Certificate Based Authentication 2.0

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 issued by UEM and configure the Certificate (Cloud Deployment) authentication adapter.

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

Extra Material is optional and will show you how to suppress the pop-up users see in Chrome and to automate this using UEM.

Part 1: WorkspaceOne UEM - Certificate Profile



1. On your **ControlCenter** jumpbox

- 1. Open Google Chrome
- 2. Navigate to https://cn-livefire.awmdm.com
- 3. Authenticate using :
 - Username your **e-mail address**
 - Password VMware1! (if you didn't change it from the default)

Settings	Livefire	
~ System	System > Enterprise Integration	on
Getting Started		
Branding	Workspace ONE Ac	cess 🕐
 Enterprise Integration 		
Enterprise Integration Services		
Certificate Authorities	Server	
Content Gateway	Establish trust between users, devi	ces and the hybrid cloud for a seamless user experience and powerful conditional access to a unified app ca
Cloud Connector	apps.	
Directory Services	URL	https://access.euc-livefire.com
Email (SMTP)		
VMware Tunnel	Admin Username	admin
VMware Tunnel Proxy		
> Peer Distribution	Active Directory Basic	ENABLED DISABLED
Third-Party Proxies	Ranie Henry Come	
SMS	basic oser sync	ENABLE
Pull Service Installers		
Syslog	Lise this Action Dutters to undate	Washington ONE Assess LIEM configuration to use Auto Connected LIEM ADI Key
Workspace ONE Access	Use this Action Button to update	Workspace ONE Access-DEM configuration to use Auto-Generated DEM APT Key
Configuration	USE AUTOGENERATED API	KEY
Access Management		
 Security 	Contificato	
Help	ceremente	
> Localization	Enable Workspace ONE UEM certifi trust with Workspace ONE Access a	cate provisioning for use with Workspace ONE Access and Mobile SSO. Export the issuer certificate on this p withentication adapters
Terms of Use		
S/MIME	Certificate Provisioning	ENABLE
> Advanced		
> Devices & Users		
> Content		
> Apps		
> Fmail		

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

© Settings	Global / Livefire 🗸	×
SMS Pull Service Installers Syslog Remote Management Vorkspace ONE Access Configuration Access Management	Use this Action Button to update Workspace ONE Access-UEM configuration to use Auto- Generated UEM API Key USE AUTOGENERATED API KEY	^
 Security Help Localization 	Certificate Certificate Certificate Certificate Certificate Certificate Provisioning Certificate Certi	-

- 3. In the Enterprise Integration > Workspace ONE Acces page
 - Scroll down to find the Certificate section

• Under **Certificate** select **ENABLE** (if not already enabled)

Certificate	
Enable Workspace ON Mobile SSO. Export the Workspace ONE Access	E UEM certificate provisioning for use with Workspace ONE Acc issuer certificate on this page so that you can establish trust v s authentication adapters.
Certificate	Type Pfx
	Valid Fro 5/16/2020
	Valid To 5/18/2040
	Thumbp 86C33DC6D225BD01B536AD684BA191AD234E
Issuer Certificate	EXPORT
S/MIME	
> Advanced	*
This type of file can want to keep Vidm. On Server	harm your computer. Do you Keep Discard AirWatchRootcer anyway? Keep Discard
VidmAirWatchRoot	cer ^
	$\overline{\mathbf{x}}$

4. In the Enterprise Integration > Workspace ONE Acces page

- In the **Certificates** section
 - Select EXPORT
 - When prompted, select Keep
 - Note this will download a .cer file (VidmAirWatchRootCertificate.cer)
 - Close the **Settings w**indow in the top right-corner, by selecting **x**
 - **NOTE:** You may have downloaded this certificate in a prior lab you can leverage this certificate.

🖏 Work	space ONE UEM		Global / Livefire 🗸	Add 🗸	Q	Ļ	☆ ⑦	Administrato	r 🗸
GETTING STARTED	Dashboard		Devices 🕻 Pro	files & Resources					
MONITOR	List View Device Updates		Profiles						Â
	Lifecycle Profiles & Resources	> ~	Filters >	> ADD V LAY	оит 🗸) C	EXPORT	Search List	Inst
ති ACCOUNTS	Profiles			Upload Profile	-	0	21		
APPS &	Baselines Resources			Batch Import	ecords	Found			
BOOKS	Batch Status								
	Compliance Policies	>							

- 5. In the Workspace ONE UEM admin console
 - Navigate to Devices > Profiles & Resources > Profiles > ADD > Add Profile

Add Profile			
Select a platform to start:			
205	i		
Android	A		
windows	Anor		
Windows Phone Windows Desktop Windows 7			
	/		
Select Device Type			
Windows Desiston	Windows 7		
indons beaup			
Select Context			
	Ch		
User Profile	Device Profile		
📲 Add a New Window	s Desktop Profile		
Find Payload			
General	General		
VPN	Name *	W10 - SCEP - SSO	
Credentials			
Windows Hello	version	1	
Single App Mode	Description		
Web Clips	Deployment	Managed ~	
Exchange ActiveSync		-	

- 6. In the Add Profile window
 - Select Windows > Windows Desktop > User Profile
 - Under **General**
 - Next to Name: type W10 SCEP SSO .

Deployment	Managed	×
Assignment Type	Auto	*
Allow Removal	Always	~
Managed By	ManfredVogal@gmail.com	
Smart Groups	ManfredVogal@gmail.com (ManfredVo gal@gmail.com)	×
L	Start typing to add a group	۹
Exclusions	NO YES	

7. In the Add a New Windows Desktop Profile

- In the General tab,
 - Scroll down to **Smart Groups**
 - Select you **Organization Group** (This should be your e-mail address) with the **world icon** next to it.

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

8. In the Add a New Windows Desktop Profile

- In the LEFT MENU, navigate to the **SCEP**
- Select CONFIGURE

CEP			
Credential Source	AirWatch Certificate Authority	~	
Certificate Authority *	AirWatch Certificate Authority	×	
Certificate Template *	Certificate (Cloud Deployment)	~	
Key Location	Software	¥	

9. In the Add a New Windows Desktop Profile

- Under **SCEP**, Set the following, next to:
 - Credential Source: AirWatch Certificate Authority
 - Certificate Template: Certificate (Cloud Deployment)
 - Key Location: Software
 - Select **SAVE AND PUBLISH** at the bottom right of the window

			Assign	ment Status All	٣	Filter Grid	
ssignment Status	Friendly Name	User	Platform/OS/Model	Phone Number	Organization	Group	
Added Science	MajonneDuponte Desktop 1 eeATTEND	Mark	Windows Desktop / Windows 10 (10.0.1836	-	MajonneDup	onte	
Added	MajonneDuponte VMware7,1 5 e5W10E.	Mark	Windows Desktop / Windows 10 (10.0.1836		MajonneDup	onte	
ems 1-2 of 2						Page Size: 20	

- 10. On the View Device Assignment page
 - Confirm your device is showing
 - Select PUBLISH

Troubleshooting Tips

Should the certificate not get deployed please follow the steps below to force the certificate to be pushed.



