## Installing and Configuring Horizon TRUESSO

## **Overview**

Traditionally when authenticating to Workspace ONE Access using a 3rd party authentication method, the user we will by default, not have a Single Sign-On experience when trying to launch any VMware Horizon based resource through Workspace ONE Access.

Traditionally Single Sign-On would only be an issue when using a 3rd Party authentication method. To solve this problem we would deploy what is known as the Horizon Enrollment services to facilitate a Single Sign- on experience. The Horizon Enrollment services, integrates with Microsoft Certificate Services to provide a solution to this challenge and we refer to the solution as **Horizon TRUE SSO** 

#### Since December 2019

Caching of Passwords for Horizon has been disabled and a user will always have to reauthenticate when they select their entitlement. https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/rn/VMware-Workspace-ONE-Access-Cloud-Release-Notes.html

We have already demonstrated how to facilitate a single-sign on with password based authentication. When authenticating to Workspace ONE Access using a 3rd Party authentication method and wanting to launch a Horizon based resource, one will still be prompted for password based Authentication.

In a Zero-Trust environment, it is critical we secure our Horizon Sessions with authentication methods that are not Password based.

In this lab scenario the 3rd party authentication method we use to login into Workspace ONE Access will be a certificate based method of authentication.

**In June 2020**, Caching of Passwords was re-introduced as an option to re-enable, to allow Password Single Sign-On based Authentication. Caching of Passwords is disabled by default.

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

We will start off by doing the following:

- 1. Log into a Windows 10 Desktop and demonstrate the limitation
- 2. Deploy and configure TRUE SSO
  - Deploy and configure Horizon Enrollment services
  - Integrate and configure Active Directory Certificate services with Horizon Enrollment services
- 3. Log into a Windows 10 Desktop and demonstrate the solution

Please Note. This lab is not for the faint-hearted. You will see the implementation process of deploying and configuring Enrolment services in Horizon and integration with Microsoft Active Directory services.

You will also experience first hand how reliant Enrollment services on Microsoft Active Directory Certificate services is.

# Part 1: Log into a Windows 10 Desktop and demonstrate the limitation

nuteration - w10EXT01a.euc-livefire.com - Remote Desktop Connection	tion	-		×
<b>a</b>				
Recycle Bin				
itteyed: Bin Socije Citicane Vilvare Elazie Mensorit Sobje				
€ P Type here to search	o # 2 = 🗄 🚖 📀 🕵	12:20 10 3/22/	2021	$\overline{}$

- 1. On the ControlCenter server Desktop,
  - Switch back to your the W10EXT01a.RDP session
    - W10EXT01a.RDP is enrolled into Workspace ONE UEM and has a certificate already deployed

- If necessary login as:
  - Username: administrator@euc-livefire.com
  - Password: VMware1!

+		
com/cas/t/AW-LIVEFIRE-MARKUSRN	I444/API/1.0/REST/landi	ng?EAB_CALLBACK_URL=%2F
Select a certificate Select a certificate to authenticate your	self to cas.vidmpreview.com	:443
Subject	lssuer	Serial
Mark	markusheinraadgmail	0187D1
		<u>b</u>
Certificate information		OK Cancel
	+ com/cas/t/AW-LIVEFIRE-MARKUSRN Select a certificate Select a certificate to authenticate your Subject Mark Certificate information	+ com/cas/t/AW-LIVEFIRE-MARKUSRN444/API/1.0/REST/landi Select a certificate Select a certificate to authenticate yourself to cas.vidmpreview.com Subject Issuer Mark markusheinraadgmail Certificate information

- 2. Open a **browser** on your windows 10 desktop
  - Enter your custom Workspace ONE Access URL
  - On the **Select a certificate** window note the account of the certificate and select **OK**

😼 w10EXT01a -	w10EXT01a.euc	livefire.com	- Remote Deskto	p Connection			
O Apps   VMw	vare Intelligent Hub	× +					
× ← → œ	aw-livefire-	markusrn444.	widmpreview.com/	catalog-portal/ui#	/apps		
<b>@</b>	Favorites	Apps	People Fo	r You Supp	port		
		_					
	Q Search	n Apps					
			New App	s All Apps	Categ	ories 🗸	
New A	Apps						
<b>1</b>							
	8				2		
			C	2		-	
	Calculator	Inte	ernet Explorer	Pain	t	W10IP	
₽ H	orizon ••	• 🖓 Hor	rizon •••	C Horizon		- Horizon	
a.	rearchitypha						
	-	Net	w Apps All	Apps Ca	tegories 🗸		
							×
New Apps	Passv	ord Re	quest				
	We need	your passwor	rd to sign in to Cale	ulator.			
	Passin	au					
Calculator					Cancel	Sign In	
Harizan	28	vizon	··· D Horiz	on •••	Horizon		
			MD				
MD M	ark Debio						
			_				
Account							
Sign out							

- 3. On the Workspace ONE Intelligent Hub console,
  - Under Apps,
    - Select Calculator
- Notice we are getting a Password request.
  - We used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password Auth method, to pass on to the Horizon Agent.
- Select Cancel to close the Password Request window
- In the top right-hand corner,
  - Select and right-click the User Icon ,
  - select Sign out
- Close your Browser
- Minimize your W10EXT01a.RDP session

We will now go and configure Horizon Enrollment Services, to be able to facilitate a Single Sign-On experience for 3rd Party Authentication methods

## Part 2. Installing a sub-ordinate CA and the Enrollment services



- 1. On your **ControlCenter** server
  - Open the **Remote Desktop** Folder
    - Launch the TrueSSO.RDP shortcut,
      - login as administrator@euc-livefire.com.
      - Use the password VMware1!
    - Server Manager should launch automatically on the **TRUESSO** Server, desktop interface
      - On the Server Manager Interface
        - Select Manage > Add Roles and Features

)	Add Roles and Features Wizard
Before you begin	DESTINATION SERVER TrueSSO.euc-livefine.com
Before You Begin Installation Type	This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
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 Cancel

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

	Add Roles and Features Wizard	- 0
elect installation	on type	DESTINATION SERVE TrueSSO.euc-Invefre.co
Before You Begin Installation Type	Select the installation type. You can install roles and for machine, or on an offline virtual hard disk (VHD).	eatures on a running physical computer or virtue
Server Selection Server Roles	Role-based or feature-based installation     Configure a single server by adding roles, role serv	ices, and features.
	<ul> <li>Remote Desktop Services Installation Install required role services for Virtual Desktop Inf or session-based desktop deployment.</li> </ul>	frastructure (VDI) to create a virtual machine-bas
	< Previous	Next > Install Cancel

