	by C D D D D D D D D D D D D D	

- 47. In the **Certificates** Folder
 - Right-click the **imported certificate**
 - Select Properties.
 - In the Friendly name: section type vdm.ec
 - Select OK



48. On your TrueSSO2 server

- 1. Select the **Start button** > **RUN** and type **regedit.exe**
- 2. In the regedit inventory, browse to the following location, browse to
 - HKLM\SOFTWARE\VMware, Inc.\VMware VDM\
 - What we should see is an **Enrollment Service** Key
 - HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service.
 - You will notice there is no **Enrollment Service** key, we need to create one. In our case we have to
- 3. Create the Enrollment Service key
 - Right-click VMware VDM > New > Key and type Enrollment Service as a name

22	Expand					
°.	New		· –	Yey.		
	P III Q III			String Value		
n.	Delete			DW/ORD (22-	hit) Malue	
				OWORD (64-	bit) Value	
	Export			duoin (or	ony raide	
gistry E	ditor (ma Exercity	w Male				
uter/H	KEY_LOCAL_N	ACHINE'SO	TWARE\VMware, I	sc.\VMware VDM	VErvollment Service	
BCDO	DODDDDD	° ^	Name (Default)	Type REG SZ	Data (value not set)	
SAM	DWARE		PrefertocalCa	REG_SZ	1	
SECU	RITY					
0	asses	- 1				
-	dents deukUserEnvi	onment				
G	sogle tel	- 1				
1	icrosoft	- 1				
	colla.org					
0	DBC	- 1				
-	perssH Mover					
-	olicies spisteredAppli	ation				
5	tup					
T	VMmare Drive					
2	VMware Tool VMware VDM					
	Authentic	*				
	Node Mar	1990 B				
	Ervolimen	t Service				
		-				
N	ame			Type		
	(Default)		_	REG_SZ		
"		Modify		0_32		
		Modify B	inary Data			
		Delete				
		Kename				
		Kename				
		Kename				
		Kename				
		Kename				
Johy Ed Edit V	itor fen Favorite	Help				
iday Ed Edit V Ber/Hit	itor iew Favoriter FY_LOCAL_MA	Help	TVGAEL/VMvang, Inc	WANANE VOM EN	nationant Service	
Any Ed Edit V Are/HR KEV_LC BCDD HARD	itor iew Favoriter EY_LOCAL_MA CAL_MACHIN 000000 wa240	Help ICHINE\SOF	NASE(VMoure, Inc Name ≥(Default)	Whiven VOM Le Type REG_SZ	nollevent Service Data (value not cet)	
Activy Edi Edit V Aler/HK KEV_LC BCD9 HARD SAM SECT	itor iew Favoriter EY_LOCAL_MA CAL_MACHIN X000000 W2AE	Help Help	WAREVMware, Inc. Name McDatauth ProfessorcaCa	Type REG_SZ REG_SZ	voltment Service Date (value not ext) 1	
Activy Ed Edit V Arer/HB KEV_LC BCD0 HARD SAM SECUI SOFTI	Itor Image: Favoriter EY_LOCAL_MA ICAL_MACHEN X000000 W248E	Hop CHIPSOF	WUME\VMvare, Inc. Name @Default) ■PrefetiocaCe Edit String	1/Movare VDM.Ex Type REG_52 REG_52	sufferent Service Data (salue not cet) 1 X	1
Anty Ed Edg V Anty Ed Edg V Anty Ed Edg V Anty Ed Edg Salar Soft Ca Ca Ca	iter Favoriter SY_LOCAL_MA CAL_MACHIN WARE SSIS SSIS etb	Help	WUME/VMware, Inc. Name Polauli) Prefet.ocalce Edit Sning Value name Pater LoadCr	Whiver VOME Type REG_52 REG_52	voltment Service Data (value not set) 1 X	E