 We have observed in certain scenarios the device is reporting WNS STATUS: DISCONNECTED when it should be WNS STATUS: CONNECTED. This can lead to a delay in the client certificate being deployed to the device. In the communication flow WNS (Windows Notification Services) are responsible for triggering a check in between the OMA-DM client and the Workspace ONE UEM Server. Network constraints can sometimes play a role and we recommend seeing Microsoft's guidelines: <u>https://via.vmw.com/w10WNS</u>

De	evices	> L	ist View								< 2 / 4 Recent I) List
Ν	/lar	nfre	dVogal@	@gmail.	com V	′		QUERY	SEND	LOCK	MORE ACTIONS	~
VN	/lware	e Virtual	Platform	10.0.18363	Ownershij	p: Co						
Sum	mary	, C	ompliance	Profiles	Baseline	s Apps	Updates	Content	Мо	re 🗸		
(i La	st Scan:										
								C	EXPOR	r 🗸 Is	Search List	
		Status	Profile Det	tails		Organizatio	n Group	Configu	ration Typ	pe A	Assignment Type	
	С	0	W10 - Chro	ome - ADMX		ManfredVog	al@gmail.com	Device		A	utomatic	
	С	0	W10 - Chro	ome - AutoSel	ect	ManfredVog	al@gmail.com	User		A	utomatic	
(Pendir	W10 - SCE	P- SSO		ManfredVog	al@gmail.com	User		A	utomatic	

- In the WorkspaceONE UEM Console navigate to Device > List View > Select the unique VM you are working on (Previously W10Client01).
 - Select the **Profiles** tab.
 - If you are getting a **green** tick the certificate ha been deployed and you can move to part 2 of the lab.
 - However if you are getting a **grey** tick it means the profile is pending install.



3. Navigate to the Windows 10 VM and type **access work** into the search and click the **Access work or School System settings**

Settings	- 🗆 ×
命 Home	Access work or school
Find a setting	Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device,
Accounts	such as which settings you can change. For specific info about this, ask them.
RE Your info	+ Connect
Email & accounts	Connected to Workspace ONE MDM
🔍 Sign-in options	Connected by mark@euc-livefire.com
Access work or school	Info Disconnect
A, Other users	Connected to EUC-LIVEFIRE AD domain
C Sync your settings	euchvenie.com

- 4. Click on **Connected to Workspace ONE MDM**
 - Click on Info

← Settings			
Managed by Workspace Management Server Address: https://ds1605.awmdm.com/DeviceServices/Dm.svc/tr kvbdf2/2C1C3A5D21A664F8811512A6C31562A Exchange 10: DE012F6CD6888D0543D47E5D65663510	ONE ^{ken/}		
Device sync status			
Syncing keeps security policies, network profiles, and applications up to date. Last Attempted Sync: The sync was successful Syn2021 S:31:00 AM	nanaged		
Advanced Diagnostic Report			
Your IT or support person may want additional inform troubleshooting. Create report Q Get help	ation to help with		
ManfredVogal@gmail.com D	0	QUERY SEND LOG	CK MORE ACTIONS
VMware7,1 10.0.19042 Ownership: Corporate - De Summary Compliance Profiles Baselines	Apps Updates	Content More 🗸	
() Last Scan:			
		C EXPORT V	Search List
Status Profile Details Orga	ization Group	Configuration Type	Assignment Type
O W10 - Chrome - ADMX Manfr	edVogal@gmail.com	Device	Automatic
O W10 - Chrome - AutoSelect Manfr	edVogal@gmail.com	User	Automatic
O W10 - SCEP- SSO Manfr	edVogal@gmail.com	User	Automatic

- 5. Scroll to the bottom of the page and click Sync
 - This should trigger a manual check in with **WorkspaceONE UEM** and trigger the deployment of the certificate. Allow for a few minutes while this process takes place.
 - Double check in the WorkspaceONE UEM console to make sure that there is now a Green tick next to the W10 - SCEP - SSO profile.



6. Should you require further troubleshooting check this registry key for installed profiles -

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseResourceManager\ Tracked

You can also check the Certificate store in MMC under **Personal** > **Certificates** to ensure you have the client certificate installed.

Part 2 : Configure Workspace ONE Access



- 1. On your **ControlCenter** server
 - In the Chrome browser
 - Navigate to your unique Workspace ONE Access tenant.
 - Authenticate using System Domain
 - username: Administrator
 - password: VMware1!
 - In the Web Intelligent Hub
 - In the top right corner, select the TA Icon
 - In the Tenant Admin interface
 - Select Workspace ONE Access Console

Dashboard	-	Users & Groups	Catalog 🚽	Identity & A	ccess Management	Appliance	Settings	Roles	Q Search users, groups or	applications
rectories	Ident	ity Providers	Password Recov	ery Assistan	Authentication	Methods	Policies			Manage
		Authentication Important: Where sure you update	on Methods for n you disable an au e the access policy	r Built-in Ic thentication r rules to selec	lentity Providers nethod, the authentic t another authentical	S cation methoo tion method.	d is removed a	as a choice	in the access policy rules page	e. Make
		Authenticatio	n Methods		Configure			Status	;	
		Device Comp ONE UEM)	liance (with Works	pace	1			Disabled	1	•
		Password (wi	ith Workspace ON	E UEM)	1			Disabled	1	
		VMware Verif	fy		1			Enabled		
		Mobile SSO ((for iOS)		1			Disabled	1	
		Password (Lo	ocal Directory)		1			Enabled		
		Mobile SSO ((for Android)		1			Disabled	ł	
		Certificate (C	loud Deployment)		7			Disabled	ł	

- 2. In the Workspace ONE Access admin console
 - Navigate to Identity & Access Management > Authentication Methods.
 - Select the pencil icon next to Certificate (Cloud Deployment)

Certificate (Cloud De	ployment)
Enable Certificate Adapter	
Root and intermediate CA certificates*	When enabled, SSL termination cannot be done on the Load Balancer (Load Balancer needs to be configured as PaseTbrough) Select File You can upload multiple DER and PEM root and intermediate CA certificates including concatenated PEM files
Uploaded CA Certificates	CN=Livefire (9C3F7E62F73568A9A73649A0EEBF63394B86705B2E723AE275170F5E939386EF) 🗶
User Identifier Search Order	upn subject Select the search order for locating the user identifier within the certificate. upn: UserPrincipalName value from the Subject Alternative Name, email: Email address from the Subject Alternative Name, subject: UID value from
Validate HDN Format	Cancel Save
A N	lame Da
Desktop *	VidmAirWatchRootCertificate.cer 5/ VMware Workspace ONE.html 5/ VMware Workspace ONE.film
🗄 Documents 🖈	
Eile name	VidmAirWatchRootCertificate.cer V All Files (*.*) V
rite name.	

