Windows 10 Certificate Single Sign On using an AirWatch Certificate Authority

In this lab you will be deploying a certificate to an enrolled Windows 10 virtual machine. This certificate will be generated by the built-in CA in Workspace ONE UEM.

We will later configure Workspace ONE Access to trust certificates issues by UEM and configure the Certificate (Cloud Deployment) authentication adapter.

Finally we will test everything on a Windows 10 Machine to ensure we are able to have a seamless authentication experience.

Part 1: WorkspaceOne UEM - Certificate Profile

- 1
- Open Chrome on your ControlCenter2 jumpbox and navigate to https://cnlivefire.awmdm.com Authenticate using your e-mail address and unique password
 - 1. Navigate to Groups & Settings > All Settings > Enterprise Integration > VMware Identity Manager> Configuration
 - 2. Under Certificate select **ENABLE** (this should be enabled from a previous lab)
 - 3. Under Certificate next to Issuer Certificate select EXPORT



- 2. WorkspaceOne UEM Certificate Profile continued...
- Then navigate to Devices > Profiles & Resources > Profiles > ADD > Add Profile > Windows > Windows Desktop > User Profile Give it a name : W10 - SCEP - SSO.
- 2. Select your **Smart Group** with the **World icon** for the Smart Group
- 3. Select the **SCEP** payload on the left hand navigation panel.
- 4. Select **CONFIGURE**
- 5. Set the following
 - Credential Source: AirWatch Certificate Authority
 - Certificate Template: Certificate (Cloud Deployment)
 - Issuer: LiveFire
 - Click SAVE AND PUBLISH
- 6. In the **Device Assignment** notice your device in the list of device being added. Then click **PUBLISH**





General	
Name *	W10 - SCEP - SSO
Version	1
Description	
Deployment	Managed
Assignment Type	Auto ~
Allow Removal	Always
Managed By	mintobrunella@outlook.com
Smart Groups	mintobrunella@outlook.com (mintobru nella@outlook.com)
	Start typing to add a group
Exclusions	NO YES

Add a New Windows	Desktop Profile				
General					
	SCEP				
U Credentials	Credential Source	AirWatch Certificate Authority	-		
Windows Hello			_		
Single App Mode	Certificate Authority *	AirWatch Certificate Authority	r		
🔏 Web Clips	Certificate Template *	Certificate (Cloud Deployment)	ć.		
S3 Exchange ActiveSync	lesuer *	LineFiel			
↔ SCEP ①	ISSUEL	uverie	_		
Si Exchange Web Services					
>> Custom Settings					
					(
				SAVE AND PUBLISH	CAN

			As
Assignment Status	Friendly Name	User	Platform.
Unchanged	user35CRSJ Desktop Wind	user35CRSJ	Windows

Part 2: Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication

1. Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication

- In this next section, we will configure Workspace ONE Access Certificate Auth Adaptor to trust the certificates being presented by the devices.
 - 1. On your **ControlCenter** server, use your **unique Workspace ONE Access** server and authenticate to the local directory using administrator account and password.
 - 2. Under Identity & Access Management > Manage select Authentication Methods
 - 3. Click on the **Pencil** to Configure the **Certificate (Cloud Deployment)** authentication method.
 - 4. Select the **checkbox Enable Certificate Adapter** and click **Select File** to **upload the Certificate (VidmAirWatchRootCertificate.cer**) you downloaded above in the UEM console.
 - 5. On the **Update Auth Adapter** window select **OK**
 - 6. Leave everything else in here as default and click **Save**.
 - Now navigate Identity Providers under Identity & Access Management click on Builtin
 - 8. Navigate to the **Authentication Methods** area and select the **check box** next to **Certificate (Cloud Deployment)** and select **Save** at the bottom of the page.

8 Worl	kspa	ce ONE	E™ Acc	255				
Dashboard	•	Users &	Groups	Catalog	•	Identity & Acc	ess Management	Roles
Directories	lder	ntity Provi	ders	Password R	lecov	ery Assistant	Authentication I	Methods
			Auther Importan sure you	tication I t: When you update the a	disab	nods for Bui ble an authentica s policy rules to	It-in Identity P ation method, the a select another auth	trovider:
			Auther	tication Met	hods		Configure	
			Airwat	ch External /	Acces	ss Token	ø	
			Passw	ord (AirWatc	h Co	nnector)	ø	
			Device	Compliance	e (wit	h AirWatch)	ø	
			VMwa	re Verify			Ø	
			Mobile	SSO (for iO	S)		ø	
			Passw	ord (Local D	irecto	ory)	ø	
			Mobile	SSO (for Ar	ndroid	l)	ø	
			Certific	ate (Cloud I	Deplo	yment)	Ø	