inty Ed dit V der/HK KEV_LCO HLARD SAM SECUI SOFT CG Ge Ge	Ecr Favorite F	Hop CHINE SOF	WUME/VM/wave, Inc. Name ©Datautij PrefectocaCe Edit String Value name PaterLocaCe Value data	Whivere VOM Le Type REG_52 REG_52	Instituted Service Data (value not ant) 1 X	E]
intry Ed Edit V Jan/HK REV, LC BCD0 BCD0 SAM SECUI SOFT CQ Cli De Ge MA	Itor ieu Facolitei Facolitei CAL, MACHEN WARE Intro Sauttiberfinvier ogin el cossett	Hop CHINESOF	WUME/VM/wave, Inc Name @Default) Protectocation Edit Soring Water same Protectocation Water same Protectocation Water same Protectocation Protectoca	Whiver VOMEN Type REG_SZ REG_SZ	suffraest Service Data (subus set set) 1 X	:
inty Ed der/HK KEY, LC HARD SAM SECUT Cla Cla Cla Cla Cla Cla Cla Cla Cla Cla	Ecor Facodotes TY_LOCAL_MARCHEN 2000000 VILABE SUBSE SUBSE FAUTOMETING SUBSE FAUTOMETING SUBSE FAUTOMETING SUBSE FAUTOMETING FAUTOMETI	Hop CHINE SOF	WUME UNAvere, Inc. Name Protectic calce Edit Song Vide name PaterLookCe Vide dat B	1000use 1000.50 Type 865_52 863_52	Instituted Spruce Data Data Data est ad 1 X OK Censel	:]]
Any Ed dat V dat V dat V BCD0 HARD SAM SECU SOFT Ch SECU SOFT Ch Ch SECU SOFT Ch Ch SECU SOFT Ch SAM SECU SOFT Ch SAM SECU SOFT Ch SAM SECU SOFT Ch SAM SECU SOFT Ch SAM SECU SOFT SAM SAM SAM SAM SAM SAM SAM SAM SAM SAM	Ecor Facodotes TY_LOCAL_MARCHEN 2000000 90424E STY MARE Sources Start	CHILD OF A	TWAREVINaure, Inc Neuro Monta Montali Montalia Managari Mahana Managari Mahana	VMAure VDALE Type 865_52 865_52	Inclused Social Concerning (Social Concerning) X OK Concerning Concerning	
inty Ed Edit V Arenhek BCD0 HLAD SAM SECUI Clu Clu Clu Clu Clu Clu Clu Clu Clu Clu	itor imi Favoritet Yr LOCAL MACHEN CAL MACHEN WARE MY MARE MITY MARE MITY MARE MITY MARE MITY MARE MIT MARE MIT MIT MIT MIT MIT MIT MIT MIT MIT MIT	Holp CORRESSOF	TRAFTIMount Inc Nerre (*) [Pataul) Printe CoalCa Edit String Value seare Printe CoalCa State String	NMAnane VDALEN Type REG_SZ REG_SZ	Institutent Sprives Dates not and 1 OK Cancel	
Any Ed Ed V Jackies HARD SGEU	itor imi Favoritet Yr LOCAL MACHEN CAL MACHEN WARE MITY MARE MITY MARE MITY MARE MITY MARE MITY MARE MIT MARE MIT MIT MIT MIT MIT MIT MIT MIT MIT MIT	Holp CHARTSOF	WMENMANNE, Inc. Nerre ⇒)(cdual)	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	Units Service Oute Julies not and X OX Concel	- -
Intry Ed Edit V Jacobie Salan Halfitt Sector	Eer Factor Facotities EY_LOCAL_MACHIN CAL_MACHIN STY MARE STY MARE STY MARE STY STY STY STY STY STY STY STY	Holp CHINE SOF	WARNAway Inc Nerre Catada Catada Partes costCa Edit Dring Value same Partes costCa Edit Dring Value same Partes costCa Edit Dring Value same	VXMAana V2MLD Type Type REG_S2 REG_S2	Instruct Service Date Dates not und 1 X X X X X X	
International Sectors	Exe Facebook F	Holp CO-BAR SOF	NMATUMawa, Inc Nerra Al (Inducid) Perfest cetal Perfest ce	500 Annue VOALLA Type 805 52 810 52	optiment Sprivite Other Unities not call) 1 X	