- 3. In the **Certificate (Cloud Deployment)** page
 - Select the tickbox to Enable Certificate Adapter

- Select Select File for the Root and Intermediate CA Certificates
- Select the certificate we have downloaded from the UEM console earlier
- Select Open

Please click OK to con	firm and upload file.
	Cancel OK
Certificate (Cloud De	ployment)
certificates*	
	You can upload multiple DER and PEM root and intermediate CA certificates including concatenated PEM files
Uploaded CA Certificates	CN=Livefire (9C3F7E62F73568A9A73649A0EEBF63394B86705B2E723AE275170F5E939386EF) 🗶
User Identifier Search Order	upn subject •
	Select the search order for locating the user identifier within the certificate. upn: UserPrincipalName value from the Subject Alternative Name; email: Email address from the Subject Alternative Name; subject: UID value from the Subject
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.

- 4. In the **Update Auth Adapter** window
 - Select OK.
- In the Certificate (Cloud Deployment) window
 - At the bottom of the page, select Save

workspace UNE HUD Service ×	vontes į viviware inteiliger 🔺 😺 viv	
← → C ☆ 🔒 aw-grantztrneln	ovtest.vidmpreview.com/SAAS/adm	in/identity
👖 Apps 🔇 my-ip.livefire.lab/ip 🚾 VMw	vare Horizon 🏽 🍪 UAG-HZN 🔮 U	AG-UEM 🔤 NSX manager 🍦 Ar
(8) Workspace ONE™ Access	s	
Dashboard 👻 Users & Groups	Catalog 👻 Identity & Access I	lanagement Roles
Directories Identity Providers Pa	ssword Recovery Assistant A	ithentication Methods Policie
Identity Providers (3)		
Identity Provider Name	Auth Methods	Directory
System Identity Provider	Password (Local Directory)	System Directory
Built-in	Password (cloud deployment)	LivefireSync
IDP for LivefireSync	Password (cloud deployment)	LivefireSync

- 5. In the Workspace ONE Access Console
 - Navigate Identity Providers
 - Under Identity & Access Management, select on Built-in

Directories	Identity Providers	Password Recovery A	Assistant Authentication	n Methods	Policies
	А	Authentication Methods	Select which authentication	methods the Id	P will use to authenticate users.
			Authentication Methods		Associate Authentication Method
			Password (Local Directo	ory)	
			Certificate (cloud deploy	yment)	
	c	Connector(s)	WS-1Connector (ws1-	connector.euc	-livefire.com) 🗙
			Add a Connector	You can sel connector a connector, a Important: F	ect additional connectors for high availability (HA). Create the ctivation code from the Add a Connector page and set up the and then select the connector for this IdP. For high availability, each connector must have the same
	-			authenticati	on method configuration.
	C	Connector Authentication Aethods	Authentication Methods		Associate Authentication Method
			Password (cloud deployment)		✓
	к	CC Certificate Export	Download Certificate Export the KDC server root	certificate for u	se in a Mobile Device Management profile.
	-		Save		

6. In the **Built-In** page

• Navigate to the Authentication Methods area

- Select the check box next to Certificate (Cloud Deployment)
- Select **Save** at the bottom of the page.

Dashboard Users & Groups Catalog Identity & Access Management Roles Directories Identity Providers Password Recovery Assistant Authentication Methods Policies ADD POLICY EDIT DELETE EDIT DEFAULT POLICY NETWORK RANGES Policy Name Applies to Rule default_access_policy_set 1 Application(s) 2 Ru	Dashboard Users & Groups Catalog Identity & Access Management Roles Directories Identity Providers Password Recovery Assistant Authentication Methods Policies ADD POLICY EDIT DELETE EDIT DEFAULT POLICY NETWORK RANGES Policy Name Applies to Rule default_access_policy_set 1 Application(s) 2 Ru	8 wa	orkspace ONE™ Access		
ADD POLICY EDIT DELETE EDIT DEFAULT POLICY NETWORK RANGES Policy Name Applies to Rule default_access_policy_set 1 Application(s) 2 Rule	ADD POLICY EDIT DELETE EDIT DEFAULT POLICY NETWORK RANGES Policy Name Applies to Rule default_access_policy_set 1 Application(s) 2 Rule	Dashboard Directories	d Users & Groups Catalog Identity Providers Password Reco	Identity & Access Management Roles very Assistant Authentication Methods Policies	
Policy Name Applies to Rule O default_access_policy_set 1 Application(s) 2 Rule	Policy Name Applies to Rule default_access_policy_set 1 Application(s) 2 Rule		ADD POLICY EDIT DELET	E EDIT DEFAULT POLICY NETWORK RANGES	
default_access_policy_set 1 Application(s) 2 Ru	default_access_policy_set 1 Application(s) 2 Ru		Policy Name	Applies to	Rule
			<pre>default_access_policy_set</pre>	1 Application(s)	2 Ri

- 7. In the Workspace ONE Access console
 - Navigate to Identity & Access Management > Policies
 - Select default_access_policy_set

K BACK	
default_	access_policy_set
EDIT	DELETE
Definition	

- 8. Under Policies \default_access_policy_set
 - Select EDIT

Edit Policy		
1 Definition 2 Configuration	You can create a list of ru of devices that can acces application before reauth	ules to access the applications select ss the applications, the auth method menticating.
3 Summary	Network Range	Device Type
	# ALL RANGES	Web Browser
	# ALL RANGES	Workspace ONE App

9. In the **Edit Policy** page

- Select the second tab from the left column **Configuration**
- Select All Ranges next to Web Browser in the Device Type Category

, Then perform this action	Authenticate using ~	٩
then the user may authenticate using *	Certificate (Cloud Deployment) ~	٩
If the preceding method fails or is not applicable, then	Password (cloud deployment) ~	٩
If the preceding method fails or is not applicable, then	Password (Local Directory) ~	۵ 🕂
	ADD FALLBACK METHOD	
Re-authenticate after *	8 Hour 🗸 🛈	
CANCEL		

