Windows 10 Compliance Workspace One UEM + Workspace ONE Access

Part 1: Workspace One UEM Compliance Rules

WorkspaceOne allows administrators to check the device posture in addition to the credentials provided for authentication. This ensure's that not only the provided credentials are valid, but also the device being used to access corporate resources is deemed secure and compliant. WorkspaceOne UEM has a robust compliance engine that allows administrator to set a standard for security on devices.

First you will be configuring a standard for compliance on Windows 10 using WorkspaceOne UEM

Second, you will be configuring Workspace ONE Access Access Policies to check the device compliance during the authentication process.

Third, you will bring this to life by authenticating to O365 using Workspace ONE Access certificate adapter in conjunction with device compliance.

1. Let's begin with configuring our UEM compliance rules for Windows 10. (**Note**: that the same procedure can be used for Android and iOS, but in our scenario we will be dealing with Windows 10)

 Open the Workspace One UEM console on cn-livefire.awmdm.com and authenticate using your unique credentials. Navigate to Devices > Compliance Policies > List View and click + ADD

🖏 Works	pace ONE UEM	/ LiveFire Global / Simeon - P 🗸	
GETTING STARTED	Dashboard List View Lifecycle	>	Devices > Compliance Policies List View
	Profiles & Resources	>	➡ ADD
DEVICES	Compliance Policies	~	Active Name
සි	List View		
ACCOUNTS	Event Log		

2. Select **Windows** from the **"Select a platform to start:"** window and select **Windows Desktop** from the next page as this one relates to Windows10 specifically.

• Select **NEXT** at the bottom of the page. We have now set our rule we will now select an action.

Add Compliance	e Policy			;	×
Select a platform to	start:				
Android	Apple iOS	MacOS Apple macOS	Chrome OS (Legacy)	III GINIX	
Windows Rugged	Windows				
* Select Device T	уре				
Select a platform to	start:				
Windows Phone	Windows Desktop	9 Windows 7			

- 3. In the **Actions** tab validate the check box next to "**Mark as Not Compliant**" is selected.
- This will ensure that if our device does not follow the rules set in the previous page it will be flagged as not compliant. Now notice the drop down for the actions you can take. You could go as harsh as performing an enterprise wipe, or as subtle as notifying the user via a push notification.
- In the left dropdown leave Notify as the default and change Send Email to User to "Send Push Notification to Device" from the the action dropdown.
- Select + Add Escalation and leave as default. Notice you the user will be e-mailed after 1 day of the rule still being broken. Click NEXT at the bottom of the page

1 Rules 2 Actions 3 Assignment 4 Summary	
Immediately perform the following actions 🗹 Mark as Not Compliant	
Notify × Send Push Notification to Devi × Ø Default Template	o ×
After 1 Days • Perform the following actions: Repeat 🖉 Mark as Not Compliant	
Notify Send Email to User CC: Default Template	0 ×

4. In the **Add Compliance Policy** page notice all the rules your can set in the left hand drop down. These are all the parameters an admin can set to determine whether a device is compliant with the organizations security rules. For this particular lab we will be dealing with the **Firewall Status**. Configure the following:-

- On the left under Match select the dropdown and change MDM Terms of Use Acceptance to Firewall Status
- In the 2nd drop down, this should automatically change to Is
- in the 3rd dropdown change **Good** to "Poor".

Edit Device Policy	1					×
	0	Rules ② Actions	3 Assignment	4 Summary		
Natch All Y	Of The Follo	wing Rules			_	

5. Under the **Assignment** tab next **Smart Groups** select your unique **Organization Group** marked with the **world** symbol.

Click **NEXT**

	Image: Rules Image: Actions Image: Actions Image: Action and Action a
Managed By *	Simeon - PROD - Don't Delete
	🔀 Simeon - PROD - Don't Delete (Simeon - PROD - Don't Delete) 🎽
Smart Groups	Start typing to add a group

6. Under the **Summary** Tab change the default Name **Firewall Status** to - **Windows 10 -Firewall** and click **FINISH & ACTIVATE** at the bottom of the page.