Linky Ed Linky Ed Linky Ed Linky Link Hold Sam Secul Soft Ch Secul Soft S	Iter inv Favoriter <u>TV-1004, MA</u> 200000 WARE OTV WARE of AL ALTONETIVE WARE of Set Set Set Set Set Set Set Set	Hop Convert	TWARLYMaure, Inc. Neure Charles and Charles Perfects only Value same Participation Value data	(1946aur 1/2045) Type BEG_S2 REG_S2	Institute Statute Data Data Data I I X X X X X X X X X X X X X	
Any Edit V date/HKK KEV_LCD SAM SECUI SOFT CU De Soft CU De Soft Soft CU CU De Soft N SOFT CU CU De Soft N SOFT CU CU De Soft N SOFT CU Soft N SOFT CU Soft N SOFT CU Soft N SOFT Soft Soft Soft Soft Soft Soft Soft Soft	Ecc Freedom Statements Fr. Local, MAC-199 2000000 EV. Local, MAC-199 2000000 EV. Local, MAC-199 20000 Ev. Local, MAC-199	Hop Oversion	TWARDUNAures, Inc. Neura Charlon Professor Edit Doing Value neura Professor Value data B	VMAuna VDM.Ex Type REG_SZ	ophnest Sories Data Data Data not util 1 X	
Anny Edit Atter Vitater Hill KEVY LICE SAM SECUI SOFT Clu De Soft Main Main Soft De Soft Main Main Soft De Soft Main Soft De Soft Main Soft De Soft Main Soft De Soft Main Soft De Soft Main Soft Mai	Teor TY_LOCAL_MA CAL_MALCHN 000000 CAL_MALCHN 000000 CAL_MALCHN 000000 CAL_MALCHN 000000 CAL_MALCHN 00000 COL 000000 COL 00	Hop CHINESOF	TEMET(SMaryer, Inc. Nervet ab);Ordaal Brefericourdia Edit Storig Value aans Particicaurdia Value aans	1044aaa VOAALA 1974 862,52 863,52	Inclinent Sprints Data Incline Incline Incline St. Center	
Anny Ed Gale V Annihil Storm Storm Gal Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma Na Ca De Gal Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma Ma	The Examples of the second sec	Hop Cherrisof Cherrisof S S S S S S S S	NAME VMANNE INC Nenne Michael Michael Michael Carllon Edit Song Matericanica Inderconta Materianico Materianica Materianica Materianica Materianica Materianica Ma	10740-009 10266.gc 7598 865_52 865_52	Inclused Service Service Inclusion I	
Anny Ed Care V Anny Ed Sam Security Colin	The second secon	I Hop Construction	NAME (Maar, Int Received (Control) (1000-000000000000000000000000000000000	United forder Defenses public set all 1 X X Consol X	
Anty Ed Vareners Soft Soft Ge Soft Soft Soft Soft Soft Soft Soft Soft	The Particular Section 2014 Control Co	Hap Control Sorries	WARDVMoune, Int Neura Orderadi Catadol Catadol Manarianata Manarianata S	VMAugu VDM.Lo Type 825_52 863_52	unhard loca Data 1 X X X X	
Anny EC Varen Hell KEYY-LO Die Ge Main Soft Frank Soft	SEE Try Locks And Locks And Locks And And Locks And	Hap Control SOF Softer SOF E Softer SOF E Softer So	TWARF.VM.oury. Inc. Name Inc. All Ontania Particle Conference Value name Training Conference Value data	1994.aug 1994.g.s 797 865.52 863.52	Interest Banas Por Johan et al. 1 X X X X X X X X X X X X X X X X X X	