- 10. In the **Edit Policy Rule** page, edit the following next to:
 - then the user may authenticate using * change to : Certificate (Cloud Deployment)

- if preceding method fails or is not applicable then change to Password (Cloud Deployment),
- then Select ADD FALLBACK METHOD
- Select **Password (Local Directory)** as the third authentication option.
- Select **SAVE** at the bottom of the window

of devices that can access the applications, the auth me application before reauthenticating.					
Network Range	Device Type				
# ALL RANGES	Web Browser				
# ALL RANGES	Workspace ONE App				
ADD POLICY RULE					

- 11. In the Edit Policy \ Configuration page
 - Select ADD POLICY RULE

If a user's network range is *	ALL RANGES	~	(^
and the user accessing content from *	Windows 10	~	٢			
and user belongs to group(s)	Q Select Groups		٩			
	Rule applies to all users if no group(s) selected.					
and user is registering FIDO2 authenticator *	No No		١	1		
Then perform this action	Authenticate using	~	1			
then the user may authenticate using *	Certificate (cloud deployment)	~	٩	Ð	P.	ľ
If the preceding method fails or is not applicable, then	Password (cloud deployment)	~	٩	Ð	1	
If the preceding method fails or is not applicable, then	Password (Local Directory)	~	(1)	Ð	×	•
		CANC	EL		SAV	Έ

- 12. In the **Add Policy Rule** page, add the following next to :
 - and user accessing content from : from the *drop down* select:- Windows 10
 - then the user may authenticate using: from the *drop down* select:- Certificate (Cloud Deployment)
 - If the preceding method fails or is not applicable, then : from the *drop down* select:-Password (cloud deployment)
 - Select + ADD FALLBACK METHOD
 - If the preceding method fails or is not applicable, then : from the *drop down* select:-Password (Local Deployment)
 - Select SAVE

Network Range	Device Type	Authentication	Re-authenticate	
# ALL RANGES	Web Browser	Certificate (cloud depl	8 Hour(s)	×
# ALL RANGES	Workspace ONE App	Password (cloud deplo	2160 Hour(s)	×
# ALL RANGES	Windows 10	Certificate (cloud depl	8 Hour(s)	×
ADD POLICY RULE				

CANCEL	BACK
--------	------

NEXT

13. Select **NEXT** on the **Edit Policy Page**

1 Definition	Definition
2 Configuration	Name default access policy set
3 Summary	Description Default access policy set Applications O Application(s) Configuration Policy Rule 1 If a user's network range is ALL RANGES and the user is accessing content from Windows 10 and the user belongs to the group(s) All Users then the user may authenticate using Certificate (Cloud Deployment)
	Fallback method 1: Password (cloud deployment) Re-authenticate after 8 hour(s) Advanced Properties A

14. On the **Edit Policy \ Summary** page

- Select **SAVE** .
 - You have now enabled Certificate (Cloud Deployment) as an authentication method on the default access policy.
 - Our next step is to ensure this implementation is working.

Part 3: Windows 10 Single Sign-On using Certificates



- 1. On the Desktop of **ControlCenter**
 - Open your **Remote Desktops** folder
 - RDP to your Windows 10 Client (W10Client01.RDP)
 - Authenticated using :
 - Username euc-livefire\administrator
 - Password VMware1!

N10Client01	- 172.16.30.106	- Remote Desktop Connection			
0	New Tab	× +			
Recycle Bin	$\ \ \leftarrow \ \ \rightarrow \ \ G$	aw-manfred.vidmpreview.com			
Microsoft Edge					
Witware Horieu Google			Goo	ogle	
		Q Search G	ogle or type a URL		V
			0	+	

2. On your W10Client01

- Open the Chrome Browser
- Navigate to Your unique Workspace ONE Access Tenant

3	http	os://ca	s.vid	dmpre	view.cor	m/cas X	+										-	I		×
←	\rightarrow	С		ê c	as.vidn	npreview	.com/ca	as/t/AW-N	IANFRED,	/API/1.0/R	EST/landing?E	AB_CALLB	ACK_URL=%2	Fauth%2	Flogin	%2Fembe	ddedaut	☆	θ	:
					r		Sele Selec	ct a certif t a certificat	icate te to authe	nticate your:	self to cas.vidmp	review.com	:443		×					
							Sub	ject			Issuer		Serial							
							Ma	ark			ManfredVoga	algmailcom	0187FF							
							Ce	ertificate int	formation]			ОК	Cancel						

3. On your W10Client01

- You will within a second get a prompt from Chrome to confirm the use of the installed client certificate
- Notice the URL has **/cas** which is the certificate authentication service that will validate that certificate.
- Select **OK** to confirm the use of the certificate.

NOTE: If you do not see the Certificate pop-up window, instead you are directed to the normal Access authentication page. Go back to Part 1 in UEM and ensure the Certificate profile we have published has been installed on the device.

)	Favorites	Apps	For You	Support	
	Q Sea	rch Apps			
				All Apps Categories ~	
All A	Apps				

4. You should now be authenticated to the Intelligent Hub on the Chrome browser.

This concludes the Certificate-Based authentication lab, allowing users to authentication to corporate resources securely from a managed Windows 10 device.

Extra Material: Suppress Pop-up on Chrome Part 1

In the flow above the user's experience is not ideal requiring the user to manually select the certificate from the prompt during authentication.

The various browsers handle the rules to auto-select certificates differently. In Chrome you can do this either through registry files or Chrome ADMX policies as per this article. https://www.chromium.org/administrators/policy-list-3#AutoSelectCertificateForUrls

In this lab we will show you both, first you will use the **registry option** and later we will use the **ADMP policy option** using UEM.

Alternatively you can download the Chrome Policy templates here: <u>http://dl.google.com/dl/</u> <u>edgedl/chrome/policy/policy_templates.zip</u>



1. On the **Controlcenter** base navigate to the **Remote Desktops** folder on the **desktop** and RDP to **W10Client01**



2. On the W10Client01 click **Start** and type **registry editory** and click on the **Registry Editor**

🏥 Registi	ry Ec	litor						
File Edit	Vi	ew Fav	orites Help)				
Computer	\HK	EY_LOCA	L_MACHINE	\SO	FTWARE\Policies			
		CbDefe	nse	^	Name	Туре	Data	
>		Classes			ab (Default)	REG_SZ	(value not set)	
>		Clients				-		
		CVSM						
		Default	UserEnvironr					
2		Intel						
5		Macron	nedia					
5		Microso	oft					
		ODBC						
>		OEM						
>		OpenSS	Н					
>		Partner						
~		Petisia	Collapse			1		
		Re	New		>	 Key 		
		Te	Final		· · · · · ·	Ney Ney		
		Tł	rina			String Valu	e	
5		VI	Delete			Binary Valu	Je	
>		w	Rename			DWORD (3	2-bit) Value	
>		W	Europe			QWORD (6	54-bit) Value	
>	S	/ST	ехроп			Multi-Strin	ng Value	
` > <mark> </mark> ⊦	HKE	(_U	Permissions			Expandabl	e String Value	
<	HKE/	(^	Copy Key N	ame	2	cxpandabi	e samg value	
wa			Go to LIVEV	cu	DDENIT LICED			

3. Navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies

Right click **Policies** and click **New** > **Key**. Then Type **Google**.