eral me * Windows 10 - Firewall scription * Firewall Status ce Summary signed 1 mpliant 1 • n-Compliant 0 •					
eral me * Windows 10 - Firewall scription * Firewall Status ce Summary signed 1 mpliant 1 • n-Compliant 0 ©		1 Rules 2 Actions	3 Assignment	Summary	
me * Windows 10 - Firewall scription * Firewall Status cce Summary tigned 1 mpliant 1 • n-Compliant 0 •	General	C Notes C Actions	 Assignment 	Summary	
windows 10 - Firewall scription * Firewall Status igned 1 mpliant 1 © n-Compliant 0 ©	Name *				
scription * Firewall Status igned 1 mpliant 1 © n-Compliant: 0 © PREVIOUS FINISH FINISH 8	Name *	Windows 10 - Firewall			
igned 1 mpllant 1 ♥ n-Compliant 0 ♥ PREVIOUS FINISH FINISH 8	Description *	Firewall Status			
iigned 1 mpliant 1 ♥ n-Compliant 0 ⊗ PREVIOUS FINISH FINISH 8	Device Summary				
n-Compliant 0 O PREVIOUS FINISH FINISH &	Assigned	1			
n-Compliant 0 O PREVIOUS FINISH FINISH &	Compliant	1 0			
PREVIOUS FINISH FINISH	Non-Compliant	0 0			
PREVIOUS FINISH FINISH					
PREVIOUS FINISH FINISH					
PREVIOUS FINISH FINISH 8					
PREVIOUS FINISH FINISH					
PREVIOUS FINISH &					
PREVIOUS FINISH FINISH &					
			PREVIOUS	FINISH FINI	SH & AC

7. On your **Controlcenter** desktop, open the **Remote Desktop** folder.

- Select and RDP to the W10Client01 with username Administrator and password VMware1!
 - 1. On the windows 10 desktop select **Start** > **Run**
 - 2. In the **Run** window type **WF.msc**
 - In the Windows Defender for Firewall for Advanced Security select the Domain, Private and Public Profile and change the Firewall state from ON (recommended) to OFF, Select OK to close the Windows Defender Firewall window



8. Note! The Compliance Engine will now run (runs every 5 minutes by default) a check against the devices assigned to the Compliance Rule and report back to the Admin whether there are any device that have not passed the test. Since the Firewall is disabled on the Windows 10 Device we should get a flag stating it's non-compliant. This might take a while, so move on to the next section of the lab.

- Go back to your Workspace ONE UEM console, select Devices > Details View
- Notice now there is **1 COMPLIANCE VIOLATION** and the **Firewall Status** is red



Part 2: Workspace ONE Access Access Policy Device Compliance

1.

- Let's enable Device Compliance from AirWatch then enable Authentication Method in the **Built-In** Identity Providers .
 - 1. Navigate to your unique **Workspace ONE Access** tenant and authenticate as **System Admin**
 - 2. Navigate to Identity & Access Management Tab > Setup > AirWatch
 - 3. Scroll down to Compliance Check, select the **Enable radio button** and select **Save**

Identity & Access Management	Roles	Q Search users, groups or applications	
Terms of Use Preferences	Auto Discovery Okta AirWatch	Manage	Setup
	Workspace ONE catalog will show native apps and web links configured in the UEM console Enter Device Services URL* https://ds-livefire.awmdm.com/DeviceServices Save		
Compliance Check	Enable Compliance Check to verify that managed devices adhere to Air/Watch compliance policies.		

2. Open Identity & Access Management tab and select Identity Providers. On the page Identity Providers window select Built-in

8 Wor	kspa	ace ONI	E™ Acc	ess				
Dashboard	•	Users &	Groups	Catalog	•	Identity & A	ccess Manager	nent
Directories	Ide	ntity Prov	iders	Password	Recov	ery Assistant	Authentic	ation Me
			Identit	y Provid	ers (3)		
			Identit	y Provi	Auth	Methods	Directory	N
			Syster Identif Provic	m ty ler	Pass (Loca Direc	word al story)	System Directory	AL
			Built-i	n	Mobi (for A Devic	ile SSO Android) ce	Livefiresync	AL

3. Scroll down to **Authentication Methods** and enable the **Device Compliance (with AirWatch)** checkbox and scroll down and select **Save** at the bottom of the page.