- 49. Configure the enrollment service to give preference to the local certificate authority when they are co-located:
 - Add a new String Value
 - Right-click the Enrollment Service key > New > String Value and type the name PreferLocalCa
 - Right-click the PreferLocalCa String value and select Modify and in the Value data: field enter 1
 - Select **OK** to close the window.

Edit String	×
Value name: UseKerberosAuthenticationToCa	
Value data:	
false	OK Careed
	UK Cancel

- 50. Add a new String Value (this is to rectify a bug in 2111)
 - Right-click the Enrollment Service key > New > String Value and type the name UseKerberosAuthenticationToCa
 - Right-click the UseKerberosAuthenticationToCa String value and select Modify and in the Value data: field enter false
 - Select **OK** to close the window.

Edit String	×
Value name:	
UseNTLMAuthentication ToCa	
Value data:	
true	
	OK Cancel

- 51. Add a new String Value (this is to rectify a bug in 2111)
 - Right-click the Enrollment Service key > New > String Value and type the name UseNTLMAuthenticationToCa
 - Right-click the UseNTLMAuthenticationToCa String value and select Modify and in the Value data: field enter true
 - Select **OK** to close the window.



- 52. On your TrueSSO2 server
 - From the Start button, select Run
 - Type services.msc and select OK
 - Scroll down to VMware Horizon View Enrollment Server service in services menu
 - Select and right-click the VMware Horizon View Enrollment Server service
 - Select Restart
 - Close the Services mmc



- 53. On your ControlCenter server
 - Switch to your HORIZON.RDP session



54. Select and right-click the **Start** button

•

Select Command Prompt (Admin)



- 55. In the Administrator: Command Prompt type the following:
 - cd "\Program Files\VMware\VMware View\Server\tools\bin"

C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administra tor --authDomain euc-livefire --authPassword VMware1! --truesso --environment -add --enrollmentServer TrueSSO.euc-livefire.com Enrollment server(s) added to the environment C:\Program Files\VMware\VMware View\Server\tools\bin>_

56. In the Administrator: Command Prompt type the following:-

The enrollment server is added to the global list.



C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUti authPassword VMware1!truessoenvironmentlisten	ilauthAs nrollmentSer	administrat ver TrueSSO	orauthDomai 2.corpPriv.loc	n euc-livefire aldomain cor
pPriv.local				
True SSO environment info				
Enrollment server: truesso2.corppriv.local				
Domain: corppriv.local				
Forest:				
Name: corpPriv.local				
Enrollment CertState: VALID				
Template(s):				
Name: TrueSSOTemplate				
Minimum key length: 2048				
Hash algorithm: SHA256				
Certificate Authority(s):				
Name: corpPriv-AD2-CA				
Name: corpPriv-TRUESSO2-CA				
C:\Program Files\VMware\VMware View\Server\tools\bin>				

57. Wait 2 min before doing the next command

In the Administrator: Command Prompt type the following:-

The output shows the *forest name*, whether the *certificate for the enrollment server is valid*, the name and *details of the certificate template* you can use, and the *common name* of the certificate authority.

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMwarel! --
truesso --environment --list --enrollmentServer TrueSSO2.corpPriv.local --domain
corpPriv.local
```

C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truesso --create --connector --domain corpPriv.local --template TrueSSOTemplate --pr imaryEnrollmentServer truesso2.corpPriv.local --certificateServer corpPriv-TRUESSO2-CA --mode enabled Connector created Domain: corpPriv.local Mode: ENABLED

C:\Program Files\VMware\VMware View\Server\tools\bin>

58. Enter the command to create a True SSO connector, which will hold the configuration information, and enable the connector.

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMwarel! --
truesso --create --connector --domain corpPriv.local --template TrueSSOTemplate --
primaryEnrollmentServer truesso2.corpPriv.local --certificateServer corpPriv-TRUESSO2-
CA --mode enabled
```



59. Enter the command to discover which SAML authenticators are available

Authenticators are created when you configure SAML authentication between Workspace ONE Access and a connection server, using Horizon Administrator.

The output shows the name of the authenticator and shows whether True SSO is enabled

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMwarel! --
truesso --list --authenticator
```



60. You will notice True SSO mode is Disabled. Enter the command to enable the authenticator to use True SSO mode

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMwarel! --
truesso --authenticator --edit --name "Workspace ONE Access" --truessoMode ENABLED
```

For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to VMware Identity Manager. In this case if a password was used and cached, the system will use the password. Set --truessoMode to ALWAYS if you want True SSO to be used even if a password was supplied when the user logged in to VMware Identity Manager

Part 7: Validating Workspace ONE Access User and Group Entitlements.