· · · · · · · · · · · · · · · · · · ·	Policies Microsoft Google			
	Registere	Expand		
>	Teradici	New	>	Кек
> 🔤	ThinPrint	Find		~~~
>	VMware,			String Value

4. Right Click on the **Google** and click **New** > **Key**. Then type **Chrome**.

 Partner Policies Microsoft Google Chrome 				
RegisteredAr	Expand		1	
> 🔤 Teradici	New	>	Ke	5
> ThinPrint	Find		~	·

5. Right Click on **Chrome** and click **New** > **Key**. Then type **AutoSelectCertificateForUrls**

You should now have: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ AutoSelectCertificateForUrls

Registry Editor				
File Edit View Favorites Help			Colorado de Constanto - Constanto	
	F IWARE\Policies\God	gie\Chrome\Auto	SelectCertificatesForUris	
	Name	іуре	Data	
AirWatchMDM	(Default)	REG_SZ	(value not set)	
CbDefense				
> Classes				
> Clients				
📙 DefaultUserEnvironment				
> Google				
> Intel			New >	Key
> Macromedia				61 N I
> Microsoft				String Value
> ODBC				Binary Value
> OEM				DWORD (32-bit) Value
Partner				QWORD (64-bit) Value
Policies				Multi-String Value
> Microsoft				Expandable String Value
Google				
Chrome				
AutoSelectCerti				

6. Right-Click in the white space inside the key **AutoSelectCertificateForUrls** and click **New** > **String Value**

≗lp JE\SO	FTWARE\Policies\G	oogle\Chrome\Auto	SelectCertificateForUrls
^	Name ab) (Default) ab) 1	Type REG_SZ REG_SZ	Data (value not set)

7. Give the key the name 1

File Edit View Favorites Help			
Computer\HKEY_LOCAL_MACHINE\SOF	TWARE\Policies\Go	ogle\Chrome\Auto	SelectCertificateForUrls
IWARE IRWATCH irWatchMDM bDefense lasses	Name (Default) Default) Modify	Type REG_SZ REG SZ	Data (value not set)
lients VSM efaultUserEnvironment	Modify B Delete Rename	inary Data	