Identity Provider Name	Built-in			
lleare	Select whi	ch users can authenticate using this IdP. Choose	from the available director	rries from the list below
00010	Syster V LiveFi	m Directory re Sync1		
Network	Select whi below.	ch networks this IdP can be accessed from. Cho	ose from the available ner	twork ranges from the list
Authentication Methods	Select whi	ch authentication methods the IdP will use to aut	henticate users.	
Authentication Methods	Select whi Authent	ch authentication methods the IdP will use to aut	henticate users.	n Method
Authentication Methods	Select whi Authent Device	ch authentication methods the IdP will use to aut ication Methods // Compliance (with AirWatch)	henticate users. Associate Authentication	n Method
Authentication Methods	Select whi Authent Device Mobile	ch authentication methods the IdP will use to aut ication Methods // Compliance (with AirWatch) SSO (for IOS)	henticate users.	n Method
Authentication Methods	Select whi Authent Device Mobile Passwo	ch authentication methods the IdP will use to aut ication Methods // Compliance (with AirWatch) SSO (for IOS) vrd (Local Directory)	henticate users.	n Method
Authentication Methods	Select whi Authent Device Mobile Passwo Certific	ch authentication methods the IdP will use to aut iscation Methods // Compliance (with AirWatch) SSO (for iOS) vrd (Local Directory) ate (Cloud Deployment)	Associate Authentication	n Method
Authentication Methods	Select whi Authent Device Mobile Passwc Certific	ch authentication methods the IdP will use to aut ication Methods // Compliance (with AirWatch) SSO (for iOS) wrd (Local Directory) ate (Cloud Deployment) 	Associate Authentication	n Method

- 4.
- Now Navigate and select Policies in the Identity & Access Management tab
 - 1. Next to the **SSO** policy select the **radio button** and select **EDIT**
 - 2. In the Edit Policy window select Configuration
 - 3. Select ALL RANGES next to the policy that applies to "Windows 10"
 - In this policy you will see that Certificate (Cloud Deployment) is the primary authentication method that is being used. We will now add device compliance, as an additional Access requirement, to allow user access. Select the + next to Certificate (Cloud Deployment)
 - 5. Next to **If the preceding method fails or is not applicable, then** CHANGE **Password** (cloud deployment) to Select fallback method....
 - 6. You will now have an **"and"** clause. In the dropdown select **Device Compliance** (AirWatch).
 - 7. Select **SAVE** at the bottom of the page.
 - 8. Select **NEXT** on the following page and **SAVE** again on the **Summary** of the **Edit Policy** page.



Part 3: Windows 10 Compliance in Action

- 1. Windows 10 Compliance in Action
- We will now test for Compliance as an authentication method.
 - 1. Navigate to the Desktop of the **ControlCenter2** and open the **Remote Desktop** folder and launch an RDP session using the **W10client01.RDP** client.
 - 2. Open **Chrome** within the **W10** machine that was enrolled. Now type in **Office.com** . Select the **sign-in to your account ICON** on the right-hand side of the page.

- 3. On the **Sign In** window type your **custom user** eg user35crsj@sanjose35.euclivefire.com, select **Next**
 - You will get a **pop up** from Chrome that will request you to select the appropriate certificate to use for authentication.
- 4. On the **Select a certificate** window select **OK**
- At this point Workspace ONE Access will check the validity of the certificate, but also send an API compliance query to Workspace ONE UEM to ensure the device is compliant (This is using the **UDID** that is present to vIDM in the certificate)