We will be validating an undocumented issue we have come across in the latest 2108 Connector version of Workspace ONE Access
8 w	orkspace ONE" Acco	ess	
Dashboar	rd 🔹 Users & Groups	Catalog 👻	Identity & Access Manageme
	NEW	Web Apps	CATEGORIES ~
	Application	Virtual Apps C	Collection
	🛛 🚯 BambooHR	Settings Hub Configura	ation

- 1. In the Workspace ONE Access Console
 - Select the **Catalog** tab
 - From the dropdown, select Virtual Apps Collection

Virtual Apps Coll	
Name	Source Type
• Horizon	Horizon
SYNC V DELETE Sync with safeguards Sync without safeguards Zon	

- 2. In the Virtual Apps Collections window
 - Select the radio button next to Horizon
 - Select the **dropdown** next to **SYNC**
 - Select Sync without safeguards

👖 Apps 🔇	my-ip.livefire.lab/ip VMware Hor	
8 Works	Pace ONE" Access	
Dashboard	V Users & Groups 🕻 atalog 🔻 Id	
Vi	rtual Apps	
Application		

- 1. In the Workspace ONE Access console
 - Select the Users & Groups tab

Users (10)			
User Name	User ID	Domain	Directory
Admin, Tenant	administrator	System Domain	System Directory
L Debio,Mark	Mark	euc-livefire.com	LivefireSync
L Dusello, Fernando	Fernando	euc-livefire.com	LivefireSync
L Goodsell,Clint	Clint	corppriv.local	corppriv.local
L Ikin,Kevin	Kevin	euc-livefire.com	LivefireSync

- 2. In the **Users** Interface
 - Select Goodsell, Clint

Sets to test cli Image meritation and and and and and and and and and an					
First Name Circl Circl Consolid Searance Circl Consolid Sear	<back list<="" td="" to="" user=""><td></td><td>Profile Groups Two-Factor Auther</td><td>ntiaction Apps</td><td></td></back>		Profile Groups Two-Factor Auther	ntiaction Apps	
Last ture Ocodedi Circ Constantion Constantio		First Name	Clint		
Clif Goodsall (Chin) Lise anale Clif disclopupPhi com Directory: Enail disclopupPhi com Directory: To assign or unassign the admin role to the user, click hare Directory: To assign or unassign the admin role to the user, click hare Directory: To assign or unassign the admin role to the user, click hare Directory: The Plane / Oronge / The Plane / Administration / Oronge Click to User Lit Plane / Oronge / The Plane / Administration / Oronge Click closed 1 Click closed Plane / Oronge / The Plane / Administration / Oronge Click closed 1 Click click is enaided Plane / Oronge / The Plane / Administration / Oronge Projectory Plane / Oronge / The Plane / Administration / Oronge Directory Plane / Oronge / The Plane / Administration / Oronge Directory Plane / Oronge / The Plane / Administration / Oronge Directory Plane / Oronge / The Plane / Administration / Oronge Directory Plane / Oronge / The Plane / Administration / Oronge Directory Plane / Oronge / The Plane / Administration / Oronge Directory Plane / Oronge / The Plane / Oronge		Last Name	Goodsell		
(Control Exat indicoorphic control Densite::::::::::::::::::::::::::::::::::::	Clint Goodsell	Username	Clint		
Bitelsong Output Mall Ruk User Process Material Child(Scorp/Process) To assign or unassign the admin role to the user, click heres Child Controll Impact Administration Child Child Process Administration Child Process Administration Child Child Process Administration Child Process Administre Child Process Administration Child Process Administrel	(Clint) Domain: corppriv.local	Email	clint@corpPriv.com		
To assign or unasage, the administre to the user, idick heres Tripping the identication of the user, idick heres The Concell	Directory: corppriv.local Status: 🥝 User is enabled	Role	User		
Version local	Principal Name: Clint@corpPriv.local Distinguished Name: CN=CLINT		To assign or unassign the admin role to the use	r, click here	
Literation Literation District Constraint Children District Constraint District Constraint <td><back list<="" td="" to="" user=""><td></td><td>Profile Groups Two-Factor Author</td><td>entication Apps</td><td></td></back></td>	<back list<="" td="" to="" user=""><td></td><td>Profile Groups Two-Factor Author</td><td>entication Apps</td><td></td></back>		Profile Groups Two-Factor Author	entication Apps	
Exact Call		1 Entitlements			Add Entitlemen
Circl Condedi Circl		Expand All			
Domain: componitudii Statu: Uncerto:: componitudii Statu: Uncerto:: componitudii Submain:: Coll:: Componitudii: Componitudi: Componi	Clint Goodsell (Clint)	> Web Applications (0))		
Statust: Use is enabled Principalities Marcia: Child GoopPrinced Statust: Child Statust: Child Statust: Control Network	Domain: corppriv.local Directory: corppriv.local	↔ Horizon View Deskto	ops (1)		
Vincipuid Manane: Child GroupPhin Vial Manae: Child Gro	Status: 💙 User is enabled	ITEM	TYPE	DEPLOYMENT	
Extensit (b: 6x49025 4226 4376 4506 550 C Car Co Code C Car Co Code C Car	Principal Name: Clint@corpPriv.local Distinguished Name: CN=CLINT GOODSELL,OU=SALES,DC=CORPPRIV,D C=LOCAL	W10_CorpPri	Horizon View Desktop	User-Activated	1
Cases 20 Total and the second and t	External ID: daef3625-e2a5-4a79-b15b- 2efdcd5f1300	> Horizon View Applic	ations (0)		
	Sack to User List	1	Profile Groups Teo-Factor Authentication Apps		
Circ Open Construction > The Applications (1) Description comprision > The Applications (1) Description > The Applications (1)		0 Entitlements			
Cline Code/all > Table Applications (1) Density comparison > Table Solutions (1)		Expand All			
Operation componential Detention, componential Status QU err is realised → Maticas Ware Detectings (B) realised realised realised <threalise< th=""> realised realis</threalise<>	Clint Goodsell (Clint)	> Web Applications (0)			
Status Other is noticed memory bases: Conject/memory memory bases: Conject/memory Doubling-base Address Conject/memory This user is not entitled to any applications of this type: Conject/memory This user is not entitled to any applications of this type: Image: Solution This user is not entitled to any applications of this type: Image: Solution This user is not entitled to any applications of this type:	Domain: corppriv.local Directory: corppriv.local	✓ Horizon View Desktops (0)			
Dotanguadate Name: CII-CLUT This user is not estilled to any applications of this type Control Line: Control	Status: User is enabled	ITEM	TYPE DEPLOTMENT		
Vicinary View Applications (8) Vicinary View Applications (8) max rec	Distinguished Name: CN=CLINT GOODSELL,OU=SALES,DC=CORPPRIV,D		This user is not entitled to any applications of this type.		
mm mm<	External ID: daef3625-e2a5-4a79-b15b- 2efdod5f1300	V Horizon View Applications (0)			
Exercise User	2 Eastle	ITEM	TYPE DEPLOYMENT This user is not entitled to any applications of this type.		
	Delete User				