8. Right-click on the 1 and click Modify...

iputer (HKEY_LOCAL_MACHIN	VE\SOFT	WARE\Policies\Go	ogle\Chrome	AutoSelectCertificateFo	orUrls				
>	SAM	^	Name	Type	Data					
	Edit String				× (value not	set)				
Ť.	Value erme:				{"pattern"	"https://cas.vidm	npreview.com", "filter	°{		
	1									
	Value data:									
	ttem":"https://cas.vidmp	review.c	om","filter":{"ISSUE	R":{"CN":"emu	sk"}}}					
			OK	Cano	el					
Ļ	Google	_								
1	Intel									
	Macromedia									
5	Microsoft									
5	ODBC									
>	OEM									
a a										
CONSO	ier - [console koot(ce	runcate	- Current Oser(Pe	ersonal/Certin	catesj					
	Action View Favori	ites W	indow Help							
File A			indent indep							
File A	2 💼 🔏 🗞									
File A	🖄 📰 🦨 🖦 🗙									
File /	🖄 📷 🦨 🕒 🗙 Local NonRemovable A Remote Derkton	lssu	ed To		Issued By	Đ	xpira			
File	Local NonRemovable A Remote Desktop Smart Card Trusted R	i Issu	ed To	0453CC63E	Issued By AirWatchCa	E) 21	xpira 6/11/			
File 4	Employee Content of the second s	i Issu Pilssu Pils Issu	ed To EFA05C70C7R5648 ser32SCR	A453CC63E	Issued By AirWatchCa emusk	E 20 21	ixpira (6/11/ (2/03/			
File /	Local NonRemovable A Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Devices	i Issu Si Issu	ed To FFA05C70C7R5648 ser32SCR	a4530063E	lssued By AirWatchCa emusk	E 21 21	ixpira 16/11/ 12/03/			
File A > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Local NonRemovable A Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Devices Windows Live ID Tok	Survey and a second sec	ed To FEADSC 70C 7R564R ser32SCR	MASSCC63E	Issued By AirWatchCa emusk	E 21 22	ixpira 16/11/ 2/03/			
File A > =	E Total NonRemovable A Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Packaged Ap Trusted Devices Windows Live ID Tok WindowsServerUpda	Survey of the second se	ed To FFA0SC 70C 7R564R ser32SCR	4453CC63E	Issued By AirWatchCa emusk	E 21 22	xpira 16/11/ 12/03/			
File 4	Local NonRemovable A Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Devices Windows Evier ID Tok Windows ServerUpda tificates - Current Us	Survey and a second sec	ed To FFA05C 70C 7R5548 ser325CR an Certificate General Details	A453CC63E	Issued By AirWatchCa emusk	E 2i 22	xpira 6/11/ 12/03/			
File 4	Local NonRemovable Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Devices Windows Live ID Tok Windows ServerUpda tifficates - Current Usp Personal	San	ed To EFEADSC 70C 7R5548 ser32SCR General Details	Certification P	Issued By AirWatchCa emusk	E 21 22	ixpira 16/11/ 2/03/			
File 4	Cocal NonRemovable A Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Packaged Ap Trusted Devices Windows Live ID Tok Windows ServerUpda tificates - Current Us Personal	Sale	ed To EEAnSC TOC 7R5548 ser32SCR General Details Show: <al></al>	6453CC63E Certification F	Issued By AirWatchCa emusk	E 21 22	xpira 6/11/ 2/03/			
File 4	Continue of the second se		ed To EEADSC 70C 7R5648 ser32SCR General Details Show: CAll> Eadd	Certification F	Issued By AirWatchCa emusk	22 22 >	ixpira 6/11/ 2/03/			
File 4	Control C	Sur Sur	ed To FEANSC 70C 785548 ser325CR General Details Show: <all> Field</all>	0453CC63E Certification F	Issued By AirWatchCa emusk Path Value Value	E 22 22 >>	xpira 6/11/ 2/03/			
File 4	Local NonRemovable ~ Remote Desktop Smart Card Trusted R Trusted Decktoged Ap Trusted Deckes Windows Live ID Tok Windows ServerUpda diffactes - Current Up Descond Centificates Tousted Root Centific Enterprise Trust Intermediate Centific Enterprise Trust	San	ed To ed To FEADSC 70C 785548 ser325CR General Details Show: ktps://www.edu/action.org Field Show: ktps://www.edu/action.org	0453CC63E Certification P	Issued By AirWatchCa emusk Value V3 0195ab	E 22 22 >>	xpira 16/11/ 22/03/			
File A > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Local NonRemovable A Remote Deaktop Smart Card Trusted R Trusted Packaged Ap Trusted Devices Windows ErverUpda Undows Live ID Tok Windows ServerUpda Centificates Trusted Robot Centric Interprise Trust Internedista Centific Active Directory Uses	Survey of the second seco	ed To FEADSC70C785648 ser32SCR Certificate General Details Show: <al> Field Yersion Signature al Signature al</al>	6453CC63E Certification F er opritium	Issued By AirkVarchCa emusk Path Value V3 0195ab d+b51285A	E 21 22 >>	xpire 6/11/ 2/03/			
File A -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> -> ->	Local NonRemovable Remote Desktop Smart Card Trusted R Trusted Packaged Ap Trusted Devices Windows Live ID Tok Windows ServerUpda tricates - current Up Personal Certificates Trusted Root Certific Enterprise Trust Intermediate Certific Active Directory User Trusted Poulishers Trusted Poulishers		ed To ed To Certificate General Detais Show: <al> Field Serial numbo Serial numbo Serial numbo</al>	er gorithm	Issued By AirWarchCa emusk Value V3 0195ab ehs1375A	6 2 2 2 2 2	xpira 6/11/ 2/03/			
File 4 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Control C		el Certificate el Certificate General Details Show: cAl> Field Version Serain number	Certification F	Issued By AirWarchCa emusk Value V3 0155ab dha512R5A dha512R5A	6 2 2 2	xpira 16/11/ 22/03/			
File 4 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Local NonRemovable A Remote Desktop Smart Card Trusted R Trusted Packaged Ap Tousted Derkces Windows Live ID Tok Windows ServerUpda Tousted Derkces Windows ServerUpda Tousted Noal Centrice Trusted Noal Centrice Trusted Noal Centrice Trusted Noal Centrice Thirde Pachages Untrusted Centrice Thirde Pachages Untrusted Centrice Thirde Pachages		Person Show: Allow Person Show: Allow Show: Allow Show:	Certification F	Issued By AirWatcht's emusk 2ath Vale V3 C135ab eta1325A d4513 careerer d2020 06137	E 22 22 ×	2;pire 16/11/ 2:/03/			
File 4 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Control C		and the second s	Certification F	Issued By AirWarchCa emusk Value Va	127 127	xpir# 6/11/ K			
File 4 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Control C		and the provided of the provid	Certification F	Issued By AirkVarchCa emusk Value V3 0 055bb dha51355A dha53 20 Arch 200 00:33 22 March 200 00:33 22 March 200 00:33	22 22 24 25 25 25 27 27 27	xpr# KATU 2203/			
File 4 Image: Constraint of the second	Contributed Party Root Certificate Fundhering Viewer		Ad To Certificate General Details Show: (All)> Field System and the System an	er gorithm	AirWarchCa emusk Path Value V3 0195ab ehs125A 4hs125A 22 March 2030 08:37 1 Inser35C/D	127 127 127 127	ixpra 16/11/ K			

9. Fill in the Value data with the following replacing the highlighted text with the issuer value from your certificate. This is the certificate issuer name. When using **UEM certificates** this is the name of the Organization group from which the Certificate profile has been created.

{"pattern":"https://cas.vidmpreview.com","filter":{"ISSUER":{"CN":"emusk"}}}

Note: Some organizations may have multiple certificates issues by the same CA and will require more detail in that scenario reference link at the top of the lab

EXAMPE:

Software\Policies\Google\Chrome\AutoSelectCertificateForUrls\1 = "{"pattern":"https://www.example.com","filter":{"ISSUER":{"CN":"certificate issuer name", "L": "certificate issuer location", "O": "certificate issuer org", "OU": "certificate issuer org unit"}, "SUBJECT":{"CN":"certificate subject name", "L": "certificate subject location", "O": "certificate subject org", "OU": "certificate subject org unit"}}"

Policies	× +					- 0	×
(< → C ∆ (Chrome chrome://policy					* 0	:
Apps							
Policies					Filter polici	es by name	
Reload policies Exp	ort to JSON Copy as JSON				Show po	licies with no value	e set
Status							^
Google update							
Last fetched: 2 hours a	igo						
Chrome Policies					_		
Policy name	Policy Value	Source	Applies to	Level	Status		
AutoSelectCerti 🖻	{"pattern":"https://cas.vidmpreview.com","filter":	Platform	Machine	Mandatory	ок	Show more	
Google Docs Offline							J
D 11	n-P	2	· · · · · · ·	1	21 1		

10. Open Chrome on W10Client01 and browse to chrome://policy

You should now notice that you have a Chrome Policy **AutoSelectCertificateForUrls**. This is a sanity check to make sure that the Registry entry has been successfully created.

NOTE: if you do not see the policy. Click **Reload policies** in the top left at which point you should see the policy appear.



11. In the navigation bar type the **Workspace ONE Access URL** and hit enter. You will be authenticated and land on the **Intelligent hub page.**

You will notice a in the URL a redirect to cas.vidmpreview.com at which point the certificate gets presented and validated, however the user is not prompted to select the certificate.

Extra Material: Suppress Pop-up on Chrome Part 2

In this part we will look at how we can automate the process so our entire fleet of Windows 10 managed devices will get the chrome policy to auto-select the appropriate certificate for SSO in the Chrome browser.

We again have two options to realize this. One is to use the above registry option. Export the registry, create a .bat file that installs the registry key and upload to UEM as Files/ Actions part of Product Provisioning.