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

elect destinati	DD Server TruessOwic-Ive	SERVE fre.co
Before You Begin	Select a server or a virtual hard disk on which to install roles and features.	
Installation Type	Select a server from the server pool	
Server Selection	Select a virtual hard disk	
Server Roles	Server Pool	
Features	Etter.	
	ringi	_
	Name IP Address Operating System	
	TrueSSO,euc-livefire.com 192.168.110.81 Microsoft Windows Server 2012 R2 Datacenter	
	1 Computer(s) found	
	This page shows servers that are running Windows Server 2012, and that have been added by us Add Servers command in Server Manager. Offline servers and newly-added servers from which o collection is still incomplete are not shown.	sing t data

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

select server ro	les
Before You Begin	Select one or more roles to install on the selected server.
Installation Type	Roles
Server Selection	Active Directory Certificate Services
Server Roles	Active Directory Domain Services
Features	Active Directory Federation Services
	Active Directory Lightweight Directory Services
	Active Directory Rights Management Services
Add Roles an	d Features Wizard
Add features that are now	ired for Active Directory
Certificate Services?	and for Active Directory
The following tools are required	to manage this feature, but do not
have to be installed on the same	server.
A Remote Server Administrati	on Tools
<ul> <li>Role Administration Too</li> </ul>	ls
Active Directory Certi     Teels) Certification	ficate Services Tools
(roots) certificatio	in Accounty management roots
<ul> <li>Include management tools (</li> </ul>	if applicable)
	Add Eastware Cased
	Add Features Cancel
Before You Begin	Add Features Cancel Select one or more roles to install on the selected server.
Before You Begin Installation Type	Add Features Cancel Select one or more roles to install on the selected server. Roles
Before You Begin Installation Type Server Selection	Add Features Cancel Select one or more roles to install on the selected server. Roles Concerning Descharge Contribution Services
Before You Begin Installation Type Server Selection Server Roles	Add Features Cancel Select one or more roles to install on the selected server. Roles Roles Active Directory Contificate Services Active Directory Contificate Services
Before You Begin Installation Type Server Selection Server Roles Features	Add Features Cancel Select one or more roles to install on the selected server. Roles
Before You Begin Installation Type Server Selection Server Roles Features AD CS	Add Features     Cancel       Select one or more roles to install on the selected server.       Roles       Chrise Directory Centificate Services       Active Directory Federation Services       Active Directory Federation Services       Active Directory Federation Services
Before You Begin Installation Type Server Selection Server Roles Reatures AD CS	Add Features     Cancel       Select one or more roles to install on the selected server.       Roles       Chice Directory Centificate Services       Active Directory Federation Services       Active Directory Federation Services       Active Directory Linkhaudidh Directore Sanitar
Before You Begin Installation Type Server Selection Server Roles Features AD CS IAccess Services	Add Features Cancel Select one or more roles to install on the selected server. Roles           Chiles Directory Centificate Services           Active Directory Centificate Services           Active Directory Centificate Services           Active Directory Centification Services           Active Directory Centification Services           Active Directory Centification Services           Active Directory Centification Services
Before You Begin Installation Type Server Selection Server Roles Features AD CS J Access Services 4 Services	Add Features     Cancel       Select one or more roles to install on the selected server.       Roles       Other Directory Cettificate Service:       Active Directory Cettificate Service:
Before You Begin Installation Type Server Selection Server Rolos Features AD CS Acces Services Services	Add Features     Cancel       Select one or more roles to install on the selected server.       Roles       Active Directory Certificate Services       Active Directory Pederation Services       Active Directory Federation Services       Active Directory Federation Services
Before You Begin Installation Type Server Selection Server Rokes Peatures AD CS IAccess Services d Services	Add Features Cancel Select one or more roles to install on the selected server. Roles
Before You Begin Installation Type Server Selection Server Roles Pathues AD CS IAccess Services d Services services	Add Features Cancel Select one or more roles to install on the selected server. Roles Control Directory Contificate Service Active Directory Contificate Service Active Director Planation Services Active Director Linkhusicher Directory Cancier

- 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

elect features		DESTINATION SERVI TrueSSO.euc-livefire.co
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	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 provid the ability to model a range of business processes.
	< III > Next	> Install Cancel

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



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

1	Add Roles and Features Wizard	_ <b>_</b> X
Select role servi	ices	DESTINATION SERVER TrueSSO.euc-livefire.com
Before You Begin Installation Type	Select the role services to install for Active Directory Certif	icate Services
Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certificate Enrollment 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

onfirm installa	tion selections	TrueSSO.euc-liver	fre.cor
Before You Begin	To install the following roles, role services, or features on selected server, cl	ick Install.	
Installation Type	Restart the destination server automatically if required		
Server Selection Server Roles Features	Optional features (such as administration tools) might be displayed on this been selected automatically. If you do not want to install these optional fea their check boxes.	page because they hi tures, click Previous t	ave lo clea
AD CS	Add Roles and Features Wizard	×	
Role Services Confirmation Results	If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts	?	
	Export configuration settings Specify an alternate source path		

- 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

b .	Add Roles and Features Wizard	- 0
Installation pro	gress	DESTINATION SERVER TrueSSO.euc-livefire.com
	View installation progress	
Installation Type	Feature installation	
	Configuration required. Installation succeeded on TruessOleuc-Invelire.com	n.
	Active Directory Certificate Services	
AD CS Role Services	server Configure Active Directory Certificate Services on the destination server	estination
Confirmation	Castilland to the control of the con	
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 open this letails.
	< Previous Next > CI	Cancel

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

	AU CS Contiguration
Credentials	DESTINATION SERVER TrueSSO.euc-livefire.com
Credentials Role Services Confirmation Progress Results	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: EUC-LIVEFIRE\administrator Change
	More about AD CS Server Roles
	< Previous Next > Configure Cancel

- 11. On the **Credentials** window
  - Select Next

ole Services	DESTINATION SERVER TrueSSO.euc-livefire.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Certificate Request Certificate Request 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 Cancel

#### 12. On the Role Services page,

Select the Certificate Authority checkbox

otup Typo	DESTINATION SERV
etup Type	TrueSSO.euc-livefire.o
Credentials	Specify the setup type of the CA
Role Services	
Setup Type	Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to
CA Type	simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Private Key	
Cryptography	Enterprise CA Enterprise CAs must be domain members and are twically online to issue certificates or
CA Name	certificate policies.
Certificate Request	O Standaloge CA
Certificate Database	Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require
Confirmation	DS and can be used without a network connection (offline).
	More about Setup Type