NirWatch.RDP	
AppVol.RDP	
Not CaptureVM.RDP	
No. CS1-pd1.RDP	
NP.RDP	
No. PackagingVM.RDP	
NDSH01a.RDP	
No. SQL.RDP	
S UEMProfiler.RDP	
D wrsa-01a RDP	
🕞 w10AirWatch-01a.RDP	
witoParent-ota.RDP	
WorkspaceUnit.KUP	
and the connectorable	- 0
365 Login Microsoft Offic × +	
C 🟠 🗎 office.com	± Θ
icrosoft Office Products v Resources v Templates More v Buy Office 365	All Microsoft ~ (R _b)
Microsoft	
Microsoft gn in x35cg@sanjose35.euc-ihefre.com account/Ceate one:	
Microsoft In in Storaj@anjoce33.suc-livefire.com count Cease onei access your account?	
Microsoft gn in (15craj@sanjose3.seuc-livefire.com excount? Genete creef t assess your account?	
Microsoft in in 25cm/Branjore35.euc-Invefre.com count Ceele anel recoss your account? in options	
Microsoft n in Storg@sanjoselSeuc-livefre.com sount Overle onel sount overle onel in options Next	
Microsoft gn in v15cru@sanjose35.euc-livefre.com taxass.geu account taxass.geu account en options	
Microsoft gn in 135org@sanjose3.5euc-livefire.com 13corest Over account? 13cores your account?	
Microsoft In in 25crg@samjoss3.suc-interfite.com count Owner onet access for accessft Next Next	
flicrosoft: h in Scruij@sanjcute3.suc-invertire.com contril Create one: Instants Instants Konta	
Microsoft n in Storaj@sanjoes35.euc-livefire.com count Outer one: teroptime teroptime teroptime teroptime X cate to which you want to authenticate casuidirepresences.ed:43	
Microsoft gn in Historij@aarjora25 euc-livefie.com xcount Owake onel 1 access your account? In access your account? I ac	
Microsoft gn in 255rg/granjos25 suc-livefre.com coourt Ceale coel tacers your account? tacers your account? Intert which you want to autoimprevies.com.413 Tealer Tealer tacers for account for an action of the formation	
Microsoft gn in ut35rg@sanjose35.euc-livefire.com account? Create one: It access you account? It access you account?	
Microsoft gn in 1/Scrii@sanjos25.euc-livefre.com xcount Owek onel traces your acount in options Vent reficate xcount Subject works acount of the subject of the sub	
Microsoft gn in stScrij@sanjose35.euc-inefere.com account Ceate one: rt account Ceate o	

2.

- You will notice an **Access Denied** message. We can also see this in the Event audits in Workspace ONE Access.
 - 1. In your Workspace ONE Access tenant. Navigate to **Dashboard** > Reports > Audit Events and select **Show**
 - 2. Look for an event that is LOGIN failed with your custom user,
 - 3. To the right select **View Details.** Scroll down until you find the area **"failuremessage"** and read what it says.

+			
mb.vidmpreview.com/SAR	/auth/login/imbeddedauthbroker/callback?requestTimeout=08		
	A		
	- 😺		
	Workspace ONS"		
	Access Denied		
your or To act	genizations compliance policy. ess your applications, the		
followin	g must be fixed. Windows 10 - Firewall		
×	Firewall Status +		
	VIIIware		
Reports			
Audit Ev	ents 🔶 User:		
Audit Eve	ents 🗘 User: days ago to 0 days ago Show		
Audit Eve From 3	ants User: days ago to 0 days ago Show		
Audit Eve From 3	ents User: User: days ago to o days ago Show		
Audit Eve From 3	ents User: User: days ago to o days ago Show		
Audit Eve From 3	ents User: days ago to 0 days ago Show		
Audit Eve From 3	ants User:	EVENT	
Audit Eve From 3 DATE, TIME (UTC)	ants User:	EVENT LOGIN failed	
Audit Eve From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM	User: User: Show User: U	EVENT LOGIN failed (um.vmware.names.ac.co	asses:ainvatchcompliance
Audit Eve From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM	User: User: days ago 0 0 days ago Show User (DOMAIN NAME) UserSSCRSJ (eu-ivefire.com)	EVENT LOGIN failed (un:sminare sace	asses airwatchcompliance)
Audit Eve From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM	User User Show	EVENT LOGIN failed (un:symmetric names accord	asses alwatchcompliance)
Audit Evr From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM	ents User: days ago to 0 days ago Show USER (DOMAIN NAME) USER (DOMAIN NAME) USER (COMAIN NAME)	EVENT LOGIN failed (um:vmware:names.ac.org	asses aliwatchcompliance)
Audit Eve From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM	ents User: days ago to o days ago Show USER (DOMAN NAME) USER (DOMAN NAME) USER SJ (euc-livefire.com)	EVENT LOGIN failed (un: vmware names ac c	asses aiwatchcompliance)
Audit Eve From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM	ents User: days ago to a days ago Show USER (DOMAIN NAME) USERSSCRSJ (euc-livefire.com)	EVENT LOGIN failed (untyminare names acc	asses airwatchcompliance)
Audit Eve From 3	User User: User (DOMAIN NAME) USER (DOMAIN NAME) USER (DOMAIN NAME)	EVENT LOGIN failed (un:vmware-names.ac.o	asses aiwatchcompliance)
Audit Eve From 3	ents User:	EVENT LOGIN failed (um:vmware:names.ac.or	asses aiwatchcompliance)
Audit Ev From 3 OATE, TIME (UTC) Nov 14, 2019 153:31 PM Vin Det Science Automation	ents User: days ago to o days ago Show USER (DOMAN NAME) USER (DOMAN NAME) USER (State of the state of th	EVENT LOGIN failed (um:vmware.names.ac.c	asses aiwatchcompilance)
Audit Ev From 3 DATE, TIME (UTC) Nov 14, 2019 1:53:31 PM Vii De Montoresternal TalueMeessage ¹¹ TalueMeessage ¹¹ TalueMeessage ¹¹	ents User: days ago to User: User (DOMAIN NAME) UserSSCRSJ (euIvefire.com) Within UserSSCRSJ (eu-Stream and the stream and the strea	ee", (000-3500), ownfloorsond (000-3500), ownfloorsond (000-3500), ownfloorsond (0000-3500), ownfloorsond (0000-3500), ownfloorsond (0000-3500), ownfloorsond (000-3500), ownfloorsond (000-350)	asses alwatchcompliance) 1: Mour device is corrently to be final-close cal