The second option and the one we will use (just to change it up:) is to configure ADMX template using CSP. We can do this using custom profiles as described here: https://code.vmware.com/en/samples/3329/windows-10---chrome-admx#

First we will deploy the ADMX policy as part of a custom profile, then we will create a policy that configures the "AutoSelectCertificateForURL"

🖏 Works	pace ONE UEM		ManfredVogal@gmail.com
GETTING STARTED	Dashboard List View Details View		Devices > Profiles & Resources Profiles
MONITOR	Device Updates		Filters » ADD 🗸
	Lifecycle	>	Profile Details Add Pro
L DEVICES	Profiles & Resources	\sim	W10 - SCEP- SSC Upload Profile
	Profiles		SCEP Batch Import
ත	Baselines		
ACCOUNTS	Resources		
***	Batch Status		
APPS & BOOKS	Profiles Settings	>	

 Open the Workspace ONE UEM admin console and navigate to Devices > Profiles & Resources > Profiles > ADD click Add Profile

Windows		
11100115		
Select Device	Туре	
4		
Windows Des	<top< td=""><td></td></top<>	
Password Wi-Fi		
VPN Crede	ntials	
Restrictions Defen	der Exploit	
Guard Data Drotoction Windo	ur Helle	
Select Conte	ĸt	
User Profile		Device Profile
	Settings will	apply to the entire device, regardless
	Password	
	Wi-Fi	
	VPN	
	Credentials	
	Restrictions	

2. In the Add Profile window Select Windows > Windows Desktop and Device Profile

Add a New Windows Desktop Profile								
Find Payload	General							
General	General							
assword	Name *	W10 - Chrome - ADMX						
Vi-Fi	Version							
'PN	version	1						
redentials	Description							
estrictions								
efender Exploit uard	Deployment	Managed v						
ata Protection	Assignment Type	Auto ~						
/indows Hello	Allow Removal	Always v						
rewall (Legacy)								
irewall	Managed By	ManfredVogal@gmail.com						
nti-Virus								
ncryption	Smart Groups	al@gmail.com)						
/indows Updates		Start typing to add a group ۹						
roxy								
EM Updates	Exclusions	NO YES						

- 3. In the **General** payload fill in the following:
 - Name : W10 Chrome ADMX
 - Smart Groups Select the World Icon for your Organization Group {should be you email address}

Add a New Windows Desktop Profile	e	×
Find Payload		
Defender Exploit Guard		
Data Protection		
Windows Hello		
Firewall (Legacy)	Custom Settings	
Firewall		
Anti-Virus	CONFIGURE	
Encryption		
Windows Updates		
Proxy		
OEM Updates		
SCEP		
Application Control		
Windows Licensing		
BIOS		
Kiosk		
Personalization		
Peer Distribution		
Custom Settings		
	SAVE AND	PUBLISH CANCEL

4. On the left find **Custom Settings** payload and click **CONFIGURE**



- 5. Open a **new tab** and navigate to <u>https://code.vmware.com/en/samples/3329/windows-10---</u> <u>chrome-admx#code</u>
 - Click on Browse Code and Drill down to the ChromADMXinstall.xml
 - **Copy** the entirety of the XML

Defender Exploit Target Guard Target Data Protection Make Commands Atomic Windows Hello Make Commands Atomic Firewall (Legacy) Install Settings Firewall Install Settings Anti-Virus Install Settings Encryption Windows Updates Proxy	
Data Protection Make Commands Atomic Windows Hello Make Commands Atomic Firewall (Legacy) Install Settings * Firewall Anti-Virus valueName="SuppressUnsupportedOSWarning"> < sparentCategory ref="googlechtmmg"> < supportedOSWarning"> < su	
Windows Hello Make Commands Atomic Firewall (Legacy) Install Settings * Firewall Install Settings * Anti-Virus	
Firewall Install Settings * valueName="SuppressUnsupportedOSWarning"> Firewall valueName="SuppressUnsupportedOSWarning"> Anti-Virus Encryption Nindows Updates Yroxy	
Firewall unstail settings valueName="Suppressionauported/OSWarning"> YalueName="Suppressionauported/OSWarning"> YalueName=Suppressionauported/OSWarning"> YalueName YalueName	
Anti-Virus SupportedOn ref="SUPPORTED_WIN7"/> cenabledValue cdecimal value="1"/> c/enabledValue>	
Encryption <decimal value="1"></decimal> <td></td>	
Windows Updates Vindows Updates Proxy </td <td></td>	
<pre><gecmaivaue=0></gecmaivaue=0> </pre> <pre>cype://processing.com/second/sec</pre>	
DEM Updates	
explainText="\$(string.SyncDisabled_Explain)" iCEP key="Software\Policies\Google\Chrome" name="SyncDisabled"	
Application Control presentation="\$(presentation.SyncDisabled)" valueName="SyncDisabled">	
Vindows Licensing <pre>cparentCategory ref="googlechrome"/></pre>	
kenove settings -	
Personalization	
Peer Distribution	

6. Navigate back to the **Workspace ONE UEM** Console and **paste** the XML into the **Install Settings** box of Custom Settings.

Data HOLECHOIT		_	
Windows Hello	Make Commands Atomic		
Firewall (Legacy)		(F	
Firewall	Install Settings *	valueName="SuppressUnsupportedOSWarning"> <parentcategory ref="googlechrome"></parentcategory>	Ŧ
Anti-Virus		<supportedon ref="SUPPORTED_WIN7"></supportedon> <enabledvalue></enabledvalue>	
Encryption		<decimal value="1"></decimal> 	
Windows Updates		<disabledvalue> <decimal value="0"></decimal></disabledvalue>	
Proxy			
OEM Updates		<pre><policy <="" class="Both" displayname="\$(string.SyncDisabled)" explaintext="\$(string SyncDisabled Explain)" pre=""></policy></pre>	
SCEP		key="Software\Policies\Google\Chrome" name="SyncDisabled"	
Application Control		valueName="Syncbisabled">	
Windows Licensing		<pre><parentcategory rel="googlechrome"></parentcategory></pre>	5
BIOS	Remove Settings *	<delete><cmdid>1</cmdid><item><meta/><format>chr</format></item></delete>	+
Kiosk		<iype>text/plain</iype> <larget> <locuri>./Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Chrome/P</locuri></larget>	
Personalization		olicy/ <u>ChromeAdmx</u> <data></data>	
Peer Distribution			
Custom Settings			
		SAVE AND PUBL	ISH CAN

7. Paste the below XML into the Remove Settings box of the Custom Settings payload.

<Delete><CmdID>1</CmdID><Item><Meta><Format>chr</Format><Type>text/
plain</Type></Meta><Target><LocURI>./Vendor/MSFT/Policy/ConfigOperations/
ADMXInstall/Chrome/Policy/
Chrome/Mata>