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



#### 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

ryptography fo	or CA		DESTINATIO TrueSSO.euc-li	N SERVE
Credentials Role Services	Specify the cryptographic options		Key length:	
Secop type	#Microsoft Software Key Storage Provider	-	2048	
Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	SHA256 SHA384 SHA512 SHA1 MD5	s accessed b	by the CA.	
	More about Cryptography			

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

	AD CS Configuration
CA Name	DESTINATION SERVER TrueSSO.euc-livefire.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name	Specify the name of the CA. Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified. Common name for this CA: euc-livefire-TRUESSO-CA
Certificate Request Certificate Database Confirmation Progress Results	Distinguished name suffo: DC=euc-livefire,DC=com Preview of distinguished name: CN=euc-livefire-TRUESSO-CA,DC=euc-livefire,DC=com
	More about CA Name  A Previous       Next >     Configure     Cancel

#### 17. On the **CA Name** window

• Observe the CA naming convention

Select Next

<u>-</u>	AD CS Computation	
Certificate Req	uest	DESTI TrueSSC
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name	Request a certificate from parent CA You require a certificate from a parent certification authoritistic entificate from an onlia a file to submit to the parent CA. Send a certificate request to a parent CA: Select: C A name	y (CA) to allow this sub ne CA or you can store
Certificate Request Select Certification Aut	nority ? ×	
CA	Computer CA ControlCenter.euc-ivefre.com	
AD CS Configuration	OK Cencel	- • ×
Certificate Reque	ist	DESTINATION SERVER TRUESSO.euc-livefire.com
Credentials Role Services Setup Type Ca Type Private Key Cryptography Ca Name Certificate Beouts Certificate Database Confirmation Progress Peredia	Request a certificate from parent CA Tou repairs a certificate from a parent certification activity (2A) to allo the certificate. You can repeat certificate from a notifier CA or you fit is submitted bus parent CA. Sector Gamma Comparent activity of the certification of the certif	w this subordinate CA to can store your request to Select.
	You must manually get a certificate back from the parent CA to m	sake this CA operational.
	Vou must manually get a certificate back from the parent CA to m	ake this CA operational.

18. On the Request a certificate from parent CA,

- Select the radio button next to Send a certificate request to a parent CA:
- In the Select box, select the radio button, next to CA name
- To the right of the **Parent CA** box click the **Select** button
  - In Search box, enter ControlCenter and select Check Names
- Select **OK** accept the Defaults
- Select Next

A Database		TrueSSO.euc-livefire.com
Credentials Role Services Seture Turne	Specify the database locations	
CA Type	C:\Windows\system32\CertLog	
Private Key	Certificate database log location:	
Cryptography CA Name Certificate Request	C/\Windows\system32\CertLog	
Certificate Database		
Confirmation		
	More about CA Database	

### 19. On the **CA Database** window,

• Select Next

Credentials	To configure the following roles	, role services, or features, click Configure.
Role Services	<ul> <li>Active Directory Certificat</li> </ul>	e Services
Setup Type		
CA Type	Certification Authority	Enternine Schoolingte
Private Key	Contographic provider	RSA#Microsoft Software Key Storage Drouider
Cryptography	Hash Algorithm:	SHA256
CA Name	Key Length:	2048
Certificate Request	Allow Administrator Interaction	Disabled
Certificate Database	Certificate Validity Period:	Determined by the parent CA
Confirmation	Distinguished Name:	CN=euc-livefire-TRUESSO-CA,DC=euc-livefire,DC=com
Confirmation	Online Parent CA Information:	Controlcenter2.euc-livefire.com/euc-livefire-CONTROLCENTER2
	Certificate Database Location	CA C/Windows\system32\CertLop
	Certificate Database Log Location:	C?(Windows/system32)/CertLog

#### 20. On the **Confirmation** window

• Select Configure



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

## Part 3: Deploying and Configuring Horizon TRUE SSO



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

🚡 Console1 - [Console Root\Certificat	tion Authority (Le
File Action View Favorites Window	/ Help
Console Root  Certification Authority (Local)  Certificates  Revoked Certificates  Second Requests  Failed Requests  Certificate Templates  New View New Window f New Taskpad V Refresh	Name Directory Ema Domain Cont Kerberos Auth EFS Recovery Basic EFS Domain Cont h h rom Here

- 2. Expand the **euc-livefire-TRUESSO-CA i**nventory
  - Select Certificate Templates,
  - Right-click and select Manage

Certificate Templates Console		
File Action View Help		
🗢 🏟 💼 🙆 💼		
Certificate Templates (Controlce	Template Display Name	Schem ^
	Rev Recovery Agent	2
	I NSX	2
	OCSP Response Signing	3
	RAS and IAS Server	2
	Root Certification Authority	1
	The ster (Offine request)	1
	🗷 Smartcard Logon	1
	a Smartcaru Oser	1
	Representation Authority	1
	R Trust List Signing	1
	🖳 User	1
	🗷 User Signature Only	1
	R VMware Certificate	2
	Rev VMware-SSL	2
	Reb Server	1
	Workstation Authentication	2
		~
< >	<	>
a contra de la c	and the second second second	10 //CA.3 01

- 3. In the **Certificate Template** Console
  - Select the Smartcard Logon template

Certificate Templates Console		
File Action View Help		
(= =) 📰 🖾 🖬 🖬		
Certificate Templates (Controlce	Template Display Name	Sch
	🖳 Key Recovery Agent	2
	R NSX	2
	OCSP Response Signing	3
	RAS and IAS Server	2
	Root Certification Authority	1
	Router (Offline request)	1
	Sr Duplicate Template	1 1
<b>u</b>	P SI All Toslo	1
	Properties	1 1
	U     Help     Invite Certificate	1 2
	R VMware-SSL	2
	- WMware-SSL - Web Server	2 1
	교 VMware-SSL 교 Web Server 교 Workstation Authentication	2 1 2

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

Properties of New Template	×
Schiert Name Center Jesuance Requirements	
Supercenter Estanciana Casultu	
Superseded remplates Extensions Security	_
Compatibility General Request Handling Cryptography Key Attestation	n
The template options available are based on the earliest operating system versions set in Compatibility Settings.	
Show resulting changes	
Compatibility Settings	
Certification Authority	
Windows Server 2012 R2 V	
Certificate recipient	
Windows 8.1 / Windows Server 2012 R: V	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.           OK         Cancel         Apply         Help           International template         Mark 100 pages at	
These settings may not prevent earlier operating systems from using this template. OK Cancel Apply Help Fearman International Concelstance of the Many settings	
These settings may not prevent earlier operating systems from using this template.           OK         Cancel         Apply         Help           Network wave request to set of the set of the set.         Methods         Help	
These settings may not prevent earlier operating systems from using this template.           OK         Cancel         Apply         Help           International internationa	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	
These settings may not prevent earlier operating systems from using this template.	