- 3. In the **Clint Goodsell** interface
 - Select Apps tab
- 4. In the **Apps** tab
 - Expand Horizon View Desktops and Horizon Applications
 - There should be associated virtual desktops and virtual applications
 - If there are not move on to step 5, everything fine in your environment, move on to Part 8

Directories (3)	
Directory Name	Туре
System Directory	Local Directory
LivefireSync	Active Directory over LDAP
corppriv.local	Active Directory over LDAP

- 26. In the Workspace ONE Access Admin console
 - Select the Identity & Access Management tab

• In Directories area

• Select corppriv.local

Corppriv.local Type: Active Directory over LDAP	<back directories<="" th="" to=""></back>
corppriv.local Type: Active Directory over LDAP	កុ t :
Sync with Safeguards Sync without Safeguards	corppriv.local Type: Active Directory over LDAP
Sync Settings	Sync with Safeguards Sync without Safeguards
Delete Directory	Sync Settings

27. In the **corppriv.local** interface

- Select Sync,
 - From the dropdown, select Sync without Safeguards
 - Once the sync has completed
 - Select the User & Groups tab
 - Select Debio Mark
 - Select the Apps tab
 - Expand Horizon View Desktops and Horizon View Applications
 - You should now have your Virtual Desktops and Virtual Applications
 - Note this is an undocumented feature we have discovered with regard to the 2108 connector version of Workspace ONE Access