CHIOMEAdmx<	/ LOCURIX/	larget/CDat	a/ <th>/ I Lem/<!--</th--><th>Derece></th></th>	/ I Lem/ </th <th>Derece></th>	Derece>

Remove Settings *	<delete><cmdid>1</cmdid><item><meta/><format>chr</format> <type>text/plain</type><target> <locuri>./Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Chrome/P olicy/ChromeAdmx</locuri></target><data></data></item></delete> Í	
	Θ	
	SAVE AND PUBLISH CANCEL	

View Device /	(55)Griffent		Assignment Status	All	×	Filter Grid		l e
Assignment Status	Friendly Name	llsor	Platform/OS/Model	7.41	Phone Number	Organizatio	n Group	
Added	Mark VMware7.1 Window	Mark	Windows Desktop / Windo	ws	Filone Number	ManfredVos	zal@gmail.con	n
ems 1-1 of 1							Page Size: 20	

8. Click **SAVE AND PUBLISH** and **PUBLISH** on the View Device Assignment window.

	List View		Pr	rofiles
	Details View			
MONITOR	Device Updates		Fi	ilters » ADD 🗸
	Lifecycle	>		Profile Details 🛛 🗛 Add Profile 👦 pads Man
	Profiles & Resources	~	0	W10 - Chrome - Upload Profile
	Profiles		I	Custom Settings Batch Import
සි	Baselines		0	W10 - SCEP- SSO Windows Deskton - User 1 Man
ACCOUNTS	Resources			SCEP
	Batch Status			

9. Click **ADD** and **Add Profile** in the **Profiles** page.

Select a platform to start:	
Android	iOS Apple iOS
Select Device Type	Android (Legacy)
Windows Desktop	
Password Wi-Fi VPN Credentials Restrictions Defender Exploit Guard Data Protection Windows Hello Firewall FirewallV2	
Select Context	
User Profile	Device Profile

10. Select Windows > Windows Desktop > User Profile

Add a New Windows I	Desktop Profile	
Find Payload General	General	
VPN	Name *	W10 - Chrome - AutoSelect
Credentials Windows Hello	Version	1
Single App Mode	Description	
Web Clips	Deployment	Managed v
Exchange ActiveSync	, ,	
SCEP	Assignment Type	Auto ~
Exchange Web Services	Allow Removal	Always ~
User Data Custom Settings	Managed By	ManfredVogal@gmail.com
	Smart Groups	ManfredVogal@gmail.com (ManfredVog al@gmail.com)
		Start typing to add a group
	Exclusions	NO YES

- 11. In the General payload set the following:
 - Name: W10 Chrome AutoSelect
 - Smart Groups: Select the World Icon for your Organization Group {should be you e-mail address}

ind Payload		
ieneral		
PN		
redentials		
Vindows Hello		
ingle App Mode	C	ustom Settings
Veb Clips		CONFIGURE
xchange ActiveSync	L	
CEP		
xchange Web ervices		
lser Data		
ustom Settings		

12. Go to the Custom Settings payload and click CONFIGURE

Add a New Windows	Desktop Profile		×
Find Payload	Custom Catting	-	
General	Custom setting:	5	
VPN	Target	OMA DM Client ~	
Credentials	Male Comments		
Windows Hello	Atomic	-	
Single App Mode	Install Settings *	<replace><cmdid>5</cmdid><item><target></target></item></replace>	Ŧ
Web Clips		<locuri>./Device/Vendor/MSFT/Policy/Config/Chrome-Policy-googlechro</locuri>	
Exchange ActiveSync	<pre> conten</pre>	<data><![CDATA[<enabled/><data <="" id="AutoSelectCertificateForUrIsDesc" p=""></data></data>	
SCEP		<pre>value='s#xtuuy('pattern':'nttps://cas.vidmpreview.com', 'niter': ("ISSUER":("CN':'emusk")))'/>])></pre>	
Exchange Web Services			
User Data			
	Remove Settings *		ŧ
		SAVE AND PURI	
eolal - 17 earola Baell Carl Kraker - Commit Heel Davi	nanali Castili ratan)		contest
etificate	×		
of bith order off wide SI wide Party 0 System 0.00 System			
Lott Proper bei Cop	CK .		

Paste the following XML into the Install Settings section of Custom Settings. Replacing the CN value (Highlighted) with your OrganisationGroup name without punctuation. (Eg. ManfredVogalgmailcom) This is the Issuer value if you would like to double check on you W10Client01 certificate.

<Replace><CmdID>5</CmdID><Item><Target><LocURI>./Device/Vendor/MSFT/
Policy/Config/Chrome~Policy~googlechrome~ContentSettings/
AutoSelectCertificateForUrls</LocURI></Target><Data><![CDATA[<enabled/><data
id='AutoSelectCertificateForUrlsDesc'
value='1{"pattern":"https://cas.vidmpreview.com","filter":{"ISSUER":{"ContentSettings"}</pre>

Exchange Web Services User Data Custom Settings	Remove Settings *	<delete><cmdid>5</cmdid><item><target> <locuri>./Device/Vendor/MSFT/Policy/Config/Chrome~Policy~googlechro me~ContentSettings/AutoSelectCertificateForUrls</locuri></target> <data></data></item></delete>	÷
			Θ
		SAVE AND PUBL	SH CANCEL

13. **Paste** the following XML into the Remove Settings section of the Custom Settings.

<Delete><CmdID>5</CmdID><Item><Target><LocURI>./Device/Vendor/MSFT/
Policy/Config/Chrome~Policy~googlechrome~ContentSettings/
AutoSelectCertificateForUrls</LocURI></Target><Data></Data></Delete>

SAVE AND PUBLISH CANCEL	<data></data>		
		SAVE AND PUBL	(ISH CANCEL

			Assignment Status	All ×	Filter Grid	°
Assignment Status	Friendly Name	User	Platform/OS/Model	Phone Number	Organization Group	
Added	Mark VMware7,1 Window	Mark	Windows Desktop / Windo	WS	ManfredVogal@gmail.com	n
ems 1-1 of 1					Page Size: 20	`
					PUBLISH CA	NCE

14. Click SAVE AND PUBLISH and PUBLISH on the View Device Assignment window.



15. On the **W10Client01** VM close **Chrome** and Re-open it. **Navigate** to Chrome://policy you should see the AutoSelectCertificate policy there. Navigate to your unique WorkspaceONE Access URL you should not be prompted for a certificate but it should be a seemless single-sign-on experience.

This concludes the Certificate-Based Authentication on Windows 10 and the configuration of the end-points to auto-select the appropriate certificate for single-sign on.

Author: Simeon Frank