- 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**.

	Prop	perties	of New	Template	×		
Subject N	lame	Ser	ver	Issuance	Requirements		
Supersec	ded Templa	tes	Exte	nsions	Security		
Compatibility	General	Request	Handling	Cryptography	Key Attestation		
Template dis TrueSSO Te	Template display name: TrueSSO Template						
Template na TrueSSOTe	me: mplate						
Validity perio	d: ıns 🗸	]	Renewa 0	l period: hours v			
Publish c Do no Direct	ertificate in ot automatic ory	Active Di ally reenro	rectory oll if a dupli	cate certificate	exists in Active		
		Castifi					
The renewal per automatically se To change the r	iod (6 week et the renew enewal or v	s) is larger al period t alidity peri	than the maxim o the maxim od to a diffe	piates minum allowe num allowed (0 rrent value, clici	d. To hours), click OK. k Cancel.		
				ОК	Cancel		

- 6. Select the General tab,
  - Under Template display name: type TrueSSO Template,
    - You will notice **Template name** gets filled in automatically **Do NOT edit the Template name**. Leave as is in the screenshot
  - 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 1	Vame	Ser	ver	Issuance R	equirements
Superse	ded Templa	ates	Ede	insions	Security
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Purpose:	Signa	ture and s	martcard lo	gon	~
	De	lete revok	ed or expin	ed certificates (d	lo not archive)
	line	lude symm	etric algori	thms allowed by	the subject
	Arc	hive subje	ct's encryp	tion private key	
Allow priv	vate keyto	be exporte	ed		
Allow priv	vate key to with the sam	be exporte	ed		
Allow prin	vate key to with the sam natic renew cannot be	be exporte ne key val of smar created	ed t card certi	ficates, use the	existing key if a
Allow prin Renew v For autor new key Do the follow associated v	vate key to with the sam matic renew cannot be ving when t with this cer	be exporte ne key val of smar created the subject tificate is u	ed t card certi t is enrolled used:	ficates, use the	existing key if a private key
Allow prin Renew v For autor new key Do the follow associated v Enroll sul	vate key to with the sam matic renew cannot be ving when t with this cer bject without	be exporte ne key val of smar created the subject thicate is u ut requiring	ed t card certi t is enroller ised: ) any user i	ficates, use the d and when the j	existing key if a private key
Allow priv Renew v For autor new key Do the follow associated v Enroll sul @ Prompt til	vate key to with the sam matic renew cannot be wing when t with this cer bject withou he user dur	be exporte ne key val of smar created the subject tificate is u ut requiring ing enrollm	ed t card certi t is enrolled sed: ) any user i ent	ficates, use the d and when the input	existing key if a private key

- 7. Select the **Request Handling** tab change the following next to :-
  - Purpose: change: Signature and encryption to Signature and smartcard logon.
  - 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	erties of N	lew Templa	ite	×	
Subject Name	Server	leeuar	nce Requirements		
Superseded Template	es	Extensions	Security		
Compatibility General	Request Hand	fling Cryptogra	aphy Key Attesta	tion	
Provider Category:	Key Stora	ge Provider		~	
Algorithm name:	Algorithm name: RSA v				
Minimum key size:	2048				
Requests can use an     Requests must use or	ne of the follow	allable on the su wing providers:	bject's computer		
Providers:	What's Th	nis?			
Microsoft Software Ke	ay Storage Pro	wider			
Request hash:	SHA256			v	
🗌 Use altemate signatu	re format				
ОК	Cano	el App	Ny Help		

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

	Pro	perties	of New	Template	×	
Compatibility	General	Request	Handling	Cryptography	Key Attestation	
Supersec	ed Templa	stes	Ede	msions	Security	
Subject N	lame	Sen	ver	Issuance R	equirements	
Do not store certificates and requests in the CA database     Do not include revocation information in issued certificates						
[	ОК		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	Request	Handling	Crypto	graphy	Key	Attest	ation
Super	seded Template	s	Extensions		Security		Serv	er
	Subject Name			ssuanc	e Requir	ement	s	
Require	the following fo	r enrollme	nt:					
	certificate manag	ger approv	val					
🗹 This	number of auth	orized sig	natures:	1				
I.								
пу	ou require more	than one	sgnature, a	sutoenn	olment is	not al	lowed	
Pol	cy type required	in signatu	ure:					-
Ap	plication policy							~
App	lication policy:							
Ce	rtricate Heques	t Agent						~
13:51	Jance policies:				-			-
						Pi	od	
						Re	move	
					_			
Require	e the following fo	r reenrolin	nent:					
⊖ San	e criteria as for	enrollment	t					
Vali	d existing certific	ate						
	Allow key based	renewal	(7)					
	quires subject inf uest.	formation (	to be provid	led with	in the ce	rtificat	e	
Rea								
Rei reg *Contr	ol is disabled due	e to <u>comp</u>	atibility 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

Group or user names: Authenticated Users Commistrator (administrator@euc-livefire.com) Commin Admins (EUC-LIVEFIRE\Domain Admins) Comming Admins (EUC-LIVEFIRE\Enterprise Admins)	
Add Remove	
Parmiseione for Arthantinstad Lleare Allow Danie Select Users, Computers, Service Accounts, or Groups	×
Select this object type: Users, Groups, or Built in security principals From this location:	
	_
Object Types	×
Select the types of objects you want to find.	
Object types:	
Image: Service Accounts         Image: Service Accounts	
ОК С	ancel

- 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

Select Users, Computers, Service Accounts, or Group	ps	×
Select this object type:		
Users, Computers, Groups, or Built-in security principals		Object Types
From this location:		1
euc-livefire.com		Locations
Enter the object names to select (examples):		
TRUESSO		Check Names
Advanced	ОК	Cancel

- 12. In the Enter the object names area
  - Type Truesso
  - To the right select Check Names
  - Select OK

eneral	Compatibility	Request	t Handling	Cry	ptography	Key Attestatio
-	Subject Name			Issua	ance Requir	rements
Super	seded Template	S	Extensions		Security	Server
Group o	or user names:					
Ad Co En TF	lministrator (adm omain Admins (E iterprise Admins RUESSO (EUC-I	inistrator@ UC-LIVEF (EUC-LIV LIVEFIRE	₽euc-livefin FIRE\Doma /EFIRE\Ent /\TRUESS0	e.cor in Ad erpris 0\$)	n) dmins) se Admins)	
				A	dd	Remove
Parmier	ione for TRUES	50			Allow	Denv
Permiss	ions for TRUES	SO			Allow	Deny
Permiss Full C	ions for TRUES Control	SO			Allow	Deny
Permiss Full C Read	ions for TRUES Control 1	SO				Deny
Permiss Full C Read Write Enrol	ions for TRUES Control 1 1	SO				Deny
Permiss Full C Read Write Enrol Auto	ions for TRUES Control d e enroll	SO			Allow	Deny