Where making, S&L term mak	
Rot and intermediate C A certificates Viou can upload multiple DER and PEM root and intermediate CA certificates including concatenat Uploaded CA Certificates CN=mintobrunellaoutlookcom (4EEBE1DAAE597AC58B32F597EE3C6C0E0A6F09840A649A030E7A33CFB4E61968) Upn subject Select the search order for locating the user identifier within the certificate. upn: UserPrincipalNam Yalidate UPN Format Validate the format of the UserPrincipalName field Request Timeout 0 Timeout in seconds to wait for a response. A value of zero will wait indefinitely. Certificate Policies Accented	e configured
You can upload multiple DER and PEM root and intermediate CA certificates including concatenal Uploaded CA Certificates CN=mintobrunellaoutlookcom (4BEBE1DAAE597AC58B32F597EE3C6C0E0A6F09840A649A030E7A33CFB4E61968) * Upin subject • Order Select the search order for locating the user identifier within the certificate. upn: UserPrincipalNam the Subject Alternative Name; subject: U Validate UPN Format • Request Timeout • Image: Certificate Policies • Accented •	
Uploaded CA Certificate CN=mintobrunellaoutlookcom (4BEBE1DAAE597AC58B32F597EE3C6C0E0A6F09840A649A030E7A33CFB4E61968) Implice User Identifier Search upilisubject Implice Order Salect the search order for locating the user identifier within the certificate, upn: UserPrincipalNam the Subject Alternative Name; subject: UserPrincipalNam field Validate UPN Format Implice Implice Validate the format of the UserPrincipalName field Implice Implice Request Timeout Implice Implice Implice Certificate Policies Implice Implice Implice Accented Implice Implice Implice Implice	ted PEM file
(4BEBE1DAAE597AC58B32F597EE3C6C0E0A6F09840A649A030E7A33CFB4E61968) User Identifier Search Order Upn subject Select the search order for locating the user identifier within the certificate. upn: UserPrincipalNan the Subject Alternative Name; email: Email address from the Subject Alternative Name; subject: U Validate UPN Format Validate UPN Format Image: Comparison of the UserPrincipalName field Request Timeout 0 Timeout in seconds to wait for a response. A value of zero will wait indefinitely. Certificate Policies Accepted	
User Identifier Search Order Upp subject Order Select the search order for locating the user identifier within the certificate. upp: UserPrincipalNan the Subject Alternative Name; email: Email address from the Subject Alternative Name; subject: U Validate UPN Format Validate the format of the UserPrincipalName field Request Timeout 0 Timeout in seconds to wait for a response. A value of zero will wait indefinitely. Certificate Policies Accepted Cancel	1
Salect the search order for locating the user identifier within the certificate. upn: UserPrincipalNan the Subject Alternative Name; email: Email address from the Subject Alternative Name; subject: U Validate UPN Format Validate the format of the UserPrincipalName field Request Timeout 0 Timeout in seconds to wait for a response. A value of zero will wait indefinitely. Certificate Policies Accepted	
Validate UPN Format Validate the format of the UserPrincipalName field Validate the format of the UserPrincipalName field Request Timeout	ne value fror JID value fro
Validate the format of the UserPrincipalName field Request Timeout	
Request Timeout 0 Timeout in seconds to wait for a response. A value of zero will wait indefinitely. Certificate Policies Accepted	
Certificate Policies Accepted Cancel	
Certificate Policies	
Accepted Cancel	
Cancel	
	Save
Update Auth Adapter	
Please click OK to confirm and upload file.	

ubband a lines f	Course Catalan a Lun	No. 2 Annual Management	Relas	
ctories	iders Password Recovery A	sistant Authentication Me	ethods Policies	
	Identity Providers (3)			
	Identity Provider Name	Auth Methods	Directory	Ne
	System Identity Provider	Password (Local Directory)	System Directory	AL
	Bult-In	Password (Local Directory) Certificate (Cloud Deployment) Mobile SSO (for IOS) Password (cloud deployment) Device Compliance (with AirWatch)	LiveFire Sync1	AL
Casek to MP Like	Identity Provider Name	Bult-in		
	Users	Select which users can authenticate us System Directory VLVeFire Sync1	ing this IdP, Choose from the availabl	e directories fror
	Network	Select which networks this IdP can be before.	accessed from. Choose from the avai	lable network ra
Delete IdP		ALL DANGES		
	Authentication Methods	Select which authentication methods t	he lot will use to authenticate users.	
		Device Compliance (with AirWatch		nocatoon Metho
		Mobile SSO (for iOS)	······································	
		Password (Local Directory)	~	
		Certificate (Cloud Deployment)	 Image: A start of the start of	
	Connector(s)	WS1-Connector1 (ws1-connecto Add a Connector You car connect connector Importa authent	seuc-livetire.com X swiect additional connectors for high for activation code from the Add a Co to, and then select the connector for ext: For high availability, each connect ication method configuration.	availability (HA), nnector page an this IdP. or must have the
	Connector Authentication Methods	Authentication Methods Password (cloud deployment)	Associate Authenticat	ion Method
	KDC Certificate Export	Download Certificate Export the KDC server root certificate f	for use in a Mobile Device Manageme	nt profile.
		Save Cancel		

2.