- 3. Windows 10 Compliance in Action continued...
- Use your RDP connection and go back and enable the Windows Firewall on the Windows 10 machine.
 - 1. Select **Start** > **RUN** and type **wf.msc**
 - 2. Right click **Windows Defender Firewall with Advanced Security on Local Computer** and select **Properties**
 - 3. Re-enable the **Domain**, **Private** and **Public Profiles** by selecting the **dropdown** next **Firewall state** and change **Off** to **On** (recommended)
 - 4. Select **OK** to close the **Windows Defender Firewall with Advanced Settings on Local Computer**



4.

- Navigate back to your Workspace ONE UEM Console
 - 1. Select **Devices** > **List View** > and select your **Windows 10 device**
 - 2. It take about 5 minutes for your Status to change in Workspace ONE UEM. Keep refreshing your screen
 - 1. If **WNS status: Disconnected** shows then try rebooting your Windows 10 machine.
 - 2. If this does not work Select **Query** > **Security** and **Query** > **Health Attestation**
 - 3. You should now see the device listed as **compliant** and the **Firewall status** as green in the WorkspaceOne UEM console.



5

- Revert back to your Windows 10 virtual machine
 - 1. Open a browser and type Office.com
 - 2. On the right of the page select the Sign into your accounts ICON
 - 3. On the **Sign in** type your **custom user email address** eg. user35crsj@sanjose35.euclivefire.com select **Next**
 - 4. On the Select a certificate window select OK
 - 5. On the Stay signed In? window select NO
 - 6. Notice the Single Sign-On using the **Certificate + the Compliance Check** against UEM worked successfully and you now have access to the application



6.

•

- If you go to Workspace ONE Access, select the Dashboard > Reports > Audit Events
 - 1. Select Show ,
 - notice the EVENT is LAUNCH and your User , the OBJECT is Office365 with Provisioning,
 - 2. Select View Details
 - 3. Notice Audit Events are reporting a successful login using Certificate (Cloud Deployment) and Device Compliance (with AirWatch).

This completes the **Windows 10 Compliance** with **Workspace ONE Access** and **Workspace ONE UEM Lab**. This is a single example of the many options for compliance that could be used not restricted to Windows 10, but also other platforms

	Reports			
	Audit Events From 1 days	User:	Show	
	Audit Eve	nts		
	DATE, TIME (UTC)	USER (DOMAIN NAME)	EVENT	OBJECT
	Nov 14, 2019 5:25:34 PM	user35CRSJ (euc-livefire.com)	LAUNCH (WSFed12)	Office365 with Provisioning
	OBJECT Office365 with Provis View audit eve "testant" 722035 "actorDustries" "	ioning Dents detail VEFIREMB", 9, "user35CRS.", uc-livefire.com, 19433.e014.4ede83c792 a/5.0 (Windows NT 10.0; V 26A91027A046AA724f 26A91027A046AA724f 26A91027A046AA724f 26A91027A046A4724f 1005471, 10054-4346-9f20-135 firea656 with Provisioning" wwser",	Export as CSV View Details View Details view Details cideL1126/ddf*. min64, x64) AppleWebKi ::ese7563759", 2a72c603a",	
IJ	"success" : "true", "actorExternalid" : "resourceType" : "\ } }	"ac7e6c71-a579-43da-b8 WSFed12"	13::4c:dQe5a5e2dQ".	