- 13. For the **Permissions for TRUESSO** 
  - Select the Security tab
  - Select the **Read** and **Enroll checkboxes**
  - Select OK to close the TrueSSO Template Properties,

Console1	- [Console Root\Certification Au	thority (Local)\euc-livefire-TRUESSO-CA\Certi
File Action	n View Favorites Window Help	
(† 📫 🖄 🖥	T 🗟 🛃 👔	
Console Roo Certifica Certifica R R Is Is P P F F	ot tion Authority (Local) livefire-TRUESSO-CA levoked Certificates sued Certificates lending Requests ailed Requests iertificate. Tomolotes Manage New View New Window from Here New Taskpad View Refresh Export List Help	Name         Directory Email Replication         Domain Controller Authentication         EFS Recovery Agent         Basic EFS         Domain Controller         Web Server         Certificate Template to Issue         Subordinate Certification Authori         Administrator
Carble al R	Contract Translation on this Contract	
chable additiona	Certificate Tempiates on this Certificati	on Authority

14. Switch to the Certificate Authority Console

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

ote: If a certificate template that was re formation about this template has been I of the certificate templates in the orga or more information, see <u>Certificat</u>	cently created does not appear on this list, you may need to wait until replicated to all domain controllers. Inization may not be available to your CA. e Template Concepts.	
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	
	Server Authentication, Client Authentication	
🖳 VMware-SSL		

#### 15. In the Enable Certificate Templates window,

- Select your TrueSSO Template
- Select OK

Certificate Templates Console			
File Action View Help			
Certificate Templates (Controlce	Template Display Nar	me	Schema Version
	🗟 Directory Email Re	plication	2
	Domain Controller	r	1
	Real Domain Controller	Authentication	2
	EFS Recovery Ager	nt	1
	Enrollment Agent		1
	Enrollment Agent	(Computer)	1
	R Exchange Enr	Duplicate Template	
	Rechange Sign	All Tasks	>
	🕮 Exchange Use	Phil Turks	
	2 IPSec	Properties	
	IPSec (Offline	Help	
	Kerberos Auti		

- 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	Security
Templa	te display name:			
Enrollm	ent Agent (Compute	r)		
Minimur	n Supported CAs: V	Vindows 2000		
Templa	te name:			
Machin	eEnrollmentAgent			
Validity 2 Publ	years  years  lish certificate in Acti Do not automatically i Directory	Ve Directory reenroll if a duplic	penod: weeks ~	exists in Active
	OK	Cancel	Apply	Help

### 17. In the Enrollment Agent Properties window

• Select the Security tab

Enrollment Agent (Compute	r) Properties	:
General Request Handling Subject Nar Group or user names:	me Extensions Security	
Authenticated Users Comain Admins (EUC-LIVEFIRE\Do Enterprise Admins (EUC-LIVEFIRE\I TRUESSO (EUC-LIVEFIRE\TRUES	main Admins) Enterprise Admins) SSO\$)	
	Add Remove	
Permissions for TRUESSO	Allow Deny	
Full Control		
Read		
Write Enroll		
For special permissions or advanced setti Advanced.	ngs, click Advanced	
OK Cancel	Apply Help	

- 18. In the Enrollment Agent Properties window (Security Tab)
  - Select Add and add the TRUESSO Computer account
  - Ensure Read and Enroll permissions are selected

• Select **OK** to close the **Enrollment agent** properties

Console1 - [Console Root\Certification Authorit	ty (Local)\euc-livefire-TRUESSO-CA\Certificate
Console Root  Console Root  Certification Authority (Local)  Certification Authority (Local)  Revoked Certificates  Pending Requests  Failed Requests  Certificates  New  New  New  New  New  New  New  N	Name     Actions       Image: Enrollment Agent (Computer)     Certification       Image: TrueSSO Template     Directory Email Replication       Image: Directory Email Replication     More       Image: Domain Controller Authentication     EFS Recovery Agent       Image: Directory Email Replication     Efs Recovery Agent
Enable additional Certificate Templates on this Certification Au	thority

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

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

ote: If a certificate template that was recently cre formation about this template has been replicate I of the certificate templates in the organization n or more information, see <u>Certificate Templa</u>	eated does not appear on this list, you may need to wait until d to all domain controllers. may not be available to your CA. ate Concepts.	
Name	Intended Purpose	^
Authenticated Session	Client Authentication	
🖳 CA Exchange	Private Key Archival	
CEP Encryption	Certificate Request Agent	
Code Signing	Code Signing	
Cross Certification Authority	<ai></ai>	
Enrolment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrollment Agent (Offline request)	Certificate Request Agent	
Rechange Signature Only	Secure Email	

- 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 processing
  - On your existing TrueSSO server
    - Select and right-click the Start button
    - Select Command Prompt (Admin)



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



- 23. Configure CA to ignore offline CRL errors
  - certutil -setreg ca\CRLFlags +CRLF\_REVCHECK\_IGNORE\_OFFLINE



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



- 25. On the TrueSSO server desktop
  - Launch the **software** shortcut and open the **Horizon2106** folder.
  - Select the installer, VMware-Horizon-Connection-Server-x86\_64-8.3.0-18294467
  - Select Run



#### 26. On the **Welcome** window

Select Next

ġ	VMware Horizon Connection Server
	License Agreement Please read the following license agreement carefully.
	VMWARE END USER LICENSE AGREEMENT PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.
	IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS
-	< Back Next > Cancel

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

VMware Horizon Connection Server         X
Destination Folder Click Next 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
< Back Next > Cancel
< Back Next > Cancel

#### 28. On **Destination Folder** window

• Select Next

😾 VMware Horizon Connection Server	$\times$
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 Enrollment 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	

- 29. On the **Installation Options** window
  - Select Horizon Enrollment Server
  - Select Next

VMware Horizon Connection Serve	r	
Firewall Configuration		
Automatically configure the Windows F connections.	irewall to allow incoming TCP proto	lo
In order for Horizon Enrollment Server must be allowed through the local Win 32111 (View Framework channel).	r to operate on a network, specific dows Firewall service. The incomin	ncoming TCP port g TCP port is
Configure Windows Firev	vall automatically	
O Do not configure Window	vs Firewall	
	< Back Next >	Cancel