Sack to User List		Profile	Groups	Two-Factor Authentication Apps	
	1 Entitlements				Add Entitlement
	Expand All				
Clint Goodsell (Clint)	> Web Applications (0)				
Domain: corppriv.local Directory: corppriv.local	➤ Horizon View Desktops (1)				
Status: 🔇 User is enabled	ITEM	TY	PE	DEPLOYMENT	
Principal Name: Clint@corpPriv.local Distinguished Name: CN=CLINT GOODSELL,OU=SALES,DC=CORPPRIV,D C=LOCAL	W10_CorpPriv	н	orizon View D	esktop User-Activated	1
External ID: daef3625-e2a5-4a79-b15b- 2efdcd5f1300	> Horizon View Applications ())			
✓ Enable					

- 28. Once the sync has completed
 - Select the User & Groups tab
 - Select eGoodselbio Mark
 - Select the Apps tab
 - Expand Horizon View Desktops and Horizon View Applications
 - You should now have your Virtual Desktops and Virtual Applications
 - Note this is an undocumented feature we have discovered with regard to the 2108 connector version of Workspace ONE Access
 - In the authoring of this lab there were a lot more attempts made. On a first test and write, its not possible to validate the scope of this issue.
 - It might be necessary to reach out to your instructor for further assistance

Part 8: Testing Untrusted Domain Integration with Workspace ONE Access



- 1. On your ControlCenter Server
 - Open a New Incognito mode window session with your Chrome browser



2. In the Chrome browser

- Using your custom Access URL, launch your Workspace ONE Access porta
- In the **Select your Domain** area
 - Select corpPriv.local
 - Select Next

Workspace ONE*	
username clint	
password	
corppriv.local	
Sign In	
Forgot password?	
Change to a different domain	
vm ware:	

- 3. In the Workspace ONE Access login
 - Under **username**
 - enter clint
 - Under **password**
 - enter VMware1!
 - Select Sign In

Favorites Intellig	ent Hub X	: +			
← → C ↔	aw-nikko4	44hilivefire.vidr	npreview.com/	catalog-po	rtal/ui#/ar
S my-ip.livefire.lab/ip	p 🚾 VMware H	orizon® ass NS	SX manager 🛛 🖷	App Volum	ies Mana
	EUCLI	F Favorites	Apps	People	For You
	_				
	Favorites				

- 4. In the Web based Intelligent Hub
 - Select the Apps tab

👽 Apps Intelligent Hub 🛛 🗙 🕂	
← → C ☆ 🔒 aw-nikko444hiliv	efire.vidmpreview.com/catalog-port
S my-ip.livefire.lab/ip 🔤 VMware Horizon®	🔍 🗚 NSX manager 🛛 📲 App Volume
EUCLF	Favorites Apps People
	Q Search Apps
All Apps	
W10_CorpPriv	
Horizon	
Categories	
All Apps	Virtual Apps

- 5. In the Web based Intelligent Hub
 - Under the Apps tab
 - Select the W10_CorpPriv entiltlement



- 6. On your Horizon web client
 - Note that you had a single sign-on experience
 - Log off when done

Part 9: Unified EndPoint Integration with the Active Directory Untrusted Domain



- 1. On your laptop / Desktop
 - login with your Custom Workspace ONE UEM Credentials



- 2. In the Workspace ONE UEM Admin Console
 - Go to GROUPS & SETTINGS > All Settings

	engel.markham	
	System Getting Started Branding Enterprise Integration	
	Security Help Localization Terms of Use S/MIME Advanced	
System		
Enterprise Integration Services Certificate Authorities Content Gateway Cloud Connector Directory Services		
Email (SMTP) VMware Tunnel		

- 3. In the Workspace ONE UEM Admin Console
 - Under System, select Enterprise Integration
 - Under Enterprise Integration, select Directory Services

Bind Password		CHANGE
	Domain	Server
	euc-livefire.com	ControlCenter.euc-live
	ADD DOMAIN	
> Advanced		

4. In the Workspace ONE UEM Admin Console

- In the **Directory Services** window > **Server** Tab
 - Scroll down and select + ADD DOMAIN

ırd		СНА
	Domain	Server
	euc-livefire.com	ControlCenter.euc-live:
	corpPriv.local	ad2.corpPriv.local
	ADD DOMAIN	
ist relationship the specified	YES NO	()