- Configuring Workspace ONE Access Certificate (Cloud Deployment)
 Authentication....continued
 - 1. Navigate to **Policies** under **Identity & Access Management** then click on the **SSO** policy.
 - 2. Select Edit
 - 3. Next to **Configuration** select **+ADD POLICY RULE.**
 - 4. In the Add Policy Rule window add the following, next to : -
 - 'and user accessing content from' to Select Windows 10 from the drop down
 - then the user may authenticate using* change to Certificate (Cloud Deployment)
 - "if the preceding method fails or is not applicable, then" change Select failback method... to Password (Cloud Deployment)
 - 5. Select **SAVE**
 - 6. Select +ADD POLICY RULE.
 - 7. In the Add Policy Rule window add the following, next to : -
 - 'and user accessing content from' select Web Browser from the drop down
 - then the user may authenticate using* change to Certificate (Cloud Deployment)
 - "if the preceding method fails or is not applicable, then" change Select failback method... to Password (Cloud Deployment)
 - 8. Select **SAVE**,
 - 9. Next to **ALL RANGES for Windows 10** on the left select the **6 DOTS** and drag to the top
 - 10. Select **NEXT**, select **SAVE**.

ectation Identity Providers Passward Re	covery Andia					
ADD POLICY EDIT DEL	ETE EC					
PulsyName						
O defect_access_petity_set						
• sso	2					
: ALL K IUS						
: ALL R Web Br	b					
ADD POLICY RULE						
company Edit Po	icy Rule					
If a sale"x network range is "	×085 0					
and user accessing contant from * Windo						
and user belongs to group(c)	of droups					
Rule ap	lies to all users if no group(i) selected.					
Then perform this action Autoer	can unip					
then the user may authenticate using * Centre	de (Claud Deployment) - © ®					
If the preceding method fails or is not	e soue deployment					
applicable, then						
6 a	D FALLRECK MITHOD					
Network Range Devi	e Type					
ALL DANCES	new 10					
T ALL NAVOES AND	<i>na</i>					
ALL RANGES IOS						
ADD POLICY RULE						
JOATTON .	Add Policy Rule					
If a user's network range is	* ALIONOIS					
and user accessing content from	We have . 0					
and user belongs to group	0 Q.Select Orean. D					
	Rule applies to all users if no group(c) selected.					
Then perform this acti	* Autorologicality 0					
then the user may authenticate using	Centificate (Dead Dealeyment)					
Fite preceding method fails or is not applicable, then Password (cloud deployment) D						
	R ADD FALLBACK MITHOD					
opproximiting to the second	CANCE, SHE					
Network Range Device Typ	Authentication Re-authentic					
Windows 10	Certificate (Cloud Depl. B Hour(s)					
ALL RANGES Android	Mobile SSO (for Androi 8 Hour(s)					
ALL RANGES IOS	Hoble SSO (for IOS)+1 B Hour(s)					
ALL RANGES Web Brows	r Certificate (Cloud Depl. 8 Hour(s)					

Part 3: Windows 10 Single Sign On using Certificates

- Now that the administrative elements are in place we will now test the authentication flow from our Windows 10 VM.
 - 1. On the **ControlCenter2** VM on the desktop you will find the **Remote Desktop** folder. In this folder click double click on **w10client01.RDP**
 - 2. Inside the Windows 10 Virtual Machine **open Microsoft Edge** from the desktop and type **OFFICE.COM** in the address bar
 - 3. In the Office.com page select Sign In
 - 4. In the **Sign in** window, type your **email address**. eg user35crsj@sanjose35.euclivefire.com.
 - 5. Select Next
 - 6. Notice now that you are being re-directed to **cas.vidmpreview.com** in the URL field and you are prompted for a **Certificate.**
 - 7. Click **OK** on the pop-up for your certificate and notice your are straight into your WorkspaceOne bookmarks Tab.
 - 8. Now click on any one of your **Office365 deeplinks** and notice your are authenticated without further credentials. If you get prompted to "Stay Signed in?" simply click **No**.
 - 9. You are now authenticated to your O365 environment using a certificate based authentication method.

This completes this lab.