- 30. On Firewall configuration window
  - Select Next

🖁 VMware Horizon Connection Serve	er	>
Ready to Install the Program		
The wizard is ready to begin installatio	m.	
VMware Horizon Connection Server wi	Il be installed in:	
C:\Program Files\VMware\VMware Vie	ew\Server\	
Click Install to begin the installation or	Cancel to exit the wizard.	
	< Back Install	Cancel

- 31. On the **Ready to Install the Program** window
  - Select Install

😾 VMware Horizon Connec	tion Server	$\times$
<b>vm</b> ware <sup>,</sup>	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 Cance	(

- 32. On the Installer Completed Window
  - Select Finish

Settings File Explorer Search Run	
Shut down or sign out	
Desktop	
2 Run	×
Type the name of a program, folder, document, or resource, and Windows will open it for you.	or Internet
Open: mmc This task will be created with administrative	privileges.
OK Cancel	Browse
= > Ħ 🤗 🚍 🔤 📃	

#### 33. On the TrueSSO server

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



#### 34. In the **Console** window,

• Select File > Add/Remove Snap-in..

ailable snap-ins:			Selected snap-ins:	
nap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Demoure
Active Directory Sch	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor			
Active Directory Use	Microsoft Cor			Move Up
ActiveX Control	Microsoft Cor			
ADSI Edit	Microsoft Cor		Add	Move Down
Authorization Manager	Microsoft Cor		Nuu 2	
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor	~		Advanced
		-		

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

ertificates snap-in	
This snap-in will always manage certificate	as for:
O My user account	
O Service account	
Computer account	
	< Back Next > Cancel
	< Back Next > Cancel
lect Computer	< Back Next > Cancel
elect Computer	< Back Next > Cancel
elect Computer Select the computer you want this snap-in	< Back Next > Cancel to manage.
elect Computer Select the computer you want this snap-in This snap-in will always manage: (a) Local computer: the computer this	< Back Next > Cancel to manage. consele is a proise on)
elect 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)
Select Computer Select the computer you want this snap-in This snap-in will always manage: (a) Local computer: the computer this Another computer:	to manage.
Elect Computer Select the computer you want this snap-in This snap-in will always manage:  © Local computer: the computer this Another computer:  Another computer:  Allow the selected computer to be c only applies if you save the console	< Back
Select Computer Select the computer you want this snap-in This anap-in will always manage:  © Local computer: the computer this Another computer: Another computer: Allow the selected computer to be c only applies if you save the console	< Back
Select Computer Select the computer you want this snap-in This snap-in will always manage:	console is running on)  Browse  changed when launching from the command line. This .
Select Computer Select the computer you want this snap-in This snap-in will always manage: © Local computer: the computer this O Another computer: Allow the selected computer to be c only applies if you save the console	< Back     Next >     Cancel       to manage.
Select Computer Select the computer you want this snap-in This snap-in will always manage: © Local computer: the computer this O Another computer: C Another computer: C Allow the selected computer to be c only applies if you save the console	< Back
Select Computer Select the computer you want this snap-in This snap-in will always manage:	< Back
Select Computer Select the computer you want this snap-in This snap-in will always manage: © Local computer: the computer this. Another computer: Another computer: Allow the selected computer to be c only applies if you save the console	< Back
Select Computer Select the computer you want this snap-in This anap-in will always manage:	< Back

#### 36. On the **Certificates Snap-in**

Select Computer account radio button

- Select Next
- On the Select Computer (accept defaults ) and select Finish
- Select OK

🚡 (	Console1 - [Console Root\Ce	rtificates (Local Computer)\Personal\	Certif
🚡 File Action Vie	ew Favorites Window Help		
🗢 🌩 🖄 🗔 🕻	] 🙆 📄 🔽 📩		
Console Root	Issued To	Issued By	Expir
ک 🖓 Certificates (Lo ک 📫 Personal	cal C 😰 euc-livefire-TRUESSO-C/	A euc-livefire-CONTROLCENTER2	10/7/
Truste	All Tasks 🔸	Request New Certificate	
Enterg	View +	Import	
Intern Truste	New Window from Here	Advanced Operations	
Distribution of the second	New Taskpad View		
Third-	Refresh		
D Truste	Export List		
D Client	Help		
b Smart Card	Trus	]	
Trusted Dev	vices		
VMware Ho	prizor		
⊳ <u>≌</u> VMware Ho	rizor		

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

Certificate Enrollment
Before You Begin
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.
Before requesting a certificate, verify the following:
Your computer is connected to the network You have credentials that can be used to verify your right to obtain the certificate
Next Cancel

#### 38. On the **Certificate Enrollment > Before you Begin** window

Select Next



- 39. On the Select Certificate Enrollment Policy window
  - Select Next

ick Enroll.	uncates. Select the certificates you want	to request, and then
Active Directory Enrollment Policy	i) STATUS: Available	Details ¥
		Details +
El entendent (gent (compatel)	ap a minaar Aronaan	o cualis -
]Show all templates		

- 40. On the **Request Certificates** windows
  - Select the checkbox in front of Enrollment Agent (Computer)
  - Select Enroll

🗐 C	ertificate Enrollment		
	Certificate Installation Results		
	The following certificates have been enrol	led and installed on this computer.	
	Active Directory Enrollment Policy		
	C Enrollment Agent (Computer)	STATUS: Succeeded	Details 💙
			Finish

#### 41. On the Certificate Installation Results window,

- Ensure the enrollment was successful
- Select Finish.

Notepad++	Pin to Quick Copy Paster	Cut Copy path Paste shortcut Copy to $\star$ Copy
Remote	Clipboa	Remote Desktops
	📌 Quick access	Horizon.RDP
CA console.msc	➡ Downloads ★ ➡ Documents ★ ■ Pictures ★	SQL.RDP TrueSSO.RDP W10Cliept01 RDP
DNS	DesktopInfo	Sw10EXT01a.RDP Sw10Parent01a.RDP Sw10Parent01a.RDP
	TunnelApp	<b>h</b>

#### 42. On your **ControlCenter** server,

Open your Remote Desktops folder

• Launch the **Horizon.RDP** session



#### 43. On the **Horizon server** desktop

Select and open your Cert Console.mmc



#### 44. In the **Certificates** Console

• **Expand** the inventory

Browse down to VMware Horizon View Certificates > Certificates

Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name
47815b94-9cc2-4fd0-a7f5-30dc	47815b94-9cc2-4fd0	1/11/2030	<all></all>	vdm.ec
🛱 broker/cs1-pd1	broker/cs1-pd1	1/3/2021	<all></all>	ConnectionBroker
🕼 broker/cs1-pd1	broker/cs1-pd1	6/12/2020	<all></all>	ConnectionBroker
🛱 router/cs1-pd1	router/cs1-pd1	6/12/2020	<all></all>	MQRouter
🛱 router/cs1-pd1	router/cs1-pd1	1/3/2021	<all></all>	MQRouter
🛱 tunnel/cs1-pd1	tunnel/cs1-pd1	1/3/2021	<all></all>	Tunnel
🕼 tunnel/cs1-pd1	tunnel/cs1-pd1	6/12/2020	<all></all>	Tunnel

- 45. In the Certificates Console
  - Expand the console or scroll across the console and notice the guid based certificate has a friendly name of vdm.ec

SCS1-pd1 - cs1-pd1.euc-livefire.com - Remote Desktop Connection						
<b>E</b>	cert Consol	e - [Console Roo	t\Certificates (Local	Comp		
🚡 File Action View	🚟 File Action View Favorites Window Help					
🗢 🔿 🖄 🖬 🐇 🖣						
Console Root	Issued To	•	Issued By	Expirat		
⊿ 🙀 Certificates (Local	🙀 47815b <mark>04-0</mark>	cc2-4fd0->7f5-30dc	47815b94-9cc2-4fd0	1/11/2		
⊿ 🦳 Personal	🛱 broker/	Open	broker/cs1-pd1	1/3/20		
Certificates	🕼 broker/	All Tasks 🕨	Open	6/12/2		
Trusted Root C	Grouter/			6/12/2		
Enterprise Trus	Couter/	Cut	Export	1/3/20		
Intermediate C		Сору	tunnel/cs1-pd1	1/3/20		
Trusted Publisł		Delete	tunnel/cs1-pd1	6/12/2		
Untrusted Cert		Description				
Third-Party Ro		Properties				
Trusted People		Help				
Client Authent						
Deskto						
Certificate Enro						
b 📔 Smart Card Tru						

- 46. In the Certificates Console
  - Select your **GUID certificate** with the friendly name of **vdm.ec**.
  - Select and Right-Click the GUID certificate,
  - Select All Tasks
  - Select Export



#### 47. On the **Welcome** window

Select Next

÷	F Certificate Export Wizard	
	Export Private Key You can choose to export the private key with the certificate.	
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
	Do you want to export the private key with the certificate?	
	O Yes, export the private key	
	No, do not export the private key	
-		
	Next Cano	el
		_

#### 48. On the **Export Private Key** page

- Select the radio button next to No, do not export the private key
- Select Next

ort File Format Certificates can b	e exported in a variety of file formats.
Select the format	you want to use:
O DER enco	ded binary X.509 (.CER)
Base-64 e	ncoded X.509 (.CER)
O Cryptogra	phic Message Syntax Standard - PKCS #7 Certificates (.P78)
Includ	e all certificates in the certification path if possible
O Personal I	nformation Exchange - PKCS #12 (.PFX)
Indud	all certificates in the certification path if possible
Delete	the private key if the export is successful
Export	all extended properties
Enable	certificate privacy
<ul> <li>Microsoft</li> </ul>	Serialized Certificate Store (.SST)

#### 49. On the **Export File Format** window

- Select the radio button next to Base-64 encoded X.509
- Select Next

				>
🐓 Certificate Export Wizard				
Specify the name of the file y	ou want to export			
Eile name:				
Et \software \Horizon \enroll.	ter		Browse	
			k	
		1	Vext Canc	el

#### 50. In the **File to Export** window

In the File name area type the following E:\software\Horizon\enroll.cer

Select Next

	X
📀 🔗 Certificate Export Wizard	
Completing the Certificate Ex	xport Wizard
You have successfully completed the Certification	te Export wizard.
You have specified the following settings:	
File Name	C:\software\Horizon7\enroll.cer
Include all certificates in the certification pat	NO h No
File Format	Base64 Encoded X.509 (*.cer)
	Finish Cancel
Certificate Export Wizard	
The export was successful.	
ОК	

- 51. On the **Completing the Certificate Export Wizard** window
  - Select Finish.
  - When prompted that The export was successful,
    - Select OK



- 52. On your **ControlCenter** server desktop
  - Switch from your Horizon RDP session to your TrueSSO RDP session

<ul> <li>Certificates (Local</li> <li>Personal</li> </ul>	l Computer)	
Certificate	5	
> 🧮 Trusted Root	Certification Authorities	
> 🧮 Enterprise Tru	ist	
> 📔 Intermediate	Eind Certificates	
> Trusted Public	st This certificates	
> Intrusted Ce	rt All Tasks	> Find Certificates
> 📔 Third-Party R	0	
> Trusted Peop	le View	> Import
> Client Auther	nt New Window from Here	
> 🧾 Preview Build	F	
> i Test Roots	New Taskpad View	
> 🦳 Remote Desk	to Refresh	
> Smart Card T	Tu Evenent List	
> Invited Device	e Export List	
VMware Hori	ze Help	
> 📔 VMware Hori	zon view Enrollment Server Trusted	1 KOO
> 🦳 Windows Live	e ID Token Issuer	
> 📔 WindowsServ	erUpdateServices	
E		

#### 53. On your TRUESSO server

- Open 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

<ul> <li>&amp; Certificate Import Wizard</li> </ul>	
Welcome to the Certificate	Import Wizard
This wizard helps you copy certificates, cer lists from your disk to a certificate store.	tificate trust lists, and certificate revocation
A certificate, which is issued by a certificat and contains information used to protect d connections. A certificate store is the syste	ion authority, is a confirmation of your identity ata or to establish secure network em area where certificates are kept.
Store Location	
O Current User	
() Local Machine	
To continue, dick Next.	
	Next Cancel

#### 54. On the **Welcome** window

Select Next

Dpen
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ « software » Horizon » v $\circlearrowright$
Organize 🔻 New folder
And Andrewski access  Desktop  Downloads  D
File name: \\horizon\software\Horizon\enroll.cer .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 Cancel

#### 55. In the File to import window

- Type the following \\horizon\software\Horizon\enroll.cer
- Select Next

-
🛞 🖻 Certificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can autorestically select a contribute store, or you can specify a location for the contribute. Autoresticate of the contribute to the set which and the type of contribute ® Recar all contributes in the following store
Certificate store: White Horizon View Enrolment Server Trusted Roots Browde
Net Cancel
Completing the Certificate Import Wizard The certificate all periods of truth. This have specified the discovery struture. This have specified the discovery struture. This have been been been been been been been be
۲
Finish Cancel
Certificate Import Wizard
The import was successful.
ОК

56. 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



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



- 58. On your **ControlCenter** server,
  - Switch to your **Chrome browser**,

- Open a new tab,
- Using your custom Workspace ONE Acces Url,
  - Log in as System admin with your custom credentials
- Select the Catalog tab > Virtual Apps Collection

8 w	orkspace ONE™ Ac	cess
Dashboar	d 👻 Users & Group	s Catalog 👻
	Virtual App	S Collecti
	• Horizon	Horizon

- 59. In the Virtual Apps Collection window
  - Select the radio button next Horizon
  - Select **EDIT** next to **NEW**

Edit Horizon Collection	
1 Connector 2 Pod and Federation	Add or modify pods. If a pod has multiple Horizon C information for any of the Horizon Connection Serve
3 Configuration 4 Summary	Horizon Connection Server         Username         Small           Horizon.euc-livefire.com         administrator         Disa
	ADD A POD

#### 60. In the Edit Horizon Collection window,

- Select 2 Pod and Federation,
  - To the right, select horizon.euc-livefire.com

	Horizon Connection Server *(			
	Horizon.euc-livefire.com			
	Username * ()			
	administrator			
	Password * ()			
	Smart Card Authentication ()			
	Disabled			
	True SSO ①			
	C Enabled			
	Sync Local Assignments ①			
	Enabled			
				CANCEL
	CANCEL BACK	NEXT		
Pod				
Horizon Connection Server	Username	Smart Card Authentication	True SSO	Sync Local Assignments
Horizon.euc-livefire.com	administrator	Disabled	Enabled	Enabled
Cloud Pod Architecture (C	PA)			
Disablad				

#### 61. In the **Edit Pod** window

• Under True SSO, change the toggle from Disabled to Enabled

• Select SAVE , select NEXT, select NEXT, select SAVE

⊿ 📲 VMware, Inc.			
VMware	Drivers		
⊳- <mark>∭</mark> VMware	Tools		
	Collapse		
	New	Key	
	Find	Ney	
Þ P	Find	Stilling value	·
- VMw	Delete	Binary Value	
⊳ - 🌺 Wow643	Rename	DWORD (32-b	it) Value
SYSTEM	Export	QWORD (64-b	it) Value
HKEY_USERS	Permissions	Multi-String V	alue
▶ IKEY_CURRENT		Expandable St	ring Value
Policies			,
Register	edApplications		
⊿ - 🔐 VMware	, Inc.		
	vare Drivers		
	vare VDM		
	Authenticate		
	.00		
	Node Manager		
▶ - 🌆 P	Plugins		
E	nrollment Service		
- WMw	vare VGAuth		
⊳ - 퉲 Wow643	32Node		
▷ ↓ SYSTEM			
HKEY_USERS			

- 62. From the **ControlCenter** server, switch back to your **TrueSSO.RDP session** 
  - 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

(	ugina -	
- 🔒 En	rollement Service	
VMwa	Expand	
Vow6432	New +	Key
SERS	Find	String Value
IDDEAIT	Delete	Dinary value
CAL_M/	Rename	DWORD (32-bit) Value
	Evnort	QWORD (64-bit) Value
	aport	
📑 Re	gistry Editor	
File E	dit View Favorites Help	
Compu	ter\HKEY_LOCAL_MACHINE\SOF	TWARE\VMware, Inc.\VMware VDM\
	> Microsoft	^ Name
	> Mozilla	ab (Default)
	> mozilla.org	ab PreferLocalCa
	Notepad++	
	> ODBC	
	Destroop	
	Policier	
	RegisteredApplications	
	Setup	
	VMware, Inc.	
	> 📙 VMware Tools	
	VMware VDM	
	- Authenticate	
	- Log	
	Node Manager	
	> Plugins	
	VMware VGAuth	
^	Name	Type
	ab (Default)	REG_SZ
	ab Pre Modify	G_SZ
	Modify Binary Data	
	Delete	
	Delete	
	Kename	
549.0		~
colt Str	ing	~
Value n	ame:	
PreferL	ocalCa	
Value	ata-	
vaue o	e.e.	
1		
	[	OK Cancel

- 63. 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
      - type the name **PreferLocalCa**
    - Right-click the PreferLocalCa String value and
      - Select Modify
        - In the Value data: field enter 1
    - Select **OK** to close the window.
    - Click to **close RegEdit**



64. On your **ControlCenter** server

- Switch to your **Horizon.**RDP session
- NOTE. At this point, to get the maximum benefit with the following steps, it would be advisable to go Full Screen with your RDP session.



- 65. On your Horizon server
  - Select and right-click the **Start** button
  - Select Command Prompt (Admin)
  - Maximise your Command Prompt window



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



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

The enrollment server is added to the global list.

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMwarel! --
truesso --environment --add --enrollmentServer TrueSSO.euc-livefire.com
```



- 68. Wait 1 min before doing the next command
  - 1. If one executes too quick, you will get the following error message
    - 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 TrueSSO.euc-livefire.com --domain euc-
livefire.com
```



69. 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 VMware1! --
truesso --create --connector --domain euc-livefire.com --template TrueSSOTemplate --
primaryEnrollmentServer truesso.euc-livefire.com --certificateServer euc-livefire-
TRUESSO-CA --mode enabled
```



70. 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



71. 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! --

For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to Workspace ONE Access. 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 Workspace ONE Access

73. On your ControlCenter server

• Minimise your Horizon.RDP Session

## Part 4: Testing to see if TrueSSO works



- 1. On your ControlCenter server,
  - Switch your Remote Desktops session to W10EXT01a.RDP.



- 2. On your W10EXT01a desktop,
  - Open your browser and type custom Workspace ONE Ascess URL

Select a certificate Select a certificate to a	uthenticate you	rself to cas.vidmpreview.com	n:443	
Subject		lssuer	Serial	
Mark		markusheinraadgmail	0187D1	

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

	Favorites	Apps	People	For You Support	
	Q Searc	h Apps			
			New Ap	ops All Apps C	Categories 🗸
New	. 4				
New	и Apps				
	0			2	-
	Calculator	Ir	nternet Explorer	Paint	W10INST

- 4. In the **Apps** tab
  - Select W10INST



- 5. In the **All Apps** area,
  - Observer your Horizon Desktop session
  - Possibly launch a RDSH session from your Workspace ONE Access console
  - This concludes this lab as

## Acknowledgements

A huge thank you Spas Kaloferov from Livefire and Rahul Jha from GSS in assisting me Troubleshoot this lab when authoring the first version

## About the Author

About the Author Reinhart Nel

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

For any questions please email Reinhart RACE-Livefire-EUC@vmware.com