- 5. In the Workspace ONE UEM Admin Console
 - Under the **Domain** area : enter corpPriv.local
 - Under the **Server** area : enter **ad2.corpPriv.local**

System > Enterprise	Integration	
Directory Serv	ices 💿	
Server	User	Group
Current Setting	🔿 Inherit (Override
Domain		Base DN*
euc-livefire.com		DC=euc-livefire,DC=cor
corpPriv.local		DC= <u>corpPriv,DC</u> =Local
Hear Object Clace *	BAPPAR	

- 6. In the Workspace ONE UEM Admin Console
 - In the Directory Services window > User Tab
 - Next to corpPriv.local
 - Enter DC=corpPriv,DC=Local

Server	User	Group	
Current Setting	🔿 Inherit	Override	
Jomain		Base DN*	
euc-livefire.com		C=euc-livefire,DC=com	+
corpPriv.local		DC=corpPriv,DC=Local	+
) Override 💿 Inherit or	Override SAVE TEST	CONNECTION	SET

7. In the Workspace ONE UEM Admin Console

- In the Directory Services window > Group Tab
- Next to corpPriv.local
 - Enter **DC=corpPriv,DC=Local**
 - Scroll down
 - select SAVE

Part 10: Enrolling the EndPoint and testing the Integration



- 1. On your **ControlCenter** server
 - · Open the Remote Desktops folder
 - Select and launch the W10EXT01a.RDP shortcut
 - Login with the username: W10EXT01a\administrator
 - Login with the **password: VMware1!**
 - Select OK



- 2. On the W10EXT01a Desktop
 - In the **Type here to search** area , type **hub**
 - When the Workspace ONE Intelligent Hub is found, select Open
 - If your **Workspace ONE Intelligent Hub** does not load properly, go services and start the **Airwatch** service



- 3. In the Workspace ONE Intelligent Hub console
 - Under Email or Server Address
 - type dw-livefire.awmdm.com
 - Select Next

Workspace ONE Intelligent Hub	-		×
		ŝ	
Email or Server Address			
https://dw-livefire.awmdm.com			
Group ID			
markham444			
Next			

- 4. In the Workspace ONE Intelligent Hub console
 - Under Group ID
 - type your UEM Tenant Group ID
 - Select Next

Workspace ONE Intelligent Hub		-	×
	Workspace ONE* Select Your Domain		
	Remember this setting		
	Next		
	vinwale		

- 5. In the Workspace ONE Intelligent Hub console
 - Under Select Your Domain
 - From the dropdown select corpPriv.local
 - Select Next



- 6. In the Workspace ONE Intelligent Hub console
 - Under **username**
 - enter Clint
 - Under password
 - enter VMware1!
 - Select Sign in
 - Note you will get a Enrolling your device this will take several minutes window
 - When prompted, select I Agree
 - On the Congratulations window, select Done
 - On the Hello, Clint window, select Get Started

https://cas.vidmpreview.com/cas: × +				
\leftarrow \rightarrow C \triangle \triangleq cas.vidmpreview.com/cas/t/AW-L	IVEFIREENGELRN/API/1.0/REST/lan	ding?EAB_CALLBACK_U	IRL=%2Fauth%2Flog	jin%2Fembeddedauth
Apps .	Select a certificate Select a certificate to authenticate yours	elf to cas.vidmpreview.con	n:443	×
	Subject	Issuer	Serial	
	Clint	engelmarkham	018F9D	
	Certificate information		OK Ca	incel
L				

- 7. In the W10EXT01a desktop
 - Launch your **browser**
 - Enter your custom Workspace ONE Access URL
 - At the Domain Login, from the dropdown, select CorpPriv.local
 - Select Next
 - In the Select a certificate,
 - Select OK

	ι
	Add you

- 6. In the Workspace ONE Access Intelligent Web Hub
 - Select the Apps tab
 - Enter your custom Workspace ONE Access URL
 - Launch your W10CorpPriv entitlement
 - You should now have a complete Single Sign-on experience with Workspace ONE

About the Author: Reinhart Nel

https://www.livefire.solutions/meet-the-team/reinhartnel/

Any questions related to this session, email Reinhart at RACE-Livefire-EUC <RACE-Livefire-EUC@vmware